TSUTOMU SHIMOMURA Y JOHN MARKOFF

TAKEDOWN

Persecución y captura de Kevin Mitnick, el forajido informático más buscado de Norteamérica. Una crónica escrita por el hombre que lo capturó.

La captura del pirata informático Kevin Mitnick tuvo lugar la noche del 14 de febrero de 1995 y fue el final de una de las más espectaculares persecuciones de los últimos tiempos. Mitnick ha sido el "hacker" más buscado de la historia por robar información, valorada en millones de dólares, procedente del sistema informático de distintos departamentos del Gobierno de los Estados Unidos, importantes empresas y universidades. Esta obra relata la historia real de Mitnick y su lucha con uno de los autores

del libro. Fue el día de Navidad de 1994, cuando el pirata informático cometió el error de iniciar un ataque contra los ordenadores de Tsutomu Shimomura, reconocido experto en seguridad y coautor del libro. A partir de ese momento, se produjo un espectacular enfrentamiento, que convirtió a Kevin Mitnick en auténtico objeto de culto en Estados Unidos. Para apreciarlo en todo su alcance, basta con seguir el rastro de decenas de Webs dedicadas a él en Internet.

"Takedown" es el relato de una auténtica aventura informática, con

todos los ingredientes del thriller y de las viejas leyendas de forajidos y perseguidores. Es, además, un inmejorable camino para comprender todo lo que está en juego ante el enorme desarrollo de la informática en el mundo entero.

Tsutomu Shimomura es físico analista y experto en seguridad de sistemas y miembro del Centro de Superordenadores de San Diego. Markoff es periodista del New York Times.

Tsutomu Shimomura &
John Markoff

Takedown

Persecución y captura de Kevin Mitnick

REALIZADO POR

MAKANO


MK
ePUB

Título original: *Takedown (Catching Kevin)*
Tsutomu Shimomura & John Markoff, 1996
Traducción: Héctor Silva

Editor digital:Makano

Este libro está dedicado a
nuestros padres
y a la memoria del padre de John,
Mortimer Markoff

Agradecimientos

Este libro ha sido posible gracias al esfuerzo de numerosas personas. Andrew Gross, Robert Hood, Julia Menapace y Mark Seiden brindaron apoyo técnico a Tsutomu durante las muchas noches de insomnio dedicadas por éste a aclarar la irrupción del 24 de diciembre en sus ordenadores. También Mike Bowen, John Bowler, Liudvikas Bukys, Levord Burns, Soeren Christensen, Dan Farmer, Rick Francis, Brosl Hasslacher, John Hoffman, Bruce

Koball, Tom Longstaff, Mark Lottor, Jim Murphy, Joe Orsak, Martha Stansell-Gamm y Kent Walker aportaron su experiencia técnica y legal. Carl Baldini y Paul Swere, ambos de la RDI Computer Corporation, contribuyeron con hardware. Gracias por su apoyo a Sid Karin y su equipo, en el San Diego Supercomputer Center. Nuestro editor en Hyperion, Rick Kot, nos ayudó a traducir a términos accesibles una historia plagada de infinidad de detalles técnicos, y Tim Race, editor de John Markoff en el *New York Times*, aportó sus conocimientos. Deseamos asimismo dar las gracias a nuestros agentes, John

Brockman y Katinka Matson. Cuando empezamos a escribir, Nat Goldhaber tuvo la amabilidad de ofrecernos su hospitalidad. Un agradecimiento especial a Jimmy McClary y a Leslie Terzian. Y finalmente a Roger Dashen, que es desde hace mucho tiempo amigo y consejero de Tsutomu.

take-down (ták/ doun/) *adj. Deporte*. Movimiento o maniobra propia de la lucha o las artes marciales, en el que un oponente es tumbado por la fuerza al suelo.

The American Heritage Dictionary of the English Language, Third Edition

Hacker es un término sin traducción, que describe al usuario fanático del ordenador, conocedor de todos los detalles del aparato y que sabe modificarlo y utilizarlo incluso

impropiamente. De esto último deriva una segunda acepción, la de intruso o pirata informático, al que los programadores suelen llamar “cracker”, probablemente a partir del sustantivo “crack”, grieta, hendidura, etcétera. *(N. del T.)*

Prólogo

Si se encuentra usted a tres hombres sentados a solas en una furgoneta en el aparcamiento de una zona comercial a las dos de la mañana y uno de ellos está manipulando una antena de extraño aspecto extraerá naturalmente una única conclusión.

Que son polis.

Yo no lo era, y a pesar del alboroto en los medios informativos que habría de estallar tres días después, refiriéndose a mí como "cybercop" y

“cybersleuth”[1], jamás me había propuesto serlo. En el verano de 1995 lo único que yo aspiraba a ser era un aficionado al esquí, y en ese sentido no estaba teniendo mucho éxito hasta el momento. Durante la mejor época para el esquí que se recuerde en California, allí estaba yo una gélida mañana, varado en el aparcamiento de un barrio de Raleigh, Carolina del Norte, muy lejos de cualquier cosa que se pareciese a una pista de esquí.

Manejaba una antena con cierto aspecto de pistola de rayos, y en el regazo acunaba un artefacto que hacía pensar en un temporizador de grandes

dimensiones que emitía una sorda señal sibilante, muy parecida a la que produce un modem cuando establece una conexión.

El sonido proveniente del aparato se había vuelto persistente, prueba de que yo había acorralado a mi presa, un escurridizo bandido informático que, mediante una combinación de astucia delictiva y pura buena suerte, había conseguido mantenerse durante más de dos años un paso por delante del FBI y de al menos otras tres agencias de la ley.

Entretanto, yo había sido una de sus víctimas. En diciembre, él y posiblemente alguno de sus compinches

habían forzado la entrada en mis ordenadores y robado un software escrito por mí, que, perversamente utilizado, podría ocasionar estragos en la comunidad de Internet.

Ahora estaba en condiciones de tomarme la revancha. Pero ninguno de los que estábamos en la furgoneta era policía. El conductor era un robusto ingeniero de una compañía de teléfonos móviles, y en la parte de atrás se sentaba un periodista del *New York Times* que se nos había incorporado siguiendo mi odisea. Diez minutos antes, nuestra furgoneta había rodeado despacio un vulgar edificio de apartamentos,

mientras yo movía la antena a un lado y a otro, concentrado en captar en un visualizador digital la aparición de señales indicativas de que me acercaba a la fuente de la llamada del teléfono móvil. Estaba resuelto a terminar mi persecución, pero en ese momento, en medio del sopor de la fatiga causada por una semana casi sin dormir en persecución de un nebuloso rastro de huellas digitalizadas a través de las redes de ordenadores que forman Internet, experimentaba la tensión a que está expuesto aquel que se excede en un esfuerzo continuado.

Afuera el silencio era total. No

había coches ni gente por la calle, y la presencia de nuestro vehículo deslizándose en silencio en torno al bloque de apartamentos bajo el resplandor amarillo de las luces de vapor de sodio me parecía ostensible. ¿Dónde estaba él? ¿Nos estaba observando? ¿Estaba a punto de huir? Yo vigilaba el indicador del medidor de potencia, que de pronto marcó un descenso. Estaba a nuestras espaldas. ¿Sería al otro lado del edificio? El conductor dobló la esquina y vimos unos terrenos desiertos que se extendían hacia la oscuridad de la distante campiña. Los mapas que habíamos desplegado ante

nosotros en la furgoneta mostraban un parque público.

"Una ruta de escape perfecta", murmuró el periodista desde el asiento trasero.

Doblamos otra esquina y la furgoneta volvió rápidamente al frente de los apartamentos. La antena efectuó un barrido y en el oscuro interior del vehículo observé que los números parpadeaban ascendiendo otra vez. Nuestra furgoneta aminoró la marcha hacia el frente del edificio, y avanzamos sigilosamente por un aparcamiento lleno de coches vacíos. Al aproximarnos a la esquina de los apartamentos nos

detuvimos brevemente. Utilizar un equipo detector de ondas electromagnéticas es algo parecido a jugar a "colocarle el rabo al borrico". Uno recibe pequeñas pistas, pero igual se siente como volando a ciegas, como quien avanza a tropezones en la oscuridad. Ahora, en cambio, por la forma en que saltaba el medidor, yo podía asegurar que nos hallábamos casi encima de nuestro objetivo. En alguna parte, en un radio de treinta metros a nuestro alrededor, alguien estaba inclinado sobre un ordenador en conexión abierta con Internet. Era imposible descifrar el monótono siseo

que demostraba que él se hallaba aún ante el teclado. ¿Dónde estaba ahora mismo?

Los tres agachamos la cabeza para escudriñar un callejón sin salida. Desde el interior del edificio llegaba una luz proveniente de una ventana de la segunda planta. ¿Cómo reaccionaría un fugitivo que se asomara afuera en mitad de la noche y viese una furgoneta provista de una antena deambulando por el sendero de acceso a su casa? Era obvio que huiría, o tal vez algo peor. Yo no tenía la menor idea de cuál era su estado mental. ¿Se encontraba solo? No había motivo para pensar que nuestro

“ciberdelincuente” estuviese armado, pero era tarde, y una fría sensación de duda me surgía en la boca del estómago. “Si fuese él, yo estaría de frente a la ventana”, sugirió el periodista.

Tenía razón: podríamos haberlo estropeado todo. Semanas de penoso trabajo detectivesco a través del país se irían al traste, dejándonos mortificados y con las manos vacías. Decidimos que lo indicado era la cautela. La furgoneta se puso nuevamente en marcha y se desplazó rodeando la esquina del edificio.

UNO:
EL ASALTO

1. El regreso de Julia

¿Es posible cubrir en menos de dos horas, conduciendo hacia el oeste, los 310 kilómetros que hay desde Echo Summit, en la cima de la Sierra Nevada, hasta el Aeropuerto Internacional de San Francisco?

Yo lo intenté el día anterior a la Navidad de 1994, con una tormenta de nieve.

Pensaba que tenía una buena razón. Estaba deseando ver a una amiga a quien

no veía desde hacía más de dos meses y me sentía inquieto en cuanto al punto en que se hallaría nuestra relación cuando ella regresase de sus viajes. Habíamos sido íntimos amigos durante tres años y en el curso de los últimos seis meses se había hecho evidente que éramos más que amigos: estábamos enamorados. Habíamos convenido en que durante el tiempo de separación pensaríamos adónde queríamos llegar en nuestra relación. Ahora yo tenía prisa, porque estaba lleno de expectativas, pero al mismo tiempo de nervios y de incertidumbre. De lo que no tenía noción era de que mi precipitada carrera de un

extremo al otro de California fuera el inicio de una insólita aventura que estuvo a punto de cambiar para siempre mi existencia.

La tarde anterior, Julia Menapace había dejado un mensaje en el contestador automático de mi casa en San Diego: estaba en el aeropuerto de Bangkok y llegaría a San Francisco a las 13:40 del siguiente día, tras un vuelo de catorce horas. ¿Iba a ir a recibirla?

Por supuesto que sí. Había estado pensando mucho en Julia: el mensaje sugería que también ella había estado pensando en mí.

Julia, una mujer alta y graciosa,

fuerte y delgada, que a menudo lleva el cabello hacia atrás en una trenza, había sido programadora en Apple Computer y en otras empresas de alta tecnología de Silicon Valley durante casi una década. De mirada intensa y ojos de un gris azulado, se mostraba a veces introvertida, pero también fácilmente dispuesta a reír. Era una cualificada maestra de yoga y poseía una cualidad etérea que yo encontraba absolutamente cautivadora. Últimamente había estado trabajando como programadora independiente, y sus servicios eran empleados por empresas de alta tecnología en proyectos específicos de

desarrollo de software.

Aunque conocía bien el funcionamiento interno del ordenador Macintosh, nunca se obsesionó con la informática tanto como los hombres con los que trabajaba. Jamás había sido absorbida por completo por la cultura de los fanáticos del ordenador de Silicon Valley; le gustaba hacer muchas otras cosas en la vida, lejos del mundo de los ordenadores en el que el tiempo se mide en nanosegundos. Durante nuestros años de mutuo conocimiento habíamos realizado incontables viajes explorando zonas poco habitadas del país: montañas, fuentes termales, playas.

Compartíamos la afición por lo desierto, en cualquier estación.

A Julia le inspiraba una especial pasión el mundo de la montaña por encima de los seis mil metros, y en el otoño de 1994 partió hacia el Himalaya, pero antes de irse de escalada y caminata por el Nepal tuvimos una gran aventura explorando juntos el suroeste. Hicimos autoestop por los parques nacionales de Bryce Canyon y Zion, y recorrimos las ruinas anasazis en Chaco Canyon. Fue durante esos viajes cuando acabé viendo a Julia como la maravillosa persona que es, y nos enamoramos. Yo sabía que ella quería

que formalizásemos la relación, pero le había dicho que necesitaba pensar si estaba preparado para un compromiso en serio. No habíamos hablado desde inmediatamente después de su llegada a Katmandú, pero al cabo de un par de meses de reflexión decidí que quería estar con ella y pensé que era capaz de cumplir con mi parte del compromiso.

No obstante, no tenía idea de si los pensamientos de ella seguían el rumbo de los míos, y nuestra relación no era sencilla. Las cosas se mantenían ambiguas porque ella estaba además intentando terminar con una relación de siete años que llevaba largo tiempo

arrastrándose hacia un penoso final. El hombre con el que había vivido fue en una época amigo mío, uno de los fanáticos de Silicon Valley y activista de la intimidad de los datos informáticos, muy conocido por su dedicación a asegurar que la misma no fuera a perderse en la emergente edad digital. Había sido un periodo doloroso el anterior a que Julia se fuera del país, pero yo tenía claro que la relación entre ellos había dejado de funcionar y que la cuestión no era si acabaría, sino cuándo.

Pero no sabía qué iba a ocurrir en adelante. Había echado de menos a Julia y estaba deseando verla. Para mí era

importante llegar a tiempo al aeropuerto, aunque hacerlo implicaba venir desde la vertiente oriental de Sierra Nevada hasta cerca del límite del estado. Sólo un día antes me había mudado a una cabaña con techo a dos aguas en las afueras de Truckee, California —a unos doscientos metros de la estación de esquí Tahoe-Donner, en el centro mismo de una meca del esquí de fondo— y lo había hecho con Emily Sklar, una instructora de esquí de la que hacía varios años que era un buen amigo.

En San Diego, donde trabajo la mayor parte del año, me distraigo patinando, pero aunque me divierte, me

gusta mucho más el esquí de fondo. Durante los últimos tres años había aprendido una técnica de esquí llamada de patín, que se parece mucho al patinaje y aporta más velocidad que la tradicional técnica de zancadas que vemos utilizar a la mayoría de los esquiadores. En lugar de esquiar siguiendo dos angostos carriles, los de patín se deslizan hacia adelante colocando cada esquí en diagonal con la pista. También me gusta participar en carreras, y el invierno anterior había empezado a tomármelo de nuevo en serio y había intervenido en varias pruebas de biatlon, una combinación de

esquí y tiro con rifle que exige fuerza, velocidad y control.

La nieve no es, por supuesto, uno de los puntos fuertes de San Diego. El invierno anterior, los vendedores de pasajes y las asistentes de vuelo de Reno Air llegaron a conocerme bien. Una vez hasta incluí en mi equipaje de mano un piolet y lo pasé por la máquina de rayos X. Nadie se inmutó. Sólo en esa temporada de esquí me apunté más de treinta mil kilómetros entre la California meridional y la septentrional. Mi plan este año había sido pasar el invierno esquiando, tomar parte como voluntario en la patrulla de esquí

nórdico, actuar de instructor de esquí a tiempo parcial y, cuando el tiempo lo permitiese, abordar problemas interesantes de investigación.

El tipo de trabajo que hago a menudo, de informática científica e investigación en seguridad de ordenadores, se puede realizar desde casi cualquier lugar. Y como el invierno anterior había acabado volando desde San Diego prácticamente cada fin de semana, este año había resuelto sencillamente instalar mi cuartel general en la montaña durante cuatro meses. Planeaba llevarme un par de estaciones de trabajo Unix y conectar mi propia red

de ordenadores con el mundo exterior mediante una línea telefónica digital de alta velocidad.

Por lo general paso la mayor parte del año ocupando varios cargos. Hasta el invierno de 1995 era miembro residente en el Centro de Superordenadores de San Diego —una dependencia de la Universidad de California en el *campus* de San Diego, sufragada con fondos federales—, a la vez que investigador científico en el departamento universitario de física. El Centro me proporciona un despacho y el acceso a algunos de los superordenadores más rápidos del

mundo. Mi trabajo ha implicado siempre investigar en un área que ha transformado básicamente la ciencia en las últimas dos décadas: la física de ordenadores. La informática ha emergido como una tercera vía del desarrollo científico, ocupando su lugar junto a los tradicionales métodos teórico y experimental.

Mientras que antes era necesario probar las teorías científicas llevando a cabo experimentos en el mundo real, los ordenadores se han desarrollado con tal rapidez que actualmente es posible crear con toda precisión una simulación de hechos reales. Los físicos de

ordenadores procuran resolver problemas científicos mediante simulaciones. Unos ordenadores cada vez más poderosos posibilitan simular cualquier cosa de forma realista, desde el flujo del aire sobre la superficie del ala de un avión hasta la estructura básica de la materia en la cacería del quark.

La física de ordenadores trata asimismo de la propia física de la informática, que descubre cómo se pueden ordenar los electrones para manejar cantidades cada vez mayores de información de una forma cada vez más rápida; y del diseño de máquinas especializadas que superen el

rendimiento de los mejores superordenadores actuales. Como otros muchos en mi campo, que empezaron preparándose como físicos, yo he empezado en estos últimos años a dedicar cada vez más tiempo a problemas informáticos de la vida real, como el de la seguridad. Entre los físicos y los operadores es en cierto sentido una tradición consagrada. El premio Nobel Richard Feynman era famoso en Los Álamos por sus escapadas violando la seguridad en tiempos del proyecto Manhattan. Y Robert Morris, uno de los inventores del sistema operativo Unix y más tarde

principal científico de la Agencia Nacional de Seguridad, fue pionero en el descubrimiento de cómo introducirse sin autorización en un ordenador y cómo protegerlo.

Siempre me ha parecido un reto intelectual irresistible el descubrir las grietas en el blindaje de un ordenador o una red de ordenadores que, desprotegidos, podrían permitir a un ladrón digital saquear los fondos electrónicos de un banco o facilitar a espías extranjeros el acceso a los ordenadores del Pentágono. Es un mundo al que uno no puede aproximarse sólo a un nivel académico o teórico.

Hay que ensuciarse las manos. La única forma de estar seguro de que una cerradura digital es suficientemente sólida reside en saber desmontarla y entender completamente su funcionamiento. Mi investigación con diferentes modelos ha proporcionado nuevas herramientas para evaluar los puntos fuertes y débiles en redes de ordenadores.

Hasta que decidí trasladar mi base de operaciones a la montaña durante el invierno me había estado dedicando cada vez más a la investigación en materia de seguridad informática en el Centro de Superordenadores de San

Diego, o SDSC, donde quien establecía las pautas era su director, Sid Karin, un cincuentón alto, delgado, barbudo e imperturbable, que había sido ingeniero en energía nuclear. Como otros muchos que han llegado indirectamente a la informática, Sid estaba trabajando en la General Atomics, una firma contratista de plantas nucleares establecida en el sur de California, cuando resolvió que él podía desarrollar las complejas simulaciones necesarias para diseñar una planta de energía mejor que los programadores dedicados al proyecto. Una cosa llevó a la otra, y actualmente dirige el Centro, un edificio de cuatro

plantas que alberga un Cray C90 y un superordenador Intel Paragon, con la misión de ampliar las fronteras de la informática de alta energía, así como de la ciencia pura.

El Centro en sí, una aséptica construcción blanca de cuatro plantas situada en la ladera de una colina del *campus* universitario, no es un modelo de realización arquitectónica, y la llamamos "la caja en la que venía el edificio". Pero es un sitio razonablemente adecuado para la investigación, y atractivo para un montón de gente a la que no le gustan los horarios regulares ni las rutinas

burocráticas. Sid apenas parpadeó la noche en que entré patinando en su despacho.

Lo cual no quiere decir que no me haya ingeniado para molestar a algunas personas del Centro. Por ejemplo, tuve un temprano encontronazo con el subdirector de operaciones, Dan D. Drobnis, a quien yo y otros nos referimos a sus espaldas como "D^3".

Un día, en 1992, D^3 me descubrió patinando en el salón de las máquinas, un extenso espacio rodeado de vidrieras donde se aloja el hardware principal del Centro. Se puso completamente fuera de sí, insistiendo en que yo podía

estrellarme contra uno de sus ordenadores de millones de dólares, y jurando que si me acercaba patinando al edificio no volvería a poner los pies en el Centro.

Parecía una actitud extrema y poco razonable. Dado que estaba siempre atravesando el recinto en mis continuos desplazamientos entre la puerta principal y un ordenador especial para gráficos a unos treinta metros de allí, yo pensaba que andar en patines era perfectamente lógico. Pero puedo ser pragmático en ciertos asuntos, y desde aquel incidente, no es exactamente que haya evitado a D^3, pero tampoco he

entrado patinando en su despacho.

Dejando aparte los peores excesos de la burocracia, la vida en el Centro de Superordenadores ha consistido casi siempre en un compromiso razonable. Pero en diciembre de 1994 yo me había jurado que las cosas serían diferentes. Truckee, donde tengo mi cabaña de esquiador, está a veinte kilómetros del lago Tahoe, y la zona a su alrededor posee la ventaja de hallarse a suficiente altitud como para recibir la mayor parte de la nieve y estar a la vez convenientemente cerca de Silicon Valley, donde tienen su sede la mayoría de mis patrocinadores en seguridad

informática. Pero para llegar allí desde la región del lago normalmente hay que atravesar el famoso Donner Pass, donde la caravana de carretas de la partida de Donner quedó atascada en la nieve en octubre de 1846. Fue completamente ilógico por su parte intentar el paso con la estación tan avanzada. Atrapados por fuertes nevadas y ante la perspectiva de perecer de inanición, algunos de los pioneros cayeron en el canibalismo y sólo sobrevivió aproximadamente la mitad de los primitivos ochenta y siete viajeros.

Es una historia que se enseña a todos los niños de California para ilustrar las

penalidades que soportaron sus valerosos antepasados. En la actualidad, empero, la mayoría de los esquiadores que acuden masivamente cada invierno tiende a prestar poca atención a los elementos. Conozco a un ingeniero de software de Silicon Valley en cuya camiseta predilecta se lee "Donner Pass, Calif. Who's for Lunch?[2]" Pero ese día previo a la Navidad de 1994 experimenté un nuevo respeto por el paso de Donner.

Probablemente debí haber partido la noche anterior, y de hecho había considerado por un momento salir entonces y pasar la noche en la ciudad.

Pero parecía que el tiempo se iba a poner asqueroso y con nieve, y yo estaba cansado después de esquiar todo el día, así que regresé a la cabaña y me fui a dormir.

Eran alrededor de las 8:30 de la mañana del 24 de diciembre cuando saqué rápidamente mi Ford Probe alquilado de la aguanieve fangosa del sendero de acceso a mi cabaña. Todavía nevaba ligeramente, pero yo no planeaba salir del coche hasta estar abajo, lejos de las montañas, de modo que iba vestido para el invierno de California: camiseta y *shorts* Patagonia, gafas de sol Oakley y sandalias Teva. Contaba

con tiempo suficiente para un viaje descansado: por Donner Pass en la Interestatal 80, luego las estribaciones de las colinas, la travesía por Central Valley, la autopista hacia el sur por Berkeley, el puente, y finalmente al sur por San Francisco en dirección al aeropuerto situado en el borde occidental de la bahía. Calculaba estar allí a las 11:30, o a mediodía, si me detenía a tomar un batido de fresa en el bar de Ikeda, en Auburn.

Poco después de salir llamé a Caltrans por mi teléfono móvil para conocer la situación en la carretera y recibí la mala noticia: había “control de

cadenas" en la Interestatal 80 que va por las montañas. Eso significaba que allá adelante estaba nevando mucho más fuerte y que la CHP (Patrulla de Carreteras de California) estaría deteniendo a los coches para comprobar si llevaban cadenas y obligando a dar la vuelta a los que no. Por supuesto, mi Probe de alquiler no las tenía.

El informe afirmó que la carretera 50, que se extiende desde Sacramento hasta el extremo sur del lago Tahoe, estaba aún abierta. Hice un giro en redondo y partiendo en la dirección opuesta pasé por Squaw Valley y fui por la orilla del lago que pertenece a

California. Pero cualquier esperanza de poder eludir la tormenta y dejar rápidamente atrás el puesto de control de cadenas de la carretera 50, se evaporó noventa minutos más tarde, cuando llegué a South Lake Tahoe. Ante mí se extendía una larga fila de coches retenidos en la estación de control de cadenas de la CHP.

Estaba empezando a comprender lo mal preparados que debieron sentirse los Donner cuando se dieron cuenta de que la primavera no llegaría suficientemente pronto. Di media vuelta con el Probe y me fui pitando a la ciudad. Cincuenta dólares y una hora

después estaba de nuevo en la cola del control de cadenas, esperando con los demás para iniciar la lenta travesía de Echo Summit por la carretera 50.

Se hicieron casi las 11:30 antes de que me pusiera realmente en marcha. Tomad nota, ingenieros de la Ford: vuestro modelo básico Probe puede hacer 130 kilómetros por hora con las cadenas puestas, aunque con un ruido bastante molesto.

Tengo un detector de radar, lo que es una gran cosa cuando recorres largos tramos a alta velocidad en Nevada. Pero en California un detector no sirve de mucho, pues la CHP ha descubierto un

sencillo y eficaz método para pescar a los velocistas que lo llevan. En lugar de utilizar un radar, simplemente sitúan su coche blanco y negro en una rampa de entrada a la carretera, siguen al infractor a su misma velocidad durante un trecho que les permite tomarle el tiempo y luego tranquilamente cobran su presa.

Aquel día tuve una suerte tremenda, o todos los coches de la CHP estaban demasiado ocupados en controlar las cadenas para preocuparse por los excesos de velocidad.

Por el camino hice una llamada para comprobar la hora de llegada del vuelo del puente aéreo de la United en el que

Julia venía de Los Angeles. Era previsible que yo iba a llegar tarde, así que le pedí a la compañía que le transmitiera un mensaje. El mensaje no la alcanzó en Los Angeles, de modo que llamé otra vez y le pedí a la United que se lo hiciera llegar al avión, y ellos me prometieron que lo harían.

Fue un viaje de más de 300 kilómetros conduciendo por carreteras californianas, y calculo que hice un promedio de 155 por hora —algo menos con las cadenas puestas— durante los primeros 130 kilómetros de la carretera 50, y ciertamente mucho más después de haberme detenido para quitar las

cadenas.

Hacia la 1:30 había conseguido llegar, aparcar y situarme al borde mismo de la zona de control de seguridad del aeropuerto, cuando Julia, con su andar desmañado, bajó por la escalera mecánica de la terminal de la United Airlines. Por su expresión comprendí que estaba sorprendida de verme.

"Veo que no recibiste mi mensaje", dije.

"¿Qué mensaje?", replicó ella. Pero no importaba. Nos abrazamos. Más tarde me dijo que le había parecido algo preocupado.

2. Toad Hall

De todas las preguntas suscitadas por el primer ataque hay una que todavía me intriga: ¿fue simplemente una coincidencia extraordinaria que la incursión inicial fuera lanzada desde Toad Hall?

Toad Hall, una mansión de dos plantas de estilo Reina Ana exquisitamente restaurada, ubicada al norte del distrito de Haight-Ashbury y el Golden Gate Park, en San Francisco, es

propiedad de John Gilmore, un operador de Unix, libertario, y decidido impulsor de la intimidad en el medio electrónico. John había sido asimismo el quinto empleado de Sun Microsystems en 1982, años antes de que ésta se convirtiese en empresa pública y en uno de los líderes mundiales en la fabricación de estaciones de trabajo y sistemas de redes. Se fue de la Sun cuatro años más tarde, pero los millones que hizo por haber sido uno de los primeros empleados de una de las compañías americanas de mayor éxito, le permitieron comprarse una hermosa residencia.

El nombre que eligió para el lugar proviene obviamente del de la casa del Sr. Sapo en el clásico infantil de Kenneth Grahame *El viento en los sauces*. Ocurre además que "Sapo" era el apodo de una mujer con la que John vivía cuando compró la casa. En cualquier caso, el nombre era adecuado, porque el Sr. Sapo de la ficción era un personaje acaudalado y un espíritu libre, como lo era también el señor John Gilmore.

Con John y los amigos instalados, Toad Hall se convirtió en un prototipo: fue uno de los primeros hogares dotados de una red informática digital de San

Francisco, ciudad en la que siempre parecen aceptarse primero las nuevas tendencias sociales. En los cincuenta fue la generación *beat*, en los sesenta los *hippies*, en los setenta la sexualidad alternativa, en los ochenta fueron los *punks* del monopatín. Ahora en los noventa, las cibercomunas parecían brotar allí por todas partes.

El término define a un grupo de artistas indigentes, o de mensajeros en bicicleta, o incluso de hackers del distrito financiero, que se asocian para alquilar una casa o un piso o un apartamento con objeto de reunir entre todos el dinero necesario para compartir

una línea de cincuenta y seis kilobytes por segundo —arrendada a la compañía telefónica por varios cientos de dólares mensuales— con la que conectarse a Internet. Si es más solvente, el grupo podría reunir varios miles para un equipo especializado y tal vez un millar de dólares al mes para una conexión T-1 todavía más rápida.

Una línea T-1 es capaz de proporcionar datos informáticos desde la Red como vertidos con una regadera, en comparación con el chorrito de los modem que la mayoría de la gente utiliza para conectar con servicios interactivos tales como CompuServe, Prodigy y

American Online. Una línea T-1 transmitirá 1,5 millones de bytes de información por segundo. Eso es suficiente para verter el texto completo de *Moby Dick* en doce segundos o ver una película a toda pantalla en tiempo real. (Antes de que las cosas se vuelvan de verdad interesantes será necesario que las velocidades en las redes digitales se incrementen aproximadamente en dos órdenes de magnitud —el equivalente de una boca de riego—, algo que probablemente no ocurrirá antes del final del siglo).

Para mí la Red es parte de mi trabajo, pero comprendo que la gente

que tiene que pagarse su vía de acceso pueda tratar de formar una cooperativa. Aun así, la idea de comunidad me resulta rara. Si el objeto de Internet es construir "comunidades virtuales" —conjunción electrónica de personas sin vínculos personales "cara a cara"— ¿no parece extraño que sientan la necesidad de vivir también juntas? En cualquier caso, cuando se mudó a la residencia Reina Ana en 1987, John Gilmore no estaba siguiendo una tendencia, sino inaugurándola. El edificio tenía dos plantas, una para él y su compañera y la otra al principio para uso de un amigo, a quien en determinado momento se la

compró. Desde el comienzo aquel lugar no estuvo destinado a simple residencia; fue un sitio para vivir conectado. Pronto un cable coaxial de transmisión Ethernet se abrió camino por toda la casa. Aparecieron asimismo terminales de ordenador situadas en lugares diversos, desde las cómodas en los dormitorios hasta mesas en el sótano, para uso de los distintos residentes, huéspedes y visitantes ocasionales que frecuentaran Toad Hall o parasen allí. En el espacio donde otra persona habría colocado un perchero, en el vestíbulo de entrada a su piso de la segunda planta, John Gilmore instaló una Sun SPARCstation ELC.

Siguiendo la nomenclatura de Internet, Toad Hall adquirió el nombre de dominio *toad.com*, cuya vía de entrada para el resto del mundo era un ordenador Sun SPARCstation situado en el sótano del edificio. Este dominio digital era administrado por John y una ecléctica banda de programadores y *gurús* del hardware, que juntos tenían una orientación política diversa, y aunque la intimidad era prioritaria, la seguridad informática en Toad era con frecuencia muy laxa.

El experimento de John Gilmore en Toad Hall engendró con el tiempo una temprana cooperativa de Internet

llamada The Little Garden[3], nombre del restaurante chino en Palo Alto en el que tuvo lugar la primera reunión organizativa. Iniciada por un notorio fanático de los ordenadores de San Francisco llamado Tom Jennings, The Little Garden fue una de las primeras formas de conectarse directamente a Internet a bajo costo. Pero a diferencia de las actuales cibercomunas de residentes, The Little Garden no requería estar físicamente alojado en Toad Hall para disfrutar de sus beneficios electrónicos. Un miembro adquiría dos modem y colocaba uno en su casa y el otro en el sótano de Toad

Hall. Este segundo modem se conectaba mediante un router o distribuidor de comunicaciones a la red de enlace a Internet, y como resultado los miembros estaban permanentemente en la Red.

La instalación resultaba económica, porque Pacific Bell brindaba un servicio telefónico residencial sin contador. De modo que era posible dejar conectada las veinticuatro horas la línea operativa desde un teléfono de oficina por sólo una cuota mensual que los miembros aportaban a The Little Garden. Si la línea se cortaba, el modem situado en The Little Garden restablecía sin cargo la comunicación. Con el tiempo Toad

Hall tuvo más de una docena de líneas telefónicas conectadas con el lugar, y los instaladores de la Pac Bell probablemente se preguntarían qué clase de negocio turbio estarían montando allí John y su pandilla.

Toad Hall había sido el hogar de Julia durante los últimos cinco años, puesto que John Gilmore era "el otro", con quien su relación se había venido pudriendo aún antes de conocernos. En las vacaciones navideñas John se ausentaba para visitar a sus parientes en Florida, de modo que cuando Julia y yo llegamos a las cuatro de la tarde del día de su regreso desde Nepal, teníamos

Toad Hall para nosotros.

Yo conocía a John, que ahora andaba por la cuarentena, de los círculos de hackers, e incluso como amigo, desde hacía años. Él había contribuido años atrás a fundar una segunda compañía basada en algunos de los principios de una organización llamada Free Software Foundation. La idea motriz de la compañía, llamada Cygnus Support, era no vender directamente el software sino, en cambio, regalarlo y luego vender la asistencia y el mantenimiento que las empresas iban a requerir para el pleno aprovechamiento de programas tales

como lenguaje de ordenadores y herramientas de seguridad desarrolladas por la Cygnus. Es una idea de mucha enjundia, y la compañía prosperaba, incluso en un mundo dominado por Microsoft.

Delgado, con barba y el rubio cabello hasta los hombros, vistiendo a veces camisas de flores que estuvieron de moda en Haight-Ashbury por los años sesenta, John se había lanzado a la nueva empresa con una pasión que consumía la mayor parte de sus horas de vigilia. Al principio no le había importado que Julia y yo saliésemos continuamente juntos de excursión

mientras él trabajaba largas horas en su nuevo negocio, porque no le interesaban las caminatas. Pero una vez que Julia y yo intimamos en nuestra relación, las cosas entre él y yo se enfriaron.

Julia y yo encargamos la cena a un restaurante italiano llamado Bambinos. Cuando la trajeron, nos desvestimos y nos sumergimos en la bañera caliente, y comimos metidos en el agua.

En Toad Hall, el cuarto de baño de arriba es una habitación fuera de lo corriente. El suelo y un zócalo de mármol rosa y verde rodean una bañera jacuzzi de color verde oscuro y los demás elementos. En el alféizar de la

ventana hay una gran mata de espárrago centrada sobre la cascada del grifo mayor de la bañera. La fronda del helecho cae hacia el agua. Julia había puesto un casete de Karma Moffet tocando instrumentos himalayos y había encendido velas; el resto de la luz provenía de cuatro focos en lo alto que iluminaban débilmente cada esquina de la bañera.

"Esto es fantástico", murmuró Julia envuelta en vapor. Dijo que había soñado continuamente con sumergirse en agua caliente durante sus caminatas por el gélido Himalaya, donde el agua se transporta a mano desde la fuente y sólo

se calienta cuando está encima de las llamas, y donde nunca hay suficiente para bañarse. Y que en la elevada región de Solu Khumbu, en Nepal, el único calor había provenido del sol, de la pequeña cocinilla, y a veces de alguna estufa de leña alimentada con trozos de madera o con estiércol.

Mientras comíamos, Julia me contó episodios de sus aventuras. En la cocina de una cabaña donde se alojaba conoció y trabó amistad con un guía sherpa llamado Tshering y una guía de montaña oriunda de Seattle llamada Rachel DeSilva, que había conducido a un grupo de doce mujeres en la ascensión a

un pico de 6.000 metros en la región conocida como Mara. A continuación la habían invitado a escalar otra montaña, llamada Lobuche, situada al norte en dirección al Everest. Había conseguido llegar casi hasta la cima.

Yo estaba fascinado. "Ojalá yo también hubiera estado allí", fue lo único que se me ocurrió decir.

Julia había pasado su cumpleaños en el monasterio de Tengboche para celebrar el festival de Mani Rimdu. Me mostró el collar de cordel rojo que un lama tibetano le había entregado al bendecirla por su trigésimo quinto cumpleaños.

“Esa misma vez, cerca de mediodía, oí sonar unos largos cuernos, címbalos y tambores”, recordó. “Entonces se produjo una avalancha, como en cámara lenta, sobre la cara sur del Ama Dablam”.

Contó que en un momento posterior del viaje se había detenido en un lugar a contemplar la puesta de sol sobre el Everest mientras iba oscureciendo, y que fue algo tan grandioso y bello que la hizo llorar. “Pensaba en ti”, me dijo, “y deseaba que estuvieras allí para compartirlo conmigo”.

Metidos en el agua, le conté lo que me había ocurrido a mí durante su

ausencia. En el momento de su partida, yo había estado esperando una beca de investigación de 500.000 dólares anuales de la Agencia de Seguridad Nacional (NSA), la organización estatal que se ocupa de la seguridad electrónica. La NSA tiene dos misiones: una es la del espionaje exterior y la otra ocuparse de la seguridad de todos los ordenadores y comunicaciones del Gobierno. En otoño, una dependencia de seguridad informática de la Agencia me había prometido financiar un proyecto que me permitiría formar un equipo de expertos para realizar investigaciones en nuevos ámbitos de seguridad en

ordenadores. Yo estaba preparado para empezar y tenía gente comprometida para iniciar el trabajo, pero la Agencia había estado meses dándole largas al tema. Al final me había hartado del asunto, y dos de mis investigadores habían tenido que aceptar otros trabajos.

"Yo creía que todo estaría resuelto y que a mi regreso te encontraría muy satisfecho trabajando con tu equipo", dijo ella.

"Pues no", contesté. "Son asombrosamente ineptos, como todas las burocracias oficiales".

Hablamos un rato sobre la NSA y de cómo hay cantidad de gente en la

comunidad de las libertades civiles que le temen como al Gran Hermano, así como a cualquiera relacionado con ella, con el argumento de que estos últimos se corrompen por contacto. Aunque a mí nunca me lo ha parecido. Mis experiencias indican que se trata de una organización muy grande e incompetente, atada por infinidad de normas que no sirven de mucho ni para bien ni para mal. Y que cualquier persona está perfectamente capacitada para tomar sus propias decisiones.

"No quiero hacer tratos con ellos", dije.

"Lamento que no haya funcionado,

Tsutomu", dijo ella suavemente.

Estuvimos un rato remojándonos, cada uno perdido en sus pensamientos. Finalmente, cambié de tema.

"Quiero decirte algo en lo que he estado pensando", dije. "He pensado en muchas cosas mientras estabas fuera. Realmente me gustaría que tuviésemos una relación formal, si a ti te apetece".

Julia sonrió. Sin decir nada, se inclinó y me apretó contra ella.

Al parecer ahora podríamos pasar un montón de tiempo juntos. Le dije que había pedido vacaciones en la universidad y que estaba deseando irme lejos a esquiar. Por fin estaba

cumpliendo mi viejo plan de pasar un invierno en las montañas, esquiando por las mañanas y al atardecer, y dedicando el resto del tiempo a pensar y trabajar en mis proyectos de investigación.

"¿Por qué no te vienes a vivir conmigo en la montaña?, le sugerí. "Puedes esquiar, y estar fuera nos hará bien".

Nos despertamos a eso de la una de la tarde del día siguiente y Julia —que se crió en la costa Este y todavía no está del todo acostumbrada a la suavidad de los inviernos de California— me dijo que antes de quedarse dormida había visto las primeras luces del alba y había

pensado “Es Navidad, y aquí no se ve la menor señal”. Todavía estaba bajo los efectos del *jet-lag* y sentía además lo que temía que pudiera ser un constipado en ciernes. Resolvimos pasar el día en casa, poniéndonos al día con la charla y el sueño. Fuera de la bañera, en Toad Hall hacía frío, de modo que Julia, todavía ávida por absorber el calor de la civilización tras dos meses en el Himalaya, puso en marcha la calefacción central.

Poco después, mientras ella descansaba, estuve recorriendo la casa y pasé varias veces delante de la Sun SPARCstation del vestíbulo. Era un

recordatorio de que probablemente tuviese correo electrónico esperándome, pero no tuve ganas de comprobarlo.

No obstante, más o menos en ese momento, unos ominosos bytes de información circulaban por el cable Ethernet que discurría por las habitaciones y vestíbulos de Toad Hall. Desde alguna parte, tal vez a miles de kilómetros de distancia, un intruso electrónico se había hecho con el control de *toad.com* operando por control remoto la SPARCstation del sótano. Y mientras nosotros pasábamos el día juntos dos plantas más arriba, el secuestrador electrónico estaba

utilizando *toad.com* como plataforma para lanzar un ataque contra los ordenadores de mi casa en la playa, a unos 800 kilómetros al sur.

No me di cuenta esa tarde, pero el intruso se había hecho "raíz" de *toad.com*. La cuenta raíz es un omnipotente administrador de sistema de ordenadores, una rutina capaz de controlar cada operación de una máquina Unix. Por lo general está reservada al encargado o administrador de un ordenador. En un ordenador Unix como la SPARCstation del sótano de Toad Hall, ser "raíz" es como ser Dios. Una vez que se ha convertido en su

“raíz”, el operador de un ordenador puede crear y eliminar cuentas y archivos, leer el correo o los documentos de cualquier otro operador, estar al tanto de cada pulsación de otro en el teclado o manipular el software de un ordenador para copiar programas que crean secretas puertas traseras para facilitar la entrada la próxima vez.

Fuera quien fuese, el que invadió el sistema poseía un razonable grado de conocimiento y manejo de redes de ordenadores, o cuando menos de la insuficiente seguridad de *toad.com*. Era obvio que, fuera quien fuese, también había elegido como blanco específico

mis ordenadores en San Diego, sea como vendetta personal o porque suponía que mis archivos eran valiosos.

Como miembro de un pequeño grupo altamente cualificado de investigadores en seguridad de ordenadores en este país, yo poseo máquinas que almacenan información delicada, como informes sobre los fallos, errores, lagunas y vulnerabilidad de sistemas descubiertos en varios tipos de hardware y software de amplio uso, y tengo asimismo un repertorio de herramientas de seguridad. Pero había tomado muchas precauciones y el material que consideraba extremadamente valioso no era

accesible. Aun así, había una parte de la información y de las herramientas que sí estaba al alcance del decidido intruso, y que en malas manos podía ser empleada para forzar la entrada en otros sistemas de ordenadores civiles o gubernamentales, o vendida en el mercado del espionaje empresarial.

Esa noche volvimos a pedir la cena fuera, esta vez comida hindú. Mientras aguardábamos que llegase, Julia empezó a deshacer el equipaje y yo dediqué el tiempo a instalar un nuevo ordenador portátil que había recogido de casa de un amigo el día anterior después de salir del aeropuerto. Fabricado por RDI, una

empresa de la zona de San Diego a la que asesoro, se trata de un terminal compacto Unix, y yo me había ofrecido para probar el nuevo modelo. Por un momento pensé en conectarlo a la red de Toad Hall, pero no lo hice. No tenía la menor idea de que alguien estaba dedicando el día de Navidad a cometer una felonía por Internet.

Julia se sentía mal cuando despertó a la mañana siguiente, de modo que en lugar de salir de caminata por los Headlands —en Marin County, al otro lado de la bahía— como habíamos planeado, pasamos otro día tranquilo en

Toad Hall. Afuera hacía frío y estaba gris, y el único momento en que salimos de la casa fue a mediodía, cuando anduvimos hasta Haight Street para comer en Cha Cha Cha, un lugar de tapas que atrae a una variada multitud, que va desde quienes viven en el Haight hasta oficinistas del distrito financiero, pasando por gentes de tez y tipo étnico diverso procedentes de todos los rincones de la ciudad. Esa noche iba a llegar John, y era evidente que había cuestiones de las que Julia y él tendrían que hablar. Yo tenía cosas que hacer en la zona de South Bay, y si todo salía bien, dentro de unos días Julia vendría a

esquiar conmigo.

"Te veré pronto, te quiero", dijo ella mientras me encaminaba a la puerta.

"Cuídate", dije yo, y nos abrazamos.

Poco después de las 8 de la tarde monté en el Probe para cubrir el trayecto de 50 kilómetros en dirección sur hacia Silicon Valley, donde había acordado visitar a un amigo llamado Mark Lottor. Mark, joven de treinta y un años experto en hardware y niño prodigio en Internet, era un amigo con quien yo había pasado mucho tiempo explorando la tecnología del teléfono móvil. Mark es bajito y lleva el corto cabello castaño cayéndole descuidadamente sobre la frente, pero

tiene una osada afición: trepar de vez en cuando a trenes de carga como un vagabundo y darse así una vuelta por el Oeste. Pero la mayor parte de su tiempo lo dedica a Network Wizards, la pequeña empresa que lleva desde su hogar en Menlo Park y que fabrica y vende diferentes herramientas informáticas útiles, que van desde sensores de temperatura para ordenadores hasta las que se emplean para diagnóstico y vigilancia en las redes de teléfonos móviles, muy apreciadas por las empresas del ramo y las autoridades. Él y yo habíamos desmontado juntos el software que

subyace en el corazón del teléfono móvil Oki. Mark lo había destacado originalmente como un instrumento tecnológico bien concebido, y yo había leído su informe sobre el Oki 900 e incluso me había comprado uno. Una vez enterados del funcionamiento del software, comprendimos cómo podría controlarse con un ordenador personal. Por poco más de cien dólares, su hardware y su software permiten que un Oki y un barato ordenador personal rivalicen con unos voluminosos productos comerciales de diagnóstico que cuestan muchos miles de dólares.

La mayoría de la gente conoce a

Mark por su encuesta bianual de los ordenadores directamente conectados a Internet, equivalente electrónico de un censo del Ministerio de Comercio. Mark ha escrito un software que "se pasea" sistemáticamente por Internet, haciendo preguntas de comprobación en prácticamente todos los dominios informáticos importantes. Como en el caso de los humanos, muchos ordenadores optan por no responder, pero los números de Mark constituyen la mejor base para una estimación razonable del tamaño de Internet y de su rapidez de crecimiento. Su encuesta más reciente a mediados de 1995 registró 6,6

millones de ordenadores con conexión a Internet. Desde luego, esa cifra no indica cuántas personas están realmente en la red, pues un ordenador directamente conectado a Internet puede ser la entrada a la red para decenas, centenas e incluso millares de usuarios con su propio ordenador personal. Aun así, la mayoría de las estimaciones, desde las conservadoras a las audaces, se fundan en la encuesta de Mark.

Iba conduciendo presa de una cierta ansiedad, pues llevaba algún retraso para mi cita para cenar con Mark y unos amigos, y porque seguía pensando en Julia. La US 101 al sur me llevó fuera

de San Francisco pasando Candelstick Park, el aeropuerto y el margen de la bahía con su desarrollo industrial urbano, que constituye la expansión del propio valle hacia el norte. La carretera estaba húmeda debido a una fría lluvia reciente, una buena señal. Significaba más nieve allá arriba en las montañas. Mi plan era recoger a Julia en un día o dos, luego retornar a la sierra y a un invierno que parecía prometer el mejor esquí en años.

Eran poco menos de las ocho y me encontraba cerca del paso elevado de la carretera 92, límite norte no oficial de Silicon Valley, cuando una llamada del

teléfono móvil interrumpió mis pensamientos.

"Tsutomu, soy Andrew". No necesitaba haberse identificado, pues su voz, con un dejo residual de vocales de Tennessee, es reconocible al instante.

"¿Tienes un minuto? ¿Puedes buscar una línea ordinaria?"

"No me viene muy bien", respondí. Andrew Gross, que se encontraba pasando las Navidades en casa de sus padres, en Tennessee, era un estudiante de ingeniería eléctrica graduado en la Universidad de California en San Diego, y trabajaba conmigo en problemas de redes y seguridad en el SDSC (el

Centro). Era una gran promesa como investigador en seguridad informática y yo me había convertido para él en una especie de guía. Como parte de su aprendizaje, Andrew solía ocuparse de mi red cuando yo me ausentaba. Mientras hablábamos, tuve la clara impresión de que realmente lo inquietaba que yo estuviese utilizando un teléfono móvil y al mismo tiempo que tenía algo grave que decirme. Lo insté a que me diera una idea general en términos que no fuesen reveladores sino para mí.

"Dime *grosso modo* de qué se trata", dije. En el estado de ansiedad en que ya

me encontraba no tenía interés en afrontar nuevos problemas. Él hizo una pausa. Evidentemente, estaba meditando qué podía decir que no hiciera sospechar a la docena de tíos aburridos o entrometidos que probablemente en aquel momento utilizaban un radioescáner para captar ondas de telefonía móvil, como algunos lo hacen para escuchar las de la policía de carretera.

"Bueno", dijo finalmente. "Tus directorios de seguridad se han reducido".

Lo que me estaba diciendo era que alguien había forzado mis ordenadores.

Experimenté un sentimiento de malestar, algo así como cuando te das cuenta de que has sido víctima de un carterista. Repasé mentalmente con rapidez las implicaciones, pero mi reacción inmediata no fue de pánico sino de irritación ante un descuido más. Estuvimos hablando un rato y poco a poco me di cuenta de que lo que él había descubierto no era un error en los números. Se trataba de algo grave y había que ocuparse de ello.

Mi red está preparada para conservar un archivo con el registro de todas las conexiones efectuadas desde el mundo exterior: un registro completo de

quién lo hace y cuándo. Como rutina, un resumen de esta información es transmitido cuatro veces al día a un distante ordenador controlado por Andrew. Normalmente, los archivos deben resultar más extensos de una transmisión a otra. Si se había vuelto inesperadamente más corto, la conclusión lógica era que alguien había intentado borrarlo.

"Oh, joder", dije y estuve un momento pensando en qué era lo mejor que podía hacerse. "¿Por qué no conectas y ves si notas algo?", le sugerí. "Yo iré a otro sitio y veré si me entero de algo. Te llamaré dentro de un rato".

Conectados a mis ordenadores tengo un par de modem que me sirven para entrar directamente a mi red. A Andrew no se le había ocurrido conectar de ese modo con nuestras máquinas, pero ambos sabíamos que si apagábamos nuestra conexión directa con Internet nadie podría volver a introducirse fácilmente por la red, y sería más probable que los datos de mis ordenadores quedaran tal y como estaban cuando Andrew descubrió la reducción de los registros. Él ofreció enviarme los archivos acortados al terminal de correo electrónico que habitualmente llevo conmigo.

“Ten cuidado”, fue lo último que dije antes de colgar. “Asegúrate de proteger las pruebas”.

La seguridad electrónica supone un montón de compromisos. El arte está en conseguir una serie de compromisos asumibles. Es posible lograr una seguridad informática total: simplemente con que desenchufemos el ordenador y lo guardemos en una cámara acorazada, ni siquiera el mejor de los ladrones podrá robar información. Pero esta solución extrema implica asimismo que el ordenador no se pueda utilizar. Yo, como todo el mundo, tengo que hacer

concesiones en cuanto a la seguridad de mis máquinas y asumir algunos riesgos conexos.

Aunque, como muchos han comentado, Internet se parece actualmente al Salvaje Oeste, con un montón de verdaderos forajidos vagando por ella, eso no siempre fue así. Cuando yo iba al colegio en Caltech, y más tarde cuando trabajaba como investigador en física en Los Álamos, el mundo aún no había despertado a la Red. La cultura prevalente todavía ponía de manifiesto sus orígenes en ARPAnet, la antecesora intelectual de Internet establecida en 1969 y financiada por el Pentágono, y

semejaba una pequeña comunidad en la cual todo el mundo se conocía. Uno saludaba a su vecino en la tienda de comestibles y dejaba abierta la puerta de su casa.

Hoy día, con millones de personas clamando por conectarse a Internet, las normas han cambiado. El mundo avanza impetuosamente, y todo tipo de negocios y formas de comunicación concebibles adoptan la vía electrónica, y van y vienen por redes originalmente pensadas para compartir información, sin protegerla. En consecuencia, existen numerosos objetivos para tentar a bandoleros y asaltantes informáticos.

Una de las mayores dificultades para detectar un delito en el ciberespacio reside en la amplitud de las posibilidades de actuar sigilosamente en él. En el mundo material, si un ladrón penetra en la bóveda de un banco, la ausencia del dinero hará evidente que ha habido un robo. En el ciberespacio, esa bóveda puede ser destripada sin que quede rastro, al menos a primera vista, de que haya ocurrido el robo, porque el botín no consiste en el software o los datos que el ladrón pudiera llevarse, sino en la realización de una copia. Incluso programas comerciales evaluados en millones de dólares

pueden copiarse en un instante dejando intacto el original. Se trata únicamente de bytes.

En la comunidad de la Red existe una escuela de pensamiento que sostiene que, puesto que un programa de software es infinitamente copiable, las nociones convencionales sobre derechos de propiedad tienen escasa relevancia. El software debe ser libre, dicen, y propagarse libremente, y los derechos de propiedad intelectual del software no deben existir. Un prominente expositor de esta filosofía es Richard Stallman, que ha contribuido a fundar grupos tales como la Free Software Foundation y la

League for Programming Freedom.[4]

Yo creo que quien debe decidir si se desprende gratuitamente del software o ha de ser compensado por la dura tarea de escribirlo es su creador. Y ciertamente no experimento simpatía alguna hacia quienes pervierten la filosofía de la libertad de software con el razonamiento de que si puede copiarse libremente debería haber libertad para robarlo. No es admisible entrar ilegalmente en el ordenador de otro.

En estos últimos años, a medida que la Red se ha vuelto cada vez más comercial, los vendedores de

ordenadores han empezado a vender "soluciones" en materia de seguridad: hardware y software de protección que se supone hacen imposible que los vándalos se introduzcan en el ordenador de uno. Pero el problema con muchos productos de seguridad es que se trata de medidas protectoras temporales cuya propaganda excede con mucho a su utilidad. Su objeto es hacer que la gente se sienta mejor acerca de la seguridad, sin hacer nada realmente.

Una de las defensas más comunes se llama firewall[5], un programa que se interpone entre Internet y el ordenador, y está diseñado para permitir únicamente

el paso de bytes cuidadosamente examinados. Cualquier dato no reconocido como familiar resulta bloqueado. El problema con estos muros es que si bien pueden ser un filtro sumamente eficaz, también pueden hacer engorroso el uso del propio ordenador en una red. De hecho, crean una Línea Maginot en vez de una verdadera seguridad. Un muro de fuego proporciona un sólido blindaje, pero no impide que el tierno y consistente meollo en el corazón de su red sea vulnerable.

Me niego a que un temor paranoico obstaculice mi actividad. Mis

ordenadores están conectados a la Red porque ésta es un recurso que no sólo me permite compartir mi trabajo con una comunidad de investigadores, sino que además hace que todo un mundo de información —software, otros ordenadores, bases de datos— sea accesible desde mi teclado. Cualquier cosa más o menos delicada que trate de enviar o recibir por la Red es codificada por un programa que lo hace incomprensible para quien no posea la clave. Pero mis ordenadores no están rodeados por ningún extraño muro electrónico.

Tomo en cambio otras precauciones

menos complicadas como encriptar mensajes, mantener registros de actividad y guardarlos, en algunos casos con alarma. El verdadero secreto de la seguridad informática consiste en mantenerse alerta, vigilar cuidadosamente los sistemas, algo que la mayoría de la gente no hace.

Cuando un intruso se cuela en un ordenador por Internet, uno de los pasos que da como norma para evitar ser detectado es borrar los rastros de su presencia en el ordenador que ha atacado. Con frecuencia entra en los archivos de conservación automática de registros, los archivos de registro

generados por el sistema, y suprimen las huellas de su propia actividad.

Pero esto crea una situación que pocos intrusos informáticos se detienen a considerar: cuando borran el registro de su actividad, el tamaño del archivo se acorta súbitamente. En el SDSC y en mis máquinas en casa tenemos un sencillo recurso electrónico para darnos cuenta de ello. Cuando Andrew conectó con la Red desde la casa de sus padres en Tennessee para leer el correo había comprobado los directorios de nuestros archivos de registros y se dio cuenta de que teníamos huéspedes no invitados.

Me llevó otros veinte minutos llegar a la casa adosada de dos plantas de Mark. Él vivía en un edificio situado en la acera de enfrente de SRI International, el laboratorio donde hace un cuarto de siglo fue creada ARPAnet.

La creatividad se prolonga en el interior de la casa de Mark. El lugar está repleto de ordenadores personales y estaciones de trabajo, todos conectados en bloque a una red de área local. Al igual que las cibercomunidades de San Francisco, posee una conexión T-1 con el mundo exterior. Mark tiene asimismo en la sala de estar el tótem del perfecto

hacker: una máquina expendedora de Coca Cola de estilo 1950 que proporciona un toque de diseño industrial clásico. La máquina está casi siempre llena de agua embotellada, pero a veces tiene realmente Coca.

Mark me esperaba. Tenía planeado que fuésemos a Palo Alto, a pocos kilómetros de allí, a reunimos con algunos amigos para cenar, pero vio que yo tenía la mente en otra cosa.

“Lo siento”, dije. “Ha surgido algo. Necesitaré unos minutos”. Le expliqué brevemente que había tenido una intrusión y que quería evaluar los daños.

“Espero que no te lleve mucho

tiempo”, dijo Mark. “Tengo hambre”.

Pero me comprendía; el otoño anterior había pasado semanas luchando para expulsar a un obstinado ladrón electrónico que intentaba robarle el software de su teléfono móvil.

Yo sentía la urgencia de ocuparme del asunto rápidamente, antes de que los datos almacenados en mi ordenador se perdiesen o alterasen. A diferencia de un típico ordenador personal que hasta hace poco podía ejecutar un solo programa cada vez, los ordenadores Unix por lo general ejecutan simultáneamente docenas de programas, lo que significa que cambiando los datos

cualquier rastro podría borrarse con rapidez. Normalmente, yo podría fácilmente haber conectado con mis ordenadores por la red de Mark, pero como Andrew estaba a punto de clausurar el acceso exterior vía Internet, la única opción era utilizar un modem para conectar directamente a mi ordenador. Le pregunté a Mark si podía subir y ocupar el trastero, un pequeño cuarto en el que a un costado guarda ropa y al otro un PC de IBM y un modem de baja-velocidad a 2.400 baudios. Algunas personas conservan los trajes pasados de moda; Mark se niega a renunciar a una tecnología obsoleta si

todavía puede sacarle algún provecho. La seguridad del teléfono era aún un elemento que me inquietaba, pero decidí que la necesidad de actuar rápidamente superaba el posible riesgo.

Me senté en aquel apretado espacio y utilicé el modem para conectar con mis ordenadores en San Diego. Desde el PC de Mark podía controlar los ordenadores de mi pequeña red, tanto en el SDSC como los que tengo en mi casa a varias millas del *campus*. Estuve un rato ojeando por encima las interminables hileras de directorios de archivos para ver si había algo obviamente irregular. A primera vista

todo parecía normal, de modo que era improbable que se tratase meramente de la travesura de un gracioso. Tal como revelaba la alteración de nuestros archivos de registros, alguien estaba intentando cubrir sus huellas.

Procedía con pies de plomo, como lo haría cualquier detective, con cuidado de no estropear algún dato que más tarde me permitiese reconstruir cómo había ocurrido la violación. Hasta algo tan sencillo como leer un archivo puede eliminar para siempre las huellas digitales de un intruso. Vi por los directorios y los registros de administración del sistema que Andrew

estaba también conectado a mi red, efectuando el mismo tipo de examen que yo, pero con menos cuidado. Había estado dando palos de ciego, abriendo archivos para inspeccionarlos y destruyendo valiosas pruebas cada vez. Eso me fastidió, y le envié un mensaje diciéndole con brusquedad que no alterase nada. Pero él había pasado casi una hora husmeándolo todo y ya se había perdido información. Los esfuerzos de Andrew, sin embargo, habían conducido a un descubrimiento particularmente importante: algunos de los paquetes de archivos de registros que contienen información del tráfico de datos de

nuestra red habían sido abiertos recientemente y luego copiados con destino desconocido en alguna otra parte de la Red. Esto quería decir que quien quiera que fuese que había irrumpido en mis máquinas podía ahora disponer de información perteneciente a otros usuarios de las mismas, incluyendo sus contraseñas. Tomé nota mentalmente para examinar más tarde aquellos archivos de tráfico de datos y efectuar un control de daños. También interesante, aunque frustrante, fue el descubrimiento por parte de Andrew de que el actual registro de tráfico de la red estaba invalidado y no nos servía.

Teníamos ante nosotros una serie de informaciones pero ninguna que aparentase formar un cuadro completo. Una posibilidad era mirar las copias de los registros de antes de que fueran borrados y comprobar a quién correspondían los registros desaparecidos. De ello podríamos inferir quién estaba tratando de cubrir sus huellas. Vimos que alrededor de las diez de la noche anterior había habido una frenética actividad de sondeos aleatorios desde un punto de red llamado *csn.org*, que correspondía a Colorado SuperNet, un proveedor de servicios de Internet desde el que

previamente había descubierto intentos de forzamiento. Pero ninguno de los intentos de la noche anterior efectuados desde *csn.org* parecía haber tenido éxito. Comprobamos que aproximadamente a la misma hora había habido intentos de conectar a partir de dos localizaciones con nombres que sonaban a guasa: *wiretap.spies.com* y *suspects.com*[6]. Era la clase de broma que hubiera esperado si alguien estuviese intentando tomarme el pelo, aunque tales pistas no nos acercaban en lo más mínimo a entender qué había ocurrido en realidad. Vimos asimismo que por alguna razón uno de mis

ordenadores, que procesaba comunicación de programa en la red, se había puesto en marcha la noche anterior. Era algo sospechoso, pero podía no significar nada en absoluto.

Indagué un poco más a fondo, sondeando muy suavemente por debajo de la superficie. Los directorios de archivos que un operador ve están en realidad construidos a partir de otros que el ordenador conserva a un nivel mucho más profundo. Examinando estos menudos detalles al nivel más básico de la estructura de archivos de mi ordenador, yo esperaba detectar algún indicio de los cambios que hasta el más

astuto intruso podría no haber pensado en borrar.

En Ariel, el ordenador que en el SDSC me sirve como pasarela de acceso a Internet, descubrí que el intruso había dejado algunos rastros. Una buena parte de los datos ni siquiera estaba en inglés, sino más bien en las representaciones binarias que los ordenadores usan para comunicarse internamente, y de allí pude discernir unos esquemas de información todavía almacenados en el disco de mi ordenador que revelaban el espectro de un archivo que había sido creado y luego borrado. Encontrarlo fue un poco

como cuando se examina la hoja de arriba de un bloc: aunque la anterior haya sido arrancada, la impresión de lo escrito en la hoja que falta es discernible en la que queda. Al archivo que había estado allí momentáneamente y luego había sido copiado con destino a algún punto remoto y borrado después le habían llamado *oki.tar.Z*.

Era una pista mínima, pero que apuntaba en muchas direcciones posibles. ¿Qué significaba? Oki era, por supuesto, la marca del teléfono móvil en el que yo había trabajado con Mark Lottor; era el código fuente de Oki —las instrucciones originales del

programador— tras el que habían andado quienes atacaron a Mark el otoño anterior. “Tar” es un programa de utilidad de Unix que archiva y recupera archivos hacia y desde un archivo único llamado *tarfile*. Tradicionalmente se da ese nombre a una colección de archivos en una cinta magnética, pero puede ser cualquier archivo. Alguien podía haber reunido unos programas de software escritos por mí para controlar un teléfono móvil Oki, e intercalado después un único archivo con el nombre d e *oki.tar*. La “Z” indicaba que probablemente lo habían condensado empleando otro programa de utilidad

para “comprimir”, con el fin de que llevase menos tiempo transferirlos a algún lugar distante.

El hecho de que alguien hubiera acumulado apresuradamente un montón de archivos bajo el nombre de *oki* señalaba un motivo posible para el ataque a mis ordenadores: alguien estaba muy interesado en el funcionamiento interno de los teléfonos móviles. La sombra espectral de *oki.tar.Z* me proporcionó asimismo un conjunto de indicadores direccionales para determinar cuáles de mis archivos habían sido robados. Y como para poder copiarlos había sido necesario acceder

a cada uno de los archivos que fueron amontonados en *oki.tar.Z*, y como el momento del acceso había sido debidamente anotado por el ordenador, yo contaba con una descripción bastante detallada de la visita de mi ladrón.

Al otro extremo del país, Andrew tenía una sola línea telefónica, de modo que desconectó y utilizamos el correo vocal mientras yo continuaba examinando mi red desde el ordenador del trastero de Mark.

Le dije que el próximo paso era llamar a la gente de operaciones en el SDSC y hacer que parasen a Ariel, el ordenador que conecta mi red con el

mundo exterior y que está alojado en un armario de cableado junto a mi despacho. Parar un ordenador es muy distinto a apagarlo o volver a arrancarlo, operaciones que eliminan todos los datos que no hayan sido de antemano salvados y guardados en el disco duro. Un comando de parar, por el contrario, congelará el funcionamiento del ordenador dejando hasta el último byte de información exactamente en el estado que estaba cuando la máquina se detuvo. Este paso sería crucial para el análisis inquisitivo que yo ahora sabía que iba a tener que realizar, y que implicaba asimismo regresar a San

Diego. Hasta que descubriésemos exactamente cómo había sido atacada mi red, no podía volver a conectarme. Iba a tener que examinar mis sistemas con el software equivalente a una lupa, o incluso un microscopio. Y el tiempo no corría a mi favor. Lo que hacía falta en realidad era analizar unas huellas dejadas en la arena; visibles mientras no sean cubiertas por otras que recorran la misma senda.

Poco después de las nueve se presentaron mis amigos y finalmente, después de las nueve y media, Mark me apartó del trastero del ordenador. Fuimos todos juntos a The Good Earth,

un local de una cadena de restaurantes macrobióticos, en el centro de Palo Alto. Para la ayuda que mi presencia hizo a la reunión, lo mismo hubiera valido que no me hubiesen esperado. Durante parte de la cena estuve hablando con Andrew por mi teléfono móvil, tratando de organizar las cosas para que pudiésemos encontrarnos lo antes posible en San Diego. Él ya había llamado a Jay Dombrowski, responsable de comunicaciones en el SDSC, y lo había convencido de que teníamos un problema grave. Dombrowski aceptó que el Centro se hiciera cargo del coste del pasaje aéreo para que Andrew

regresase inmediatamente a San Diego.

Había pocos signos alentadores. Parando rápidamente a Ariel existía una posibilidad de que pudiésemos reconstruir parte de lo que había ocurrido, pero se había borrado información de archivo de registro, y en nuestro breve examen no habíamos podido descubrir nada que hubiera sido obviamente hecho de modo subrepticio, lo cual en muchos casos de incursión en una red es una señal reveladora.

Poco antes de las once Mark y yo nos despedimos de nuestros amigos y nos encaminamos a su casa en Menlo

Park. Yo seguía inquieto, tratando de que se me ocurriese un plan para volar de regreso a San Diego y evaluar rápidamente el asalto. Ya en casa de Mark volví a conectar con mis ordenadores y descubrí que Andrew había estado hurgando en la red después de salir yo a cenar. Me percaté de que había hecho cosas que probablemente habían borrado preciosos datos para la investigación y volví a llamarlo, para decirle que me fastidiaba que hubiera actuado de esa forma. Colgué, y me di cuenta de que para reconstruir la irrupción una vez llegado a San Diego iba a necesitar un hardware que no tenía.

Le pedí a Mark que llamase a su amiga Lile Elam, pues unas semanas antes yo había dejado guardados en su despacho de Sun Microsystems unos manipuladores y otros materiales. Hace varios años que trabajo como asesor para Sun, y Lile trabajaba allí como ayudante técnica, pero la empresa estaba cerrada por las fiestas navideñas. Yo quería saber si estaría dispuesta a reunirse con nosotros en Sun para entrar a recoger mi material.

Lile tuvo al principio dudas sobre entrar en las oficinas tan tarde por la noche, pero la convencí para que se reuniese con nosotros en el recinto de la

compañía en Mountain View, frente al edificio en el que ella trabajaba. Le hice notar que yo conocía a todo el personal importante en Sun y le prometí que si alguien preguntaba yo asumiría toda la responsabilidad. Diez minutos más tarde, cuando llegamos ante el edificio 18, Lile nos estaba esperando.

Había un problema. Aparcada justo delante de la puerta había una furgoneta blanca de vigilancia de la compañía. Eso quería decir que aunque el edificio estaba cerrado, probablemente un guardia privado de seguridad estaría recorriendo el interior; y que éste podría no aceptar de buen grado que alguien

saliese con un montón de disqueteras en medio de la noche. Y todavía peor, si bien Lile y yo teníamos el distintivo de la Sun, Mark no, y el guardia podría preguntarse qué estaba haciendo con nosotros una persona ajena a la compañía.

Sopesamos la posibilidad de aguardar a que se fuese, pero ninguno de nosotros estuvo dispuesto a pasar la noche ante el edificio. Con nuestro distintivo puesto, emprendimos la marcha por el vestíbulo hacia el despacho de Lile. Y como era de esperar, cuando habíamos recorrido dos tercios del trayecto tropezamos con el

guardia. Resultó que habíamos exagerado nuestros temores. El hombre admitió la presencia de Lile y mía, pero objetó la de Mark. Le explicamos que era un amigo de ella, y con eso pareció conformarse.

Un poco con la sensación de haber cruzado un puesto fronterizo, los tres continuamos por el vestíbulo hacia el despacho de Lile, donde recogimos mis disqueteras y unas tarjetas de interfaz en bolsas antiestáticas. Desde la ventana del despacho veíamos la furgoneta de la seguridad, y un par de minutos más tarde el guarda abandonó el edificio, montó en ella y se alejó. Regresamos

apresuradamente por el vestíbulo, con temor de llamar la atención al ir con las manos llenas de hardware. Una vez fuera pasamos por delante de la videocámara, nos metimos en los coches y partimos.

Cuando regresamos al apartamento de Mark a eso de la una y media hice mi reserva para el vuelo de las siete por Reno Air con salida de San José. Tendría que estar de pie a las seis para llegar al aeropuerto con tiempo para entregar mi Probe en Budget. Mark me deseó suerte y se fue arriba a dormir, mientras yo me tendía en el sofá del salón para pescar unas pocas horas de

sueño. Antes de caer dormido tuve un último pensamiento: “Este año, el esquí tendría que esperar”.

3. Evaluación de daños

Los Ángeles ha ido gradualmente transformándose en su propia imagen en la película futurista *Blade Runner*: una tecnópolis brumosa y anárquica.

No es que San Diego, donde yo vivo, sea una prístina ciudad de la California meridional, pero tiene una calidad de vida que nunca me parece encontrar en Los Ángeles. Cada vez que regreso a casa en un *jet* comercial que baja de golpe sobre el distrito financiero

antes de aterrizar mirando al océano, me parece una isla. Circundada por el desierto, la ciudad suscita una tangible sensación de futuro que surge de la combinación de los severos ángulos de la aséptica arquitectura del siglo XXI, las exuberantes palmeras, el verde brillante de los parterres y el océano. No escasea la arquitectura extraña, que va de los abruptos edificios modernistas en el *campus* de la Universidad de California, donde yo trabajo, al surrealista templo mormón sobre la I-5, diseñado para evocar alguna mítica iglesia del Renacimiento europeo.

A mi salida de San José había

habido largas colas y un caos masivo que me recordó por qué no suelo viajar tras un puente de tres días. Al día siguiente a la Navidad el aeropuerto era una burbujeante masa de gente presa de un compartido afán por llegar a su casa. A eso de las ocho y media de la mañana del lunes, con apenas cuatro horas de sueño, me dirigí al exterior del aeropuerto. Iba cargado con treinta kilos de equipo recogido la noche anterior, incluido el prototipo del RDI PowerLite. Me sentía frustrado por hallarme en San Diego en lugar de estar regresando al lago Tahoe a esquiar. El vuelo de Andrew llegaría un poco más

tarde, así que me arrimé al bordillo y cogí un taxi para realizar el viaje de treinta dólares que me llevaría directamente al Centro y a mi despacho.

Describirlo como despacho es en realidad una concesión graciosa. Lo que tengo es un pequeño cuarto sin ventanas al lado de un gabinete de cableado aún más pequeño. Está abarrotado de diversos monitores de ordenador, hardware variado, como disqueteras y otros recambios, y una caja fuerte del Gobierno que me quedó de mi época de funcionario de laboratorio federal y que lleva la inscripción PROPIEDAD DEL LABORATORIO NACIONAL DE LOS

ÁLAMOS. Como viajo tan a menudo, no es frecuente que trabaje en el despacho, pero lo utilizo como zona de almacenamiento. Siempre hay muchísimos libros y al menos un montón de correo sin abrir que mi secretaria ha puesto en alguna parte. Hay asimismo varios monitores de ordenador conectados por un manojo de cables de vídeo a Ariel, la vieja estación Sun Microsystems que está metida en el gabinete de cableado. Éste alberga asimismo algunos modem y otros varios ordenadores, incluyendo uno que funciona como distribuidor de comunicaciones, un controlador de

tráfico para todos los datos de Internet que me llegan.

Varios años antes yo había preparado a Ariel de modo que el background[7] de su terminal de vídeo mostrase permanentemente la imagen de satélite meteorológico más reciente enviada por Internet desde la Universidad de Illinois en Champaign-Urbana.

Mis ordenadores llevan nombres de ángeles caídos de *El paraíso perdido* de Milton. Al contrario que Jerry Pournelle, el articulista de la revista *Byte* que parece querer instilar vida a sus ordenadores domésticos llamándoles

“Ezequiel” y nombres por el estilo en su columna mensual, yo no tengo la menor intención de antropomorfizar las máquinas con las que trabajo. Para mí los ordenadores son básicamente objetos. Lo que yo por mi parte he buscado son nombres que estuvieran obviamente relacionados, pero de una forma que a un observador casual no le resultara enseguida evidente. Si se hace bien, resulta de buen gusto. Tenía que ser además un conjunto numeroso, porque siempre que aparece un nuevo ordenador necesito darle un nombre. Los ángeles caídos de Milton se revelaron como una fuente idónea, porque yo

quería algo que brindase muchas posibilidades de elección y también que fuera aceptado por los censores de nombres de la red.

Antes de decidirnos por los ángeles, Sid y yo habíamos tenido una charla sobre el problema de los nombres, en la que él me había dicho: "No quiero hacer de censor, pero tampoco hace falta que usted sea ofensivo". En el mundo de la red de ordenadores hay algunas personas que parecen creer que tengo una "pose". Puede que así sea, pero aquel era el modo que Sid tenía de intentar persuadirme de no suscitar innecesarios choques con la política de

pensamiento de la red.

Yo prefiero por norma trabajar con los ordenadores más rápidos disponibles en cada momento, pero tengo una especie de debilidad sentimental por Ariel, que vino conmigo de Los Álamos. La existencia de Ariel se inició como Sun-3. La Sun empezó a producir los Sun-3 en 1985, lo cual en términos de generaciones de ordenadores lo convierte en una antigualla. La tendencia es que nuevas generaciones de microprocesadores aparezcan a intervalos de dieciocho meses. Retroceder seis generaciones en tecnología de ordenadores sería

equivalente a volver a la era del caballo y la calesa.

Ariel tiene una curiosa historia. Hace tiempo, con Brosl Hasslacher, un físico de Los Álamos que ha sido mi mentor a lo largo de los años, acudimos a la Sun a discutir sobre unos problemas que teníamos con un ordenador mucho más caro y poderoso. Un ejecutivo de la Sun salió al muelle de carga y nos encontró a Ariel como una especie de premio de consolación. Desde entonces, Ariel se ha convertido en un vagabundo, habiendo vuelto en un momento dado a Caltech, donde fue utilizado por un estudiante que había trabajado conmigo

como interno, antes de venir a parar finalmente a mi gabinete de cableado. Actualmente lo empleo básicamente para el correo, para almacenar material de menor importancia y como una bifurcación o salto que me dé acceso a Internet.

Tan pronto como entré en mi despacho abandoné mis maletas. Eché una ojeada a uno de los monitores del ordenador que había sido congelado la noche anterior por un operador del Centro. En la visualización de la ventana de la consola, la que da información sobre el estado del sistema, había un mensaje de error proveniente del

XNeWS interpreter, el programa que controla la visualización de información en la pantalla del ordenador:

```
   process(0x480088,
'teal.csn.org  NeWS  client',
runnable)
   Error: /syntaxerror
   Command: '.psparse_token'
```

Intenté brevemente interpretar el mensaje pero no descubrí ninguna evidente vulnerabilidad. Puse a Ariel de nuevo en funcionamiento el tiempo suficiente para inspeccionar los registros estadísticos conservados en el modem que conecta los ordenadores de mi casa con el Centro. Lo que vi

demostraba que los datos extraídos de mi red personal no habían sido muchos. El registro del modem mostraba que había estado conectado cinco días, y que durante ese tiempo habían circulado aproximadamente cuatro megabytes de datos en cada dirección. No era sino el tráfico de rutina en casa y el hecho de que fuera equilibrado en ambas direcciones indicaba que nadie había sustraído datos de mis máquinas. Fue un alivio: el blanco principal había estado en otra parte, probablemente entre los ordenadores del vecino gabinete de cableado.

Llamé a Sid Karim, el director, para

informarle. Se mostró en general comprensivo sobre mi problema, pero no estaba dispuesto a otorgarme un cheque en blanco para resolverlo. Me dijo que si mi descripción de la situación era razonablemente correcta, podría proporcionarme algún dinero para ayudar con el control de daños. Traducido cortésmente, me estaba advirtiendo que más valía que tuviera razón en mis sospechas. Tampoco aceptó pagarme los habituales honorarios de consultor, diciéndome: "Tsutomu, en rigor usted está de vacaciones".

Me dije que aquello era cuanto

podía esperar dadas las circunstancias, y salí a coger el Acura que había dejado en el aparcamiento del Centro mientras estaba de viaje para irme a casa.

Los ordenadores que tengo en el SDSC y en casa están conectados por una línea de modem de alta velocidad que está siempre abierta. Había resuelto ir primero a examinar las cosas en casa, porque allí es donde guardo los datos y los programas que realmente me importan.

Mi casa está a unos diez minutos de coche desde el Centro, en una de esas comunidades de viviendas relativamente nuevas que salpican el paisaje del sur de

California. La ruta diaria me lleva a pasar por delante de la Scripps Clinic y por lo que llaman el San Diego's Biotech Row[8]. Así como la Universidad de Stanford sirvió de incubadora a Silicon Valley, Scripps ha nutrido a una generación de biólogos convertidos en empresarios. Mi barrio fue construido en su mayor parte en los setenta y mi casa es una vivienda adosada que encaja perfectamente entre sus vecinas. No es mi idea del mejor estilo arquitectónico, pero está cerca del *campus* y me brinda la sensación de estar fuera de la ciudad. Veo y huelo el océano, y arriba, desde la ventana de mi

dormitorio, oigo por la noche las olas que rompen en la playa. Veo también el parque estatal de Torrey Pines, al que acudo cuando me hace falta un sitio donde estar a solas y pensar. La playa está aislada de los ordenadores y fuera del alcance del teléfono móvil, y a veces voy allí con un simple bloc de notas, cuando necesito concentrarme.

Tras aparcar en el garaje entré en mi casa y la encontré fresca y silenciosa. Para el gusto de la mayoría de la gente, el mío es un hogar espartano. Aunque tiene tres dormitorios y un estudio, el mobiliario es escaso: futones, sillas y mesas desperdigadas por ahí. Yo

duermo arriba en el dormitorio principal y uso los otros dormitorios como cuarto de equipos y zona de preparación para aventuras y expediciones diversas. En los últimos años he dedicado tiempo a realizar largos viajes con la mochila al hombro, he recorrido el Círculo Ártico y he seguido un eclipse en Baja California.

La ausencia de muebles se debe a la abundancia de ordenadores. En un momento dado podría tener en casa hasta doce máquinas conectadas a Internet, que pueden enchufarse en el momento, dependiendo de lo que ocurra. Muchas de las máquinas están apiladas

en uno de los armarios y algunas ni siquiera tienen monitor, son simplemente unas cajas con procesador, memoria y discos. Tengo allí algunos PowerLite; una SPARCstation Voyager, que fue un decepcionante experimento de la Sun para introducirse en el mercado del ordenador portátil; Osiris, una estación de trabajo sin disco que se halla en la cabecera de mi cama y que utilizo con frecuencia como ventana hacia Internet; un par de servidores, Rimmon y Astarte, ordenadores rápidos de Sun con grandes discos buenos para almacenar datos y números críticos; otro router; un servidor de terminal; un ordenador de

demostración con muro de fuego… y la lista continúa.

Mientras que la mayoría de las actuales oficinas modernas conectan sus ordenadores con una tecnología llamada Ethernet, que fue desarrollada en el legendario Centro de Investigación de Palo Alto de la Xerox Corporation en los años setenta, los de mi casa están unidos por cables de fibra óptica empleando una tecnología llamada ATM, o Modalidad de Transferencia Asincrona. Una red ATM organiza la información de forma distinta a la de Ethernet. Los datos son divididos en "células" en lugar de en "paquetes". Las

células son por lo general más pequeñas que los paquetes, y todas ellas del mismo tamaño. Esto significa que ATM está mejor diseñada para enviar vídeo y audio. Además, en una red ATM la velocidad máxima de enlace de la red está siempre garantizada; no hay que preocuparse de compartirla con el vecino de al lado. Muchas personas en las industrias informática y de telecomunicaciones creen que ATM va a ser la ola del futuro. No tiene, como otras redes, una única velocidad definida, y es escalable, o sea que puede irse volviendo más rápida con el avance de la tecnología. Mi equipo es ya quince

veces más rápido que Ethernet: lo bastante para transmitir imágenes de vídeo sorprendentemente claras, mucho mejores que cualesquiera que puedan verse en los televisores actuales. Las empresas telefónicas y cablegráficas ya se están preparando para reemplazar sus redes analógicas de cable de cobre por redes de fibra óptica ATM. Sus partidarios confían en que para fin de siglo las redes de datos ATM serán tan fácilmente accesibles en los hogares como las tomas de teléfono y los enchufes en la actualidad. Eso es lo que se prevé, al menos. Yo he estado realizando calladamente experimentos

con delicados aspectos básicos de ingeniería que han de ser resueltos antes de que nada de esto se convierta en una realidad de consumo.

Lo que me fascina es el poder inherente a las redes de ordenadores de alta velocidad y lo que se puede hacer con ellos, en contraste con las posibilidades de un solo ordenador aislado. Sun tiene un eslogan propagandístico: "La red es el ordenador". Más allá del truco publicitario hay ahí un inmanente fondo de verdad que está implícito en la reciente onda de interés popular en Internet. Los ordenadores individuales

no tienen ya mucho interés; es en el ordenador en común que está emergiendo de la red donde se esconde el futuro. En consecuencia, yo tengo por todos lados cables de color naranja, blanco y beis. Algunos de ellos atraviesan las paredes y otros están a la vista. Esos cables transportan datos informáticos en forma de diminutos destellos de luz. Imaginen ustedes un rayo de luz que se enciende y apaga cientos de millones de veces por segundo. (Como experimento, puede encender una linterna a un extremo de un rollo de fibra óptica. Al mirar el otro extremo verá nítidamente un punto de luz

semejante a una estrella). Una cosa es indudable: los cables de fibra óptica resisten mucho mejor que los cables normales de cobre el quedar apretados por una puerta.

Muerto de cansancio me detuve un momento a la entrada de mi casa, contento de volver al hogar pero frustrado por no estar en las montañas. A continuación desconecté la alarma y subí a mi dormitorio con intención de dormitar un rato mientras esperaba la llegada de Andrew. Era una brillante mañana de sol, y desde mi cuarto veía, más allá de los tejados, Torrey Pines y el océano. La habitación estaba en

silencio. No había ruido de ventiladores ni rumor de disqueteras. Aunque hay allí tres ordenadores, tengo la convicción de que los seres humanos y las partes móviles de los ordenadores no congenian.

Aparentemente, nada había cambiado, pero había algo raro. Sentado en mi cama ante Osiris con las piernas cruzadas toqué la trackball o bola de seguimiento y el Screensaver o salvapantallas dio paso a un campo de ventanas. Inmediatamente noté que el gran rectángulo situado del lado izquierdo de la pantalla de Osiris y que usualmente está conectado sea con el

mundo exterior o con Ariel en el Centro, estaba completamente vacío. Totalmente en blanco. No mostraba señales de vida, nada del texto que debía haber estado mostrado incluso si el ordenador con el que estaba conectado estuviera parado.

Pensé para mí, esto es extraño, porque aun cuando Ariel estuviese congelado allá en el SDSC, la pantalla de Osiris debería registrar su presencia. Me levanté de la cama y volví a mirar a Osiris y a pensar otro poco. No registraba nada. Lo paré. Fui y detuve su ordenador modal, Astarte. Luego congelé sistemáticamente mis demás ordenadores. Todo mi mundo

informático quedó en suspenso, como repentinamente congelado.

Retorné a la planta baja y al mirar en la nevera me di cuenta de que no había mucha comida en casa. No es nada sorprendente, porque me lo paso viajando. Estuve rebuscando y encontré unas tabletas energéticas Power Bars, con las que por el momento tendría que conformarme.

Regresé al dormitorio para tratar nuevamente de analizar la irrupción. Mi primer paso sería hacerme con algunos instrumentos de investigación para examinar las huellas del intruso. Encendí mi nuevo RDI y empecé a

montar una pequeña caja de herramientas con programas capaces de recoger y analizar datos. Lo que quería saber era qué archivos habían sido leídos, modificados o creados. Es sencillo precisar el tiempo en que ocurren cosas en un ordenador, porque el sistema operativo registra rutinariamente la hora de cualquier cambio en un archivo. Con esa información se podría componer una cronología de las actividades del intruso. Pero como también es posible alterar sistemáticamente esa información, yo sabía que era importante no darle un crédito absoluto.

Tenía ahora un montón de ordenadores congelados en los cuales las huellas del intruso estaban ocultas en forma de electrónicas cifras 1 y 0. Mi plan era quitar los discos e insertarlos en un nuevo ordenador para efectuar el análisis, pues haciendo los discos "sólo de lectura" sería posible evitar cualquier peligro de emborronar accidentalmente los datos mientras los exploraba. Me quedé mirando el ordenador portátil, que era un prototipo y podría no funcionar. Las máquinas recién salidas de fábrica tienden a tener fallos que pueden resultar irritantes. Puede que tuviera suerte. Si funcionaba,

yo podría determinar qué archivos había tocado el intruso y cuándo. Entonces posiblemente podría también descubrir de qué forma había forzado su entrada en mis ordenadores.

Poco antes de mediodía llamé a Andrew, que había llegado a San Diego varias horas después que yo, yendo después a su casa a dejar sus cosas. Él había realizado un vuelo desde Tennessee aun antes de que yo lo hiciera desde San José, y ambos nos sentíamos bastante cansados. Acordamos reunimos a cenar esa noche para perfilar un plan de acción. La última vez que hablé con Andrew había sido a las dos y media de

la mañana, poco antes de acostarme. Él no había dormido nada la noche anterior, pero dijo que había conseguido descansar un poco durante el vuelo. Finalmente, al anochecer me tendí en la cama y me quedé dormido, sólo para despertar más tarde todavía medio amodorrado, pero convencido de que los próximos días iban a ser intensos y de que dar una cabezada aunque fuese un rato era ventajoso.

La imagen espectral de *oki.tar.Z* no me abandonaba. ¿Qué significado tenía? Hacía unos años yo había ayudado a Mark Lottor desmontando el software incluido en la estructura del teléfono

móvil Oki. Generalmente, los programas que controlan un teléfono móvil están metidos en un chip ROM en el interior del mismo. Pero la mayoría de los teléfonos posee un interfaz no especificado con el mundo exterior, que posibilita su control remoto desde un ordenador. Nosotros examinamos cuidadosamente el software y retrocedimos paso a paso desde los 1 y los 0 insertos en el chip hasta las instrucciones generadas por los creadores del software. Este procedimiento es todavía objeto de controversia, pero las últimas resoluciones judiciales han sostenido en

general que se trata de una actividad legítima. Mark quería poder controlar el teléfono Oki para desarrollar un instrumento de diagnóstico de campo destinado a las empresas de telefonía móvil y a las agencias estatales de control.

Puesto que no contamos con la ayuda de la Oki para descubrir cómo controlar sus teléfonos, tuvimos que desmontar el software para ver cómo funcionaba. Lo que encontramos fue una cantidad de elementos no especificados de cuya existencia los usuarios no tienen la menor idea. Un teléfono móvil es en realidad poco más que una radio con un

diminuto ordenador personal, de modo que cuando examinamos minuciosamente el software del Oki no nos sorprendió que hubiera sido escrito por unos hackers verdaderamente capaces.

Con comandos que se pueden insertar en el teclado de un teléfono Oki es posible obtener toda clase de datos de diagnóstico sobre cómo se está comportando —por ejemplo, la intensidad de su señal—, que son sumamente útiles para los técnicos. Muchas otras marcas de teléfonos móviles funcionan tan bien como el Oki como escáner telefónico móvil. Pocas personas están al tanto de que

conociendo qué teclas pulsar en el teclado de su teléfono móvil pueden escuchar fácilmente todas las conversaciones telefónicas que estén ocurriendo en la vecindad; truco que, desde luego, constituye una violación de la Ley de la Intimidad de las Comunicaciones Electrónicas. Pero puesto que la intimidad no existe en absoluto en el actual sistema telefónico móvil, la escucha clandestina de las llamadas se ha convertido en un pasatiempo generalizado.

En 1992 testifiqué ante una audiencia parlamentaria convocada por el diputado Edward Markey acerca de la

existencia de esa capacidad no especificada del teléfono móvil. Una vez que el presidente de la comisión me hubo garantizado una inmunidad especial, cogí un teléfono móvil AT&T nuevo y sin usar —en realidad el mismo teléfono Oki, todavía en su envase termorretráctil, pero con la etiqueta de la AT&T y vendido por ésta—, lo armé y presioné una serie de teclas. Inmediatamente el Comité pudo escuchar conversaciones por teléfono móvil provenientes de todas partes de la colina del Capitolio.

Después, un agente del FBI, robusto y de mediana edad, vino y me dijo:

“Ahora mismo está usted bajo inmunidad parlamentaria, pero que yo no le pesque haciendo esto fuera de este recinto”. Su observación confirmó una cosa que he notado trabajando con el FBI: estos tíos no tienen ningún sentido del humor.

Oki.tar.Z no sólo sugería un motivo para el forzamiento que habíamos sufrido, sino que también insinuaba quién podía haberla perpetrado. Unos meses antes, en octubre y noviembre, alguien había intentado repetidamente forzar su entrada en los ordenadores de Mark Lottor, en un esfuerzo por robar el mismo software del Oki móvil que había

sido sustraído de Ariel.

Mark estaba en vías de establecer un nuevo negocio casero. Internet estaba en auge, y él había descubierto que existía un mercado dispuesto a publicar páginas en una World Wide Web en rápida expansión. Por consiguiente, Network Wizards estaba creando *catalog.com*, un emplazamiento de red gratuito que permitiese a la gente exponer información de catálogo o lo que fuese que quisiera comunicar. La Red, desarrollada originalmente como herramienta de investigación científica por un programador de ordenadores en el CERN, el centro de investigación en

física en Ginebra, Suiza, había surgido casi de la mañana a la noche como vehículo adecuado para permitir el comercio electrónico en Internet.

Además de su servidor de archivos Network Wizards, la red Ethernet de la casa de Mark servía de soporte a otros dos ordenadores. Lile, la amiga de Mark, había creado Art on the Net, una galería artística virtual alojada en una estación de trabajo Sun cedida para posibilitar a una nueva generación de artistas digitales la exhibición de sus obras. Otra Sun en su red había sido donada como emplazamiento de red a la League for Programming Freedom, una

organización de hackers dedicada a la cruzada de Richard Stallman para crear un mundo de software libre, compartido.

Desde principios de octubre Lile había estado notando un comportamiento extraño del registro de correo electrónico con el proveedor comercial de servicio en Internet, Netcom. Intentaba hacer que su correo fuera enviado a *art.net* de Sun desde Netcom, sólo para encontrar poco después que el archivo enviado había desaparecido. Se quejó a Netcom, pero el encargado del soporte telefónico le dijo que no podía ser un problema de seguridad, pues, según le explicó, "no hemos tenido una

irrupción en tres semanas".

Un sábado por la mañana a mediados de octubre, Mark se despertó y bajó a prepararse un café. Fue hasta el ordenador a leer el correo y estaba sentado cerca del servidor de archivos cuando sin motivo aparente éste empezó a producir un prolongado sonido *grrrrrrrr*.

"Qué raro", pensó. Se suponía que el ordenador, ligado a Internet por una conexión de alta velocidad T-1, estaba desactivado. Cuando lo conectó a la máquina vio que lo que estaba apareciendo era un largo listado de todos sus archivos. Siguió mirando y

comprendió que alguien estaba controlando su ordenador.

Su primer pensamiento fue que tal vez aquello fuese consecuencia de algún programa inusual con el que no estuviera familiarizado. Los ordenadores Unix tienen montones de pequeños programas llamados *demonios* que funcionan constantemente en un segundo plano ejecutando tareas domésticas. Después puso un programa llamado netstat, que proporciona información detallada sobre lo que está ocurriendo en una conexión de red local de ordenadores. Comprobó que alguien estaba conectado a su máquina desde el *art.net* Sun de

Lile.

Pero Lile estaba sentada al otro lado de la habitación frente a su propio ordenador.

"¿Estás teleconectando con mi ordenador?", preguntó Mark, refiriéndose a una rutina que se utiliza para conectar con un ordenador distante a través de la Red. Pues no.

La alarma de Mark pasó a convertirse en pánico cuando vio que la persona introducida en su máquina empezaba a aglutinar un montón de archivos. Segundos después, el pirata se puso a utilizar el ftp —protocolo de transferencia de archivos—, una rutina

común en Internet para transferencia de archivos, para mover los archivos aglutinados hacia Netcom.

Mark se horrorizó. "¿Y ahora qué hago?", le dijo a Lile, que se había unido a él observando incrédula mientras el voluminoso archivo acumulado era copiado desde su ordenador. Miró a su alrededor y se dio cuenta de que la defensa más rápida era quitarse de la Red. Corrió y arrancó de la pared el cable de datos T-1.

Más tarde, ese día, tuvimos una charla por teléfono. Después de arrancar la clavija del ordenador, Mark había examinado el archivo unificado y había

comprobado definitivamente que alguien estaba intentando conseguir el software del teléfono Oki que nosotros habíamos modificado para el sistema de diagnóstico de su teléfono móvil. Pudo determinar que no habían logrado obtener nada de verdadero valor, sino sólo un pequeño trozo del archivo. Me recomendó estar alerta, y no pasó mucho tiempo antes de que Andrew y yo viésemos algunos intentos contra nuestros ordenadores, que él repelió fácilmente.

Al día siguiente Lile y Mark se dirigieron por la autopista 17 a Santa Cruz a visitar una sauna próxima al

campus de la Universidad de California en la localidad. Mientras atravesaban las montañas, sonó el teléfono de Mark.

Él atendió, y una voz dijo "Hola". Mark reconoció inmediatamente al que llamaba como alguien a quien conocía sólo superficialmente pero que mantenía vínculos con el mundillo informático.

"Yo no he dejado mi número de teléfono ni doy el de mi móvil", dijo Mark. "¿Cómo lo ha conseguido?".

"Digamos que di con él sin saber cómo", respondió el que llamaba. "Sólo quería decirle que sé quién irrumpió en su ordenador ayer. Fueron Mitnick y sus amigos, y les dio realmente mucha rabia

no haber conseguido lo que querían".

El nombre de Kevin Mitnick le sonaba a Mark, lo mismo que a cualquiera que siguiese la historia del clandestino submundo informático. Mitnick se había criado en el valle de San Fernando, en la Baja California, durante los años setenta, y había efectuado la transición del mundo de los chalados que se entrometen en el sistema telefónico al de los piratas informáticos que utilizan las redes para forzar los ordenadores. Aparentemente, había una importante diferencia entre Kevin Mitnick y los miles de adolescentes que parecían estar imitando a Matthew

Broderick en la película *Juegos de guerra*. Mitnick se mostraba notoriamente incorregible. Con apenas treinta y un años, ya había sido detenido cinco veces a partir de 1980, cuanto sólo tenía diecisiete. Estaba habitualmente huyendo de diversos cuerpos policiales, incluido el FBI.

John Markoff, un articulista del *New York Times* especializado en tecnología a quien Mark y yo conocíamos bien, había sido coautor de un libro sobre el delito informático titulado *Cyberpunk*, en el que figuraba Kevin Mitnick. También había escrito un artículo sobre Mitnick en julio de 1994, en el que

decía que éste llevaba más de un año eludiendo a los agentes estatales y federales. El artículo añadía que Mitnick era sospechoso de haber robado software de las redes informáticas de no menos de media docena de empresas de telefonía móvil.

Mark recordó que varias semanas antes, la mañana del sábado en que atacaron su ordenador, alguien a quien conocía como amigo de Mitnick había llamado diciendo que quería comprar el software de teléfono móvil de Network Wizards, pero que quería también el código fuente, las instrucciones originales del programador con las que

se podrían modificar ulteriormente las funciones del aparato. Aunque Mark se negó a vender la fuente, el amigo de Mitnick había permanecido más de una hora al teléfono tratando de engatusarlo.

No hubo más ataques durante el fin de semana, pero en el curso de las siguientes dos semanas el intruso continuó dando constantemente la lata, irrumpiendo reiteradamente en la máquina *art.net* de Lile y en el ordenador de la League for Programming Freedom, dejando Caballos de Troya y puertas traseras.

De tanto en tanto enganchaba a Lile en sesiones de charla, utilizando un

comando llamado talk que permite a dos usuarios de un sistema Unix teclearse mensajes de ida y vuelta en tiempo real por Internet.

"¿Por qué no me cede el software de una vez?", leyó ella un día en la pantalla. "De todos modos, lo voy a conseguir".

Le pidió asimismo una cuenta en su sistema, afirmando de nuevo que de todos modos iba a conseguir uno. Lile le ofreció uno de sus estudios virtuales de artistas digitales, pero a él no le interesó. Dijo que si ella le daba una cuenta, él le revelaría quién era realmente.

“Espero que no esté enfadada conmigo”, tecleó.

Mark estaba sentado en la habitación en ese momento y la asesoraba sobre cómo responder. Intentaron hacer que el otro soltase fragmentos de información sobre sí mismo, pero con escaso éxito.

Finalmente, en diciembre, el invasor llamó por teléfono directamente a Mark para intentar convencerlo de cederle el software.

“¿Sabes quién soy?” dijo. “Quiero tu código”. Y a continuación le preguntó si estaba enfadado por las irrupciones en su servidor de archivos.

Mark respondió que no, y le explicó

que él tenía una filosofía diferente acerca de la seguridad informática: si alguien conseguía introducirse en su sistema, eso lo alertaba sobre la necesidad de reforzar sus defensas.

"Entonces continuaré intentándolo", dijo el otro. Mark le preguntó por qué estaba tan obsesionado por conseguir el código fuente del teléfono móvil Oki. El de la voz anónima respondió que quería ser invisible en la red de telefonía móvil y que creía que el poder modificar el comportamiento de su teléfono lo haría inmune al rastreo y a los artefactos de vigilancia.

Hablaron tres veces. Las dos

primeras llamadas telefónicas fueron breves, pero la tercera se extendió por más de cuarenta y cinco minutos, y durante la misma el otro preguntó: "¿No estarás grabando esto, verdad?".

Mark dijo que no, pero luego decidió que sería una buena idea. Se desplazó en silencio hasta el otro lado de la habitación y le dio a la tecla de grabación de su contestador.

El individuo sabía quién era yo, así como que había ayudado a Mark en el proyecto del teléfono móvil. Parecía estar sondeando para obtener más información sobre mí:

X: Cielos, así que tú

realmente, ejem, así que él escribió ese programa, comprendo…

Mark: Ajá.

X: ¿Por qué? ¿Lo hizo para ti, o simplemente se le ocurrió escribir un programa 8051 de desmontaje?

Mark: Hmm… No recuerdo precisamente por qué lo escribió. Una noche le salió y ya está.

X: Joder, ¿una sola noche? Eso es impos…

Mark: Ja, en realidad creo que sólo le llevó unas dos horas.

X: ¡Imposible!

Mark: (suspiro) (risas)

X: ¿Hablas en serio?.

Mark: Ajá.

X: Ese tío es un mago. Debería trabajar para tu empresa, Network Wizards[9].

Mark: Hmm… él tiene mejores cosas que hacer.

X: Todavía en San Diego, supongo…

Mark: Hmm, a veces.

X: Y en Los Álamos…

Mark: A veces.

Después de colgar, Mark llamó a Markoff y le puso la cinta para ver si reconocía la voz. El periodista nunca había conocido formalmente a Mitnick, pero había oído varias veces su voz por teléfono o en cintas. Dijo que ésta le

sonaba a la voz de él, pero no estaba seguro.

Seguidamente Mark llamó a Jonathan Littman, un escritor independiente de Marin County que estaba escribiendo un libro sobre el inframundo informático y de quien se rumoreaba que tenía clandestinamente acceso a Mitnick. Le hizo escuchar la cinta y le preguntó: "¿Reconoce esa voz?".

Littman rompió a reír. "Claro que sí. Es Mitnick".

La posibilidad de que Mitnick fuera el culpable del asalto contra mí y contra Mark resultaba intrigante, pero era una

idea que ahora no conducía a ninguna parte, de modo que la aparté de mi mente. En el inframundo informático y en todas partes mucha gente estaba enterada de que yo había trabajado con Mark en software de teléfono móvil. En este momento lo que necesitaba hacer era recoger datos y encontrar cuanto antes la forma de proteger nuestros ordenadores. Empleando las herramientas de software que había reunido, me puse a escanear la primera de las disqueteras extraídas de los ordenadores que habían sido congelados. Quería descubrir todos los archivos que hubieran sido leídos,

aquellos en los que se hubiese escrito, los que tuvieran la fecha cambiada o los archivos nuevos que hubiesen sido creados a partir del 21 de diciembre, fecha en la que yo había salido de San Diego. Estuve largo tiempo sentado ante el PowerLite. Estaba seguro de que en alguna parte de aquel cenegal de datos iba a encontrar una pista o un conjunto de pistas. Nadie puede ocultar su presencia a la perfección.

Estaba explorando asimismo en busca de programas Caballo de Troya. Se trata de programas que los intrusos electrónicos a menudo se dejan atrás. Pueden activarse y efectuar en silencio

cualquier cantidad de cosas secretas o destructivas. Disfrazados de software conocido podrían estar escritos para espiar, destruir datos o proporcionar una adecuada puerta trasera para eludir la seguridad. Una forma de proteger los ordenadores contra este tipo de intromisiones es tomar una instantánea digital de todos los programas que hay en el mismo: programas de sistema operativo, rutinas, herramientas de comunicación, todo. Comparando después matemáticamente las firmas generadas de los archivos del disco sospechoso con las de la copia original conservada a salvo, se puede saber si

algún archivo ha sido alterado.

Esa noche a eso de las nueve Andrew y yo nos reunimos para cenar en un lugar próximo al *campus* llamado Pizza Nova. Andrew es un ejemplo del oriundo de la costa Este que se ha adaptado notablemente bien al ambiente playero de California. Con el cabello rubio hasta los hombros, la nariz prominente y los ojos intensamente azules, su vestimenta habitual consiste en pantalón corto, camiseta y sandalias. Andrew es asimismo muy conocido por el hecho de que en realidad no le gusta llevar zapatos de ninguna clase, rasgo que a veces puede causar problemas

cuando vamos a comer a un restaurante. Tiene la capacidad del hacker para concentrarse en un problema complejo durante un extenso periodo, ayudado a veces por varios litros de Mountain Dew. En ocasiones me disgusto con él porque se precipita a sacar conclusiones y actúa con demasiada rapidez en lugar de pensar exhaustivamente las consecuencias de una acción determinada. Pero posee una buena captación intuitiva de la estructura íntima de Internet y trabajamos bien en equipo; y es un placer trabajar con él.

Durante la cena hablamos sobre las cosas que había que explorar.

Convinimos en que por el momento era necesario concentrarse en prestar verdadera atención a todas las posibles vulnerabilidades de mi red. Una cosa que nos intrigaba a ambos era que el intruso había estado manipulando el XNeWS, un componente del sistema operativo basado en PostScript que permite dibujar imágenes en la estación de trabajo propia o en un ordenador distante. PostScript se utiliza más ampliamente como lenguaje de impresora que proporciona al programador un conjunto de comandos para decirle a la impresora dónde trazar líneas, ubicar caracteres impresos y

sombrear zonas. ¿Podía haber sido aquella una vulnerabilidad? Tal vez los intrusos hubieran descubierto en PostScript un error de diseño que les permitiese utilizarlo para hacerse a distancia con el control de un ordenador. Le di a Andrew un conjunto de tareas y yo me asigné otras. Nos separamos con el acuerdo de volver a reunimos al día siguiente en el Centro de Superordenadores.

Me fui a casa sintiéndome emocionalmente agotado y aún más exhausto; de hecho, las cosas marchaban mal. Teníamos un mortificante conjunto de indicios acerca de cómo habían sido

atacados mis sistemas. Pero no existía seguridad alguna de que fuésemos capaces de interpretarlos, y aun cuando pudiéramos reconstruir el delito, no había ninguna probabilidad de que fuésemos capaces de rastrear en Internet si nuestros agresores habían realmente cubierto bien sus huellas. Eso me carcomía, y me forzaba a pensar en cosas que me habían estado preocupando y que iban mucho más allá de esta irrupción en particular.

Cuando llegué a casa llamó Julia. Estaba en Toad Hall, y los dos lo habíamos estado pasando mal.

“Aquí estoy y me siento

empantanado", le dije. Hablamos un rato del ataque, y después de lo que ella había estado haciendo en San Francisco.

"Tras el regreso de John, las cosas marcharon bien al principio", dijo ella, "pero ahora están mucho más tensas".

Estaba claro que la relación entre ellos no había funcionado desde que yo conocí a Julia, y no parecía que nada estuviera cambiando. En nuestro primer viaje juntos al desierto, tres años atrás, habíamos ido a acampar en la nieve en el Desierto Desolado próximo al lago Tahoe, y ella me había contado sus malos presentimientos sobre su relación con John. No era feliz y se preguntaba en

voz alta si debía o no permanecer con él e intentar que aquello funcionase. Hablamos hasta muy avanzada la noche y me dijo que pensaba que debía continuar intentándolo, por un sentido de lealtad hacia su compañero.

Ahora, tres años después, yo podía afirmar que Julia sabía que la relación era perjudicial para ella, pero parecía incapaz de romperla. Yo sabía que hacía algún tiempo que ella había venía intentando ponerle fin, pero las cosas familiares la reconfortaban y le resultaba difícil separarse de ellas. Todo aquello la hacía infeliz y la deprimía. No era la primera vez que la

veía sentirse de aquel modo —un año antes había estado en Nepal con John— pero él se fue y ella se lió con otro, un americano que conoció durante el viaje. La relación continuó seis meses más, pero terminó porque ella no quiso abandonar a John.

Era como si hubiera dos Julias. Una era la mujer fuerte, independiente y aventurera que intentaba encontrar lo que la hiciera feliz y satisfecha. Pero existía también otra persona, trabada por el miedo y por los sentimientos de inadaptación e inseguridad. Yo la había visto volverse paulatinamente más fuerte y más independiente desde que nos

conocimos, y más capaz de entender mejor qué era lo que le hacía daño, pero no había podido decidirse a una ruptura definitiva con John.

Seguimos hablando de mis problemas en San Diego. Yo estaba contrariado por el hecho de estar allí, en vez de esquiando, y cuanto más consideraba el problema más evidente se me hacía que no iba a ser sencillo y que podría estar perdiendo el tiempo en una investigación inútil para descubrir cómo había ocurrido la irrupción.

Durante los últimos meses me había sentido cansado ya del asunto de la NSA. Estaba harto de ocuparme del

tema de la seguridad informática y ansiaba irme a esquiar y trabajar en otros problemas. Pero ahora, como le dije a Julia, me sentía atrapado. Estaba forzado a ocuparme de seguridad informática, pero sin los recursos que me hacían falta.

"En este momento es lo último que me apetece, pero no puedo dejarlo", dije.

"Es horrible, Tsutomu. Estoy preocupada por ti", replicó ella. Propuso venir a hacerme compañía.

Pero le dije que no, que bastante tenía ella de que ocuparse para encima tener que venir a consolarme. Yo estaba

de pésimo humor y necesitaba concentrarme sin interrupciones para acabar lo antes posible con la amenaza.

"Duerme un poco esta noche", dijo ella por último. "Mañana, entre Andrew y tú conseguiréis hacer progresos".

No parecía haber ninguna otra opción. Nos dimos las buenas noches, comprometidos a volver a hablar pronto.

En el momento en que me iba a dormir recordé que desde que había vuelto a San Diego había olvidado escuchar mi buzón de voz. Repasé la retahila de mensajes que me habían dejado en el despacho del SDSC. Escuché cuatro o cinco mensajes de

rutina, pulsando continuamente la tecla del teléfono para eliminarlos de la memoria del sistema.

Entonces oí algo que me hizo incorporar en la cama.

"Enviado el 27 de diciembre a las 4.33 P.M.", dijo la estirada y femenina voz electrónica.

Otra voz la siguió inmediatamente. Sonaba como alguien que intentase fingir un pasable acento australiano vulgar. El mensaje era inconfundible.

"Maldita sea", dijo el que llamaba. "Mi técnica es la mejor. Mi patrón es el mejor, maldita sea. Me sé la técnica rdist, la técnica sendmail, y mi estilo es

muy superior”.

Rdist y sendmail son dos variedades corrientes de ataque a redes de ordenadores, relacionados con vulnerabilidades del sistema informático sumamente conocidas Aquél no podía ser otro que mi atacante, que me llamaba para insultarme.

“Maldita sea, ¿no sabes quién soy?”, continuó. “Yo y los amigos te vamo’a machacar”.

A continuación dio la impresión de girar la cabeza para apartar la boca del auricular y parecer que el que hablaba era otro: “Eh, jefe, su Kung Fu es realmente bueno”.

“Así es”, concluyó mi interlocutor con el mismo acento australiano. “Mi estilo es el mejor”.

Esta vez no borré el mensaje. Después me tendí en la cama, mirando al techo. Aquello estaba asumiendo un tinte personal, y era evidente que quienquiera que fuese se había vuelto bastante insolente. “Esto no me hace gracia”, pensé. Si antes no había estado claro, ahora sí. Era evidente que alguien me estaba desafiando.

4. El mundo real

Con frecuencia llamamos complejas a aquellas cosas de este mundo que no entendemos, pero a menudo eso sólo significa que todavía no hemos descubierto la forma adecuada de pensar en ellas.

Durante toda mi vida como científico me he dedicado a explorar y comprender lo complejo, y he descubierto que aunque pudiera parecer que a la naturaleza se le ha ocurrido

hacer funcionar las cosas de una forma complicada, en cualquier fenómeno subyace casi siempre una explicación muy elegante y sencilla.

Esta perspectiva básica ha estado presente en gran parte de mi trabajo en campos tan diversos como la biología y la física, y los problemas relativos a la informática, en los que me he centrado durante más de una década en el Centro de Superordenadores de San Diego. ¿Cómo ordena el mundo físico sus respuestas? Esta puede parecer una pregunta tremendamente vaga, pero se encuentra en el meollo de un abordaje radical a buena parte de la ciencia

moderna. Por ejemplo, ¿qué formas existen de localizar una fuga en un cubo? Ante esto, un ordenador no tendría ningún método simple de dar con el punto preciso. Podría por un proceso iterativo recorrer punto por punto toda la superficie del cubo hasta dar con el agujero. Pero hay una solución mejor y más sencilla: llenar el cubo y dejar al agua la tarea de localizar la fuga.

Era la reflexión sobre esas cuestiones relativas a la naturaleza de la informática lo que centraba el interés del legendario físico Richard Feynman hacia el final de su vida. Yo empecé a tomar clases con Feynman sobre la

física de ordenadores cuando me inicié en Caltech como estudiante de primer curso en 1982, y pasé otro tiempo con él durante el verano de 1984 en Thinking Machines, una empresa de superordenadores que empezaba a funcionar en Cambridge, Massachusetts. Su perspectiva influyó enormemente en mi propio modo de pensar. Feynman poseía una notable capacidad para ver el mundo claramente y no ser confundido por los preconceptos en boga. Durante toda mi carrera he buscado emular el enfoque de Feynman ante la ciencia, y creo que también me ha ayudado a lograr esa perspectiva independiente el

hecho de ser un científico y el haberme criado entre dos culturas.

Yo nací el 23 de octubre de 1964 en Nagoya, Japón. Mis padres se criaron en Japón, donde vivían durante la guerra. Mi padre, Osamu, se formó como bioquímico y mi madre, Akemi, empezó a trabajar como farmacéutica. Emprendieron juntos como socios su carrera en investigación, especializándose en el estudio de la bioluminiscencia. En los años sesenta, la principal institución en la materia era la Universidad de Princeton. Fue un periodo estupendo para realizar investigación en los Estados Unidos, y

mis padres se vinieron cuando a él le ofrecieron allí un cargo como investigador residente en la facultad. Mi madre se apartó un tiempo de su propia carrera para criarnos a mí y a Sachi, mi hermana menor.

Aunque conservo tempranos recuerdos de viajes de ida y vuelta entre Estados Unidos y Japón, los primeros tiempos que puedo recordar con claridad son los años de mi niñez en Princeton. Recuerdo especialmente mi aprendizaje del inglés como segunda lengua en el parvulario y en primer grado.

El haber sido criado por dos

científicos moldeó para siempre mi forma de ver el mundo. Mi niñez se desarrolló entre la cocina de mi madre y el laboratorio de mi padre. Desde que di los primeros pasos mi familia estimuló en mí la curiosidad. Me instaban a hacer preguntas, ante las cuales nunca recibía como respuesta un "porque". La respuesta de mis padres solía ser una sugerencia para que realizase un experimento que me permitiese obtenerla por mí mismo.

El valor de la experimentación me era enseñado incluso en las circunstancias más corrientes. Una vez, cenando, se me cayó una seta al suelo, y

cuando fui a recogerla para comérmela, mi padre dijo "Está sucia".

"Yo no veo ninguna suciedad", repliqué.

El resultado de esa discusión fue que mi padre me condujo a su laboratorio para que pudiésemos examinar más atentamente la seta bajo el microscopio.

Yo era, en general, un chico discutidor, aunque mis padres me toleraban considerablemente. Era tan rápido para rebatir, incluso en mi época de escolar, que un día mi madre, exasperada, levantó ambos brazos y dijo "¿Tú que vas a ser de mayor: científico… o *abogado*?".

En los años sesenta y setenta Princeton era la comunidad académica liberal por excelencia, pero yo era todavía alguien de afuera, a pesar de que la universidad tenía una amplia población asiática. Durante este periodo retorné con frecuencia a Japón, e incluso viví allí casi dos años, lo suficiente para asegurarme de conservar la sensación de estar levemente al margen de ambas culturas. Pasé mi quinto año completo de colegio en Nagasaki. En Japón se enseñan tanto el japonés como el inglés, y fue interesante llegar a conocer la visión japonesa de América tras haberla experimentado yo personalmente.

Debido a que la investigación de mi padre implicaba estudiar medusas bioluminiscentes, pasé muchos de mis veranos en Friday Harbor, en las islas de San Juan, del estado de Washington, donde él dirigía la investigación de campo en el laboratorio de biología marina de la universidad. Yo estaba en mi elemento, en libertad con montones de otros niños aburridos de familias académicas. Aquellos veranos me brindaban tiempo libre para ayudar en el laboratorio de mi padre intentando encontrar algo útil que hacer cuando no estaba metiéndome en líos y vagando por la soledad de la isla. El clima

fresco, las alfombras de pinos Douglas y los cristalinos charcos dejados por la marea eran un maravilloso contrapunto al más civilizado, caluroso y húmedo verano de Princeton.

Cuando tenía doce años —habiendo adelantado varios cursos ya estaba en primero de secundaria— empecé a estar cada vez menos tiempo en casa. No me llevaba especialmente bien con mis padres y acabé pasando la mayor parte del tiempo en la universidad.

En esa época un amigo mío tenía un empleo con un profesor de psicología en un laboratorio que estaba haciendo

investigación neuropsicológica, y él me ayudó a conseguir un trabajo allí también a mí. Él estaba intentando poner en marcha un sistema de adquisición de datos. Era básicamente una tarea de programación en la que intervenía un ordenador DEC PDP-11/34, que era entonces el elemento estándar en todo equipo informático de laboratorio.

La primera vez que vi un ordenador fue en el parvulario. El padre de uno de mis compañeros de clase, que trabajaba en los Laboratorios Sarnoff de la RCA, trajo uno al colegio para una especie de sesión de "dime-qué-es-esto", y aunque yo no llegué a jugar con él, fue sin lugar

a dudas algo que recordaba y que me intrigó. Recuerdo claramente que incluso en aquel primer encuentro, consideré a aquellas máquinas como instrumentos que me ayudarían a resolver problemas.

Pero mi primer contacto real con la informática no empezó hasta que tuve diez años, cuando, a través de amigos, tropecé con un peculiar e informal club informático de Princeton conocido como los Resistors[10]. Resistors era un acrónimo de "Radically Emphatic Students Interested in Science Technology and Other Research Studies"[11], y lo formaba un grupo

anárquico de adolescentes (la edad media era probablemente los 15 años) que se reunía en el E-Quad, el edificio de cuatro plantas de la facultad de Ingeniería de Princeton. La primera generación de Resistors estaba influida por gente como Ted Nelson, el visionario científico social que escribió el libro *Computer Lib/Dream Machines* y que había de convertirse en el flautista de Hamelín del hipertexto. Yo fui en realidad miembro de la segunda generación, y lo que el grupo me proporcionó fue una entrada fácil en el mundo de la informática: entre otras cosas, mi ordenador personal propio en

la era de los miniordenadores y los grandes ordenadores. Pero por lo demás yo era mas bien un tanto solitario por naturaleza, y nunca llegué a tener un vínculo realmente estrecho con los otros Resistors.

El grupo fue en realidad resultado del mismo impulso que motivaría la aparición de un club de aficionados semejante conocido por Homebrew Computer Club, que emergió varios años más tarde en Silicon Valley. Aunque sus miembros eran mayores, la mayoría apenas veinteañeros, fueron también producto de la disponibilidad de los primeros chips baratos para

microprocesador, y su pasión por poseer el ordenador propio llevó directamente a la explosión de la era del ordenador personal. Gentes como Steve Wozniak y Steve Jobs crearon Apple Computer al calor de la cultura tecnológica que surgió en torno al *campus* de Stanford en la segunda mitad de los setenta. Otros miembros del Homebrew, como Lee Felsenstein, acabaron diseñando tanto la máquina Sol como la Osborne 1.

Los Resistors crecieron bajo el influjo de una edad informática anterior, con un distintivo sabor a la costa Este. El mundo de los grandes ordenadores había surgido durante los años cincuenta

y sesenta en IBM, seguido por la era del miniordenador de los setenta creado por compañías como DEC, Data General y Prime. El miniordenador fue la apoyatura de la época de la informática de tiempo compartido. Producto de la cultura del hacker del MIT, los sistemas operativos de tiempo compartido permitieron que más de una persona utilizara el ordenador al mismo tiempo. El truco fue cortar en diminutos trozos iguales las tareas informáticas y luego hacer que la unidad central de proceso del ordenador saltase de uno a otro sucesivamente. Con eso los ordenadores se hicieron enormemente más

productivos y expandieron el poder de la informática a una audiencia muchísimo más amplia. Fue asimismo el tiempo compartido lo que permitió a los jóvenes hackers como yo lograr el acceso a ordenadores poderosos.

La particular contribución de la AT&T a la revolución informática había sido el sistema operativo Unix, un programa desarrollado en los años sesenta por dos científicos informáticos de los Laboratorios Bell, Dennis Ritchie y Ken Thompson. Los sistemas operativos son una combinación de agente de tráfico, secretaria y criado dentro de un ordenador. Son los

programas que ejecutan todas las operaciones básicas de manejo y responden a los requerimientos y órdenes del usuario además de orquestar el delicado ballet que se desarrolla entre todos los distintos componentes de un sistema informático. Los sistemas operativos proporcionan asimismo al ordenador una personalidad distintiva. Cabe considerarlos como un lenguaje para hablar directamente con el hardware del ordenador.

Ritchie y Thompson, que habían quedado atónitos ante un proyecto de desarrollo de sistema operativo llamado Multics, financiado por el Pentágono,

crearon Unix como alternativa, y éste pronto se convirtió rápidamente en la herramienta de programación predilecta para el anárquico ejército de hackers que estaban conformando una cultura informática en diversas universidades y empresas por todo el país. Como miles de estudiantes de facultad de la época, yo crecí como hijo de la revolución Unix.

A diferencia del mundo del ordenador personal, en el que los sistemas operativos como el CP/M, el MS-DOS y el Apple DOS fueron elaborados a partir de cero, el Unix fue un sistema que se creó desmontando

muchos de los elementos del mundo de los grandes ordenadores y se adaptó a la capacidad de los miniordenadores y las estaciones de trabajo. Como resultado, mi generación de hackers esperaba que los ordenadores tuviesen ciertas características de las que los ordenadores personales carecían y de las que en algunos casos, más de una década después, todavía carecen. Conceptos informáticos de Unix tales como multitarea, administración de memoria de hardware, y ser portátiles, formaron parte de un evangelio que aprendí mientras me instruía en la programación Unix entre los diez y los

quince años. Era de sentido común que los ordenadores fueran capaces de hacer múltiples cosas al mismo tiempo, incluso para un usuario solo, y empleasen la administración de memoria de hardware, que asegura que un programa pobremente diseñado no abandone el espacio de memoria que le ha sido reservado y pisotee otros programas.

Crecí también sin pensar que hubiera algún modo de utilizar los ordenadores que no fuesen conectados entre sí para formar redes. Primero entré en contacto con la ARPAnet, la predecesora de la Internet financiada por el Pentágono, en

1976. Era una comunidad abierta, aunque muy pequeña —la red entera no debe haber sumado más de un centenar de ordenadores— y a mí me encantaba explorarla.

Lo que no hacía era pasar las tardes y noches forzando mi entrada en otros ordenadores, una moda que los adolescentes adoptaron casi una década más tarde. Cuando yo viajaba por la Red a mediados de los años setenta casi no había cerraduras y todo se compartía. En varios lugares alrededor del *campus* de Princeton había terminales públicos que te permitían sentarte y acceder a toda la Red. Yo probaba juegos, charlaba con

gente, y me paseaba por sitios como el MIT, Carnegie Mellon y Stanford.

Aunque mi primer lenguaje de programación fue el BASIC, creado en 1969 en Darmouth con fines educativos, pronto me di cuenta de que podía escapar de los estrechos limites de un lenguaje hacia el shell de comando de Unix. El shell —básicamente el panel de control del software del ordenador— amplió mi horizonte y me dio acceso a todos los recursos del ordenador, así como al mundo de redes que había más allá. Después de estar confinado al mundo rigurosamente controlado de Basic, el shell de Unix fue un poco como

estar en el puente de mando de la nave espacial *Enterprise*. Disfrutando mi nueva libertad, aprendí a programar en C, un lenguaje que había sido desarrollado por el mismo equipo de hackers de los Laboratorios Bell que había inventado el Unix. El C fue para mí liberador. Como lenguaje resulta complicado, pero una vez dominado es notablemente poderoso y flexible. Con C adquirí una habilidad que me hizo objeto de una gran demanda, aún en mi adolescencia.

Un graduado en ciencias informáticas llamado Peter Honeyman me ofreció mi primera cuenta Unix en

Princeton, en el ordenador DEC del departamento de ingeniería eléctrica y ciencia informática. Aunque me fue retirada después, cuando el ordenador se sobrecargó de estudiantes regulares, fue mi punto de entrada original en un mundo que pronto se convertiría en mi pasión. El PDP-11/45 era una máquina excéntrica, y Honeyman fue evidentemente lo bastante listo para advertir que otro alumno de secundaria llamado Paul Rubin y yo éramos una fuente virgen de trabajo barato. Pronto nos convertimos en administradores y cuidadores del ordenador.

En ocasiones tuve problemas por el

uso del ordenador. Recuerdo que descubrí que podía emitir un mandato para mover el brazo principal de la unidad de disco magnética de nuestro miniordenador del colegio hacia atrás y hacia adelante con rapidez. La disquetera era un monstruo IBM estándar de 14" que parecía un frisbee[12], cuya cabeza para leer v escribir datos magnéticos estaba controlada por un stepper[13] y a la cual se le podía ordenar entrar y salir y leer y escribir en cualquiera de los 203 cilindros de la unidad. Una vez que conseguí desplazarla al cilindro 0, y luego al cilindro 100, empecé a

preguntarme “Vaya, ¿qué pasaría si intentase desplazarlo al cilindro HEX FFF?”. Eso sería el equivalente al cilindro 4095… desgraciadamente, uno que no existía.

Di la orden y oí, *Rrrrr, Crunch*. Aquel fue el fin de la unidad. Fue una lección útil, y para mí puso efectivamente en cuarentena uno de los cánones de la informática que siempre se enseñan: “No te preocupes, el hardware no se rompe”.

Según iba pasando cada vez más tiempo del día alrededor de la universidad, la secundaria iba progresivamente convirtiéndose en algo

subordinado en mi vida. A un extremo del espectro me fascinaba la física porque exploraba los principios fundamentales que subyacen en todo lo que forma el universo; y en el otro extremo, la biología, en la que unos principios muy sencillos crean sistemas muy complejos. En un caso uno puede intentar simplificar, mientras que en el otro no hay ninguna posibilidad de hacerlo. Estudiaba, sí, otros campos, como psicología y geología, pero no espoleaban mi interés, porque eran más parecidos a la botánica, que para mí era el arte de establecer categorías y no requería análisis ni inteligencia.

Si bien esa incursión en las disciplinas académicas me resultó beneficiosa, fueron mis habilidades informáticas las que me hicieron parte integral de la escena universitaria. En 1978 Princeton se enfrentaba al creciente problema de la proliferación de miniordenadores. El centro informático de la facultad había tratado anteriormente de mantener el monopolio de toda la informática académica. Al efecto, le había dicho a los diversos departamentos: "Dado que nosotros proporcionamos este servicio, queremos que uséis nuestros ordenadores". Y como todo el que tiene un monopolio,

cobraba precios escandalosos. Pero los otros departamentos de Princeton descubrieron el medio de librarse de tener que depender del centro informático: la aplicación específica. Todos los diversos departamentos se las ingeniaron para adquirir su propio miniordenador individual y ejecutar complicados proyectos especiales inventados por ellos.

El departamento de astronomía había conseguido hacerse con un DEC PDP-11/60 y quería instalar Unix, pero en el personal no había nadie que supiera algo sobre él. Como yo ya andaba rondando gran parte del tiempo, mendigando,

tomando prestado o robando tiempo libre del ordenador, me pidieron que fuera a instalar un cierto hardware especializado con el que poder leer una determinada cinta magnética de datos.

Gracias a aquel proyecto me convertí en el *gurú* informático del departamento, a los catorce años de edad. Después de haber escrito para ellos un manual para usuarios que hacía que el ordenador le hablara de forma clara a unas esotéricas unidades de disco, un joven profesor ayudante, Ed Turner, me invitó a trabajar a tiempo parcial. En esa época, la tradición en el departamento era que la informática

estuviese a cargo del miembro más nuevo de la facultad. Ed no sólo me dio un empleo, sino que me introdujo en un mundo sorprendente, sacándome de mi claustrofóbica existencia de estudiante secundario.

Visto retrospectivamente, el acceso a aquel empleo fue uno de esos sucesos cruciales que me ayudaron a definir, a una edad muy temprana, quién era yo. Fue asimismo una increíble fuente de diversión, y me dio acceso a algunos de los mejores juguetes del mundo.

El resto del tiempo que pasé en secundaria estuve constantemente rondando el departamento de

astronomía, principalmente colaborando en el trabajo de procesamiento de imágenes computerizadas. Amén de aprender algo sobre igualación de esquemas y un montón sobre programación de sistemas, el cargo contribuyó a moldear de forma duradera mi actitud hacia la informática. Tratar de resolver problemas en astrofísica y astronomía me convenció de que, si una máquina no hace lo que uno quiere, hay que reprogramarla para que lo haga. Aprendí tempranamente que una máquina hace precisamente lo que se le dice que haga y nada más.

Mis responsabilidades aumentaron

hasta incluir el diseño de hardware específico para el departamento de astronomía, y en mi año de secundaria avanzada pude desarrollar un sistema de almacenamiento de datos para captar información experimental de un lanzamiento de misil financiado por la NASA en el que participaba el departamento. Mi tarea fue la de ayudar a diseñar el hardware que recogiera los bytes de información del vuelo en el White Sands Missile Range, en Nuevo México. El problema comprendía recuperar las imágenes desde las cámaras a bordo del misil, conservarlas en cinta de vídeo y luego tratar de

convertir los datos en cantidades digitales para ser almacenadas y analizadas por ordenador. El lanzamiento resultó un éxito, y proporcionó información de la franja ultravioleta del espectro en los confines del espacio.

El hecho de frecuentar una comunidad de estudiantes mayores y profesores a una edad tan temprana y el ser esencialmente precoz acabó también por causarme dificultades. Como me había saltado dos cursos, en el otoño de 1980 estaba en el último año de secundaria con quince años.

No obstante mi mediocre currículo, obtuve brillantes puntuaciones en las pruebas y fui aceptado en Carnegie Mellon a comienzos de mi último curso. Fue una decepción, no obstante, que mi otra opción, el MIT, me rechazase a pesar de que tenía recomendaciones de unos cuantos profesores tanto de Princeton como del propio MIT. A lo largo de los años de secundaria, mi actitud había sido que mientras estuviera haciendo algo que tuviese suficiente interés "intelectual", las notas no importaban.

Aburrido y con creciente resentimiento hacia lo que parecían

rituales académicos sin sentido, en ocasiones irritaba a mis profes. Una vez en una clase de Inglés nos dieron una lista de palabras que debíamos usar en ensayos escritos en el curso del semestre. Había que emplearlas en contextos adecuados, y por cada uso correcto se nos adjudicaría puntos para nuestra graduación final.

Pero a mí se me ocurrió que había una solución más sencilla, que puse en ejecución en forma de un único trabajo hecho en diez minutos. Escribí un cuento acerca de una estúpida clase de inglés en la que el profesor suministraba una lista de palabras e incluí al pie de la

letra las propuestas. Reclamé la puntuación por toda la lista, y resolví que, puesto que ahora disponía de suficientes puntos para pasar, no asistiría al curso durante el resto del periodo.

Esa clase de trucos no me hacía simpático ante los profesores.

Tampoco encajé en la secundaria con el típico empollón en informática o ciencias. Aunque no me atraían los equipos de alumnos, sí me encantaba practicar por mi cuenta toda clase de deportes. Me convertí en entusiasta ciclista, corriendo con un club local llamado el Century Road Club of

America. Me pagaba el equipo de ciclista, relativamente caro, armando de vez en cuando ruedas de bicicleta para una tienda local del ramo, Kopp's Cycles. Durante los inviernos empecé a desarrollar mi afición apasionada por el esquí de campo en la ondulada campiña de Nueva Jersey.

Durante el breve tiempo que realmente pasaba en el cole me reunía con un pequeño grupo de amigos, a uno de los cuales le llamábamos "el terrorista". Era en realidad un hábil pianista de música clásica, y aunque en ocasiones suspendía, la dirección no podía realmente tomar medidas más

severas con él porque lo necesitaba para tocar en los actos del colegio.

Era bastante famoso, y sus bromas eran siempre dramáticas: el hueco de la escalera cubierto de termita[14]; inodoros que aparecían en medio del campo de fútbol. Una vez el sistema de megafonía se quemó por entero porque él lo consideraba una herramienta de propaganda. Se convirtió literalmente en humo.

En el momento de la última de las bromas yo me encontraba a quinientos kilómetros de distancia, visitando el Carnegie Mellon para una entrevista, de modo que tenía una coartada perfecta.

Pero como se me consideraba un revoltoso, cuando entré de regreso al colegio, el director vino hacia mí y dijo: "¡Usted! ¡Ha sido usted!".

Después la dirección descubrió que el sistema de megafonía fue destruido aplicando una corriente alterna de 120 voltios a uno de los llamadores mediante un temporizador. Esto ocurrió sólo después de haber cambiado todas las conexiones en los tableros y haber hecho volar nuevamente todo el sistema, porque el temporizador estaba puesto para un ciclo de 24 horas.

El periódico del colegio estaba preparando un artículo sobre el

incidente, y nos enteramos de que estaba lleno de errores técnicos. Una tarde a última hora fuimos a la redacción, cogimos el artículo, lo revisamos y lo devolvimos a la bandeja del director del periódico. El artículo que salió resultó bastante preciso en el aspecto técnico, aunque nadie en el colegio se enteró de cómo lo había logrado.

"El terrorista" ingresó con el tiempo a Yale, pero durante la secundaria jamás consiguió ser considerado más que como un vándalo. Él, por su parte, consideraba sus actos como delitos políticos. Como alumno de secundaria tenía una formación ideológica

sumamente desarrollada. Todavía no estoy seguro de a qué parte del espectro político pertenecía cualquier otro de mi grupo. Probablemente, sería *antiestablishment*… el que fuese.

En cuanto a mí, no sé cuál fue la gota que colmó el vaso: si las calificaciones o la insubordinación. Pero una noche, durante mi año de secundaria superior, encontré al llegar a casa que mis padres habían recibido tres cartas del colegio. Dos de ellas eran de felicitación por haber ganado un concurso local de matemáticas y física; la otra era para comunicar que me habían expulsado de Princeton High School. Considerándome

como una causa perdida para el sistema educativo, el director me había dicho a comienzos de aquella semana: "No vuelva, es usted persona *non grata* Si le encontramos por aquí, lo haremos detener".

Mi respuesta fue: "¡Vale, vale, perfecto! Si no venía cuando era alumno, ¿qué les hace pensar que querría volver?".

Cuando me echaron del colegio, Carnegie Mellon rescindió su oferta. Dijeron que conservarían mi plaza para el siguiente curso académico, proporcionándome otra oportunidad de graduarme. Acabé en un concurso de

gritos con el funcionario de turno y diciéndole “No se molesten”.

Poco después, mis padres se incorporaron al laboratorio de biología marina en Woods Hole, donde mi padre había aceptado un cargo de investigador. Yo tenía aún mi puesto en el departamento de astronomía, y mis amigos seguían en Princeton, así que me encontré yendo y viniendo entre Nueva Jersey y Massachusetts.

A pesar de mi experiencia en la secundaria, yo siempre había tenido aspiraciones académicas centradas cada vez más en la física, de modo que me presenté a la Universidad de Chicago, a

la John Hopkins y a Caltech. Cuando inicié el proceso de solicitudes de ingreso tenía la impresión de que en Caltech te exigían demasiado, que era algo así como beber de una boca de incendios y, por tanto, no me había presentado. Pero yo había trabajado para Jim Gunn, un joven y brillante astrónomo de Princeton que había empezado como profesor de astrofísica en Caltech, y tras mi rechazo por parte de Carnegie Mellon, él y un par más del departamento continuaron empeñados en que yo cursase enseñanza superior y pensaron que Caltech podría irme muy bien.

Con mis calificaciones de examen y la recomendación de personas como Gunn fui admitido en Caltech para el otoño de 1982.

En el verano de 1982, con diecisiete años de edad, viajé a Baja California con intención de estudiar física y biología cuando comenzaran las clases, un mes después. Había estado antes en Caltech una cantidad de veces por mi trabajo en el departamento de astronomía de Princeton y alquilé una habitación en una casa situada justo frente al *campus*. En comparación con Princeton, este *campus* siempre me ha

parecido diminuto. Ubicado en Pasadena, apretado contra las montañas de San Gabriel, me resultaba claustrofóbico; en Los Ángeles había demasiada contaminación para andar en bicicleta, y como yo no tenía coche, carecía de un medio para escapar. Lo que no escapó a mi percepción fue que el lema bíblico del instituto, "Y conoceréis la verdad, y la verdad os liberará" (San Juan, 8:32) era el mismo utilizado por la Agencia Central de Inteligencia.

Para la entrevista sobre mi solicitud de ingreso la primavera anterior, un miembro del profesorado llamado Jerry

Pine me había visitado en mi despacho de Princeton. Pine, un físico en altas energías que había hecho la transición a la biología, me había sugerido que fuese a California antes del comienzo de las clases a trabajar en un proyecto dirigido por otro profesor de Caltech, Geoffrey Fox, físico, que conocía a través de Gunn y otros mi reputación como hacker. Fox se hallaba en las primeras etapas de diseñar una nueva clase de ordenador compatible conocido como hipercubo. Se trataba de una potente y novedosa arquitectura de ordenador acorde con la tendencia a fragmentar los problemas complejos en componentes menores y

tratarlos por ordenador de forma simultánea. La operación de ordenadores en paralelo, objetivo por entonces de investigadores y empresas en todo el país, habría de conducir más tarde a notables avances en la velocidad de los procesos y a la transformación de la industria de los superordenadores.

Cuando llegué al *campus*, el equipo de Fox acababa de poner en funcionamiento un prototipo de cuatro procesadores. Pero como nadie sabía cómo programar aquellas máquinas totalmente nuevas, mi primera tarea fue contribuir a averiguar cómo usarlas para resolver problemas que previamente

habían sido resueltos en forma secuencial. Mi misión era "ganar rapidez": tratar de encontrar formas inteligentes de conseguir más rendimiento para un problema particular, algo que yo había hecho muchas veces en Princeton. Una de las cosas que descubrimos enseguida fue que los ordenadores hipercubo eran ideales para informatizar un conjunto de problemas matemáticos conocidos como transformadas rápidas de Fourier, que se utilizan en el procesamiento de señales y tienen aplicaciones prácticas para todo, desde perseguir submarinos enemigos hasta reconocer el habla humana,

pasando por la compresión de datos.

Trabajé a tiempo completo con Fox durante el verano, pero cuando comenzaron los cursos mis intereses fueron en otras direcciones y rápidamente me aparté del proyecto. Un factor en mi alejamiento fue una oferta de empleo por parte del JPL, Laboratorio de Retropropulsión de la NASA, colina arriba desde Caltech. Los ingenieros del JPL me ofrecieron la oportunidad de trabajar en investigación en sistemas de comunicación, un área esotérica responsable de buena parte del trabajo implícito en la creación de puentes radiales con las sondas

espaciales enviadas a otros planetas, como Pioneer y Voyager. Algunos de los mejores expertos del mundo en comunicaciones estaban en el laboratorio en ese periodo y buscaban estudiantes partidarios de embarcarse en proyectos en los que no hubiera pautas fáciles que seguir. Mi experiencia con el Unix y en informática resultó ser un valor sumamente apreciado. El grupo del JPL estaba intentando desarrollar en una máquina Unix un sistema que les ayudase a diseñar un circuito integrado de galio y arsenio, y yo pronto me convertí oficialmente en el hacker y arreglalotodo de Unix.

En Caltech existe una larga tradición de manipulación inteligente del sistema por parte del hacker. Los criterios eran que toda actuación suya debía ser realizada con estilo; debía ser inteligente, divertida, y no una copia de algo ya hecho antes; y sobre todo, no debía ser destructiva o perjudicial.

Yo tomaba parte en las diabluras. Por ejemplo, había escalado algunos peñascos antes de venir a Caltech, y cuando llegué al instituto descubrí que el hecho de que el *campus* estuviese en medio de una ciudad no disuadía a los escaladores. Al escalar edificios se le llama "edificiar", y hasta hay una guía

para escaladores de la arquitectura de Caltech. Trepar a un edificio a las dos de la mañana era uno de nuestros deportes favoritos para eludir las tareas. Por supuesto, los encargados de la seguridad del *campus* odiaban que la gente trepara a sus edificios, de modo que durante mis años de estudiante allí hubo permanentemente una partida disputada entre los escaladores, que procuraban trepar sin ser descubiertos, y los guardias, que intentaban impedírselo.

Una noche, un amigo y yo resolvimos dar trabajo a los guardias de seguridad. Puesto que no había nada de

malo simplemente en andar por allí provistos de equipo para escalar, los dos nos colgamos al hombro cuerdas y demás elementos y nos pusimos a recorrer el *campus*, deteniéndonos ante las rutas de escalada más frecuentadas y de muchas de las improbables. Pronto reunimos un acompañamiento formado por un puñado de guardias que se detenían a vigilarnos a distancia con las radios funcionando y continuaron siguiéndonos durante toda nuestra gira por los puntos de acceso más importantes, hasta que, una hora más tarde, cada uno de nosotros giró y se fue a casa, en direcciones opuestas.

En el frente académico empecé el año escolar tratando de comportarme como un estudiante normal, con la esperanza de que la universidad sería distinta de la secundaria. Pero al cabo de unas semanas me di cuenta de que era en gran parte la misma experiencia y descubrí que me concentraba en lo que me resultaba de interés, sin hacer caso del hecho de que la universidad esperaba que yo superase los obstáculos de rigor a lo largo del curso.

Hubo dos clases, no obstante, que me tomé con verdadero entusiasmo. Una era un curso dictado por Ron Drever, un investigador en relatividad general muy

conocido por su trabajo con detectores de ondas gravitatorias. Los problemas en cuya solución se destaca implican la detección de efectos sumamente ínfimos en un ambiente en donde actúan desordenadamente fuerzas mayores y más potentes. La clase, compuesta en un 50 por ciento por principiantes y alumnos avanzados y el resto por estudiantes graduados, aparte de mí, estaba básicamente dedicada a cómo medir efectos gravitatorios increíblemente pequeños mediante una inteligente preparación de los experimentos. Buena parte del tiempo lo dedicábamos a repasar experimentos en

relatividad teórica, prestando atención tanto a los efectos que han sido postulados pero no medidos aún, como a las mediciones que han sido efectivamente llevadas a cabo.

Una cosa notable acerca del curso era que no tenía exámenes parciales, y la calificación final dependía de proyectar un experimento de laboratorio para medir uno de los efectos todavía sin medir predichos por la relatividad general. Yo expuse una idea para medir un fenómeno llamado inercia del marco gravitatorio utilizando de forma innovadora una herramienta llamada interferómetro láser. Todos entregamos

nuestros trabajos, y Drever comenzó una de sus últimas disertaciones anunciando: "Me siento muy defraudado con vosotros. Entre todos los trabajos encontré sólo una idea original, y fue de un principiante".

El otro curso que me produjo una enorme impresión fue uno para posgraduados dictado por Richard Feynman; Carver Mead, el padre del VLSI o diseño de Circuito Integrado a Muy Grande Escala; y John Hopfield, sobre la informática física. Hopfield, uno de los inventores de las redes neuronales, un modelo informático que remeda sistemas biológicos, fue uno de

mis consejeros, pero lo que me intrigó fue el interés de Feynman en las bases subyacentes de la informática. Feynman, uno de los principales físicos teóricos del mundo, no había dado clase en Caltech durante la primera cuarta parte de mi curso porque estaba sometido a un tratamiento contra el cáncer, pero al final de ese periodo yo me presenté y tímidamente le pregunté si podía asistir a su siguiente curso. Él me hizo un par de preguntas sobre mis antecedentes y luego me dijo que me convendría hacerlo. Acabé asistiendo al curso los dos años que pasé en Caltech.

El seminario se centraba en las

limitaciones de la informática —de quantum, de comunicaciones, de codificación, de termodinámica— y de ese modo sondeaba las últimas fronteras. Aunque yo había explorado las operaciones en paralelo incluso en la secundaria, a través de Feynman empecé a comprender que mientras los ordenadores modernos procesaban la información secuencialmente —una instrucción y un fragmento de información por vez—, la naturaleza lo hace en paralelo. Empecé asimismo a comprender que el procesamiento en serie realmente perjudica nuestro modo de pensar como científicos. Utilizar

ordenadores seriales para explorar un mundo en paralelo a menudo enmascara la sencillez real de la naturaleza.

Pasé el verano posterior a mi año de principiante de nuevo en Princeton, donde trabajé en el Instituto de Estudios Avanzados con Steven Wolfram, el físico que más tarde desarrolló el Mathematica, el programa actualmente más utilizado en colegios secundarios e institutos. Era suficiente como ocupación veraniega, pero Wolfram buscaba un codificador profesional que le ayudase a desarrollar productos de software, lo cual a mí no me interesaba. Yo escribo software, pero para resolver

mis propios problemas.

En el otoño, cuando regresé a Caltech, no tardé en descubrir que me estaba hastiando de la rutinaria tarea académica. Empecé a tomar más clases avanzadas y de posgrado, picoteando en todo con la esperanza de encontrar algo en lo que pudiese meterme de lleno. En el proceso, empero, me agoté rápidamente. Sencillamente, estaba perdiendo interés en pasar por los aros académicos sin motivo aparente. Mi rendimiento en las clases obligatorias era cada vez más pobre y me sentía desasosegado. Me gratificaban más las clases de posgrado, y empecé a pensar

en hacer otra cosa, aun cuando no tenía *in mente* nada en particular.

Durante mi primer año en informática física con Feynman había conocido a Danny Hillis, el investigador en inteligencia artificial que hacía poco había fundado la Thinking Machines Corporation, en Cambridge, Massachusetts. Feynman era allí un visitante frecuente, lo mismo que una cantidad de otros científicos e ingenieros atraídos por el enfoque radical de Danny con respecto a la construcción de un ordenador a gran escala en paralelo. Al término del año escolar, Hillis me invitó a ir a

Cambridge a trabajar en Thinking Machines durante el verano, con lo cual Feynman y yo constituimos el contingente de Caltech en lo que era esencialmente una empresa basada en el MIT.

El ordenador de la Thinking Machines —Thinking Machines Connection Machine— fue una ruptura con todo lo precedente en materia de informática de alto rendimiento, un campo hasta entonces dominado por la Cray Research. Las máquinas de Seymour Cray estaban hechas para utilizar un pequeño número de procesadores muy, muy rápidos y

sumamente costosos. En cambio, en Thinking Machines la idea fue dividir los problemas de forma que pudieran ser resueltos por más de 64.000 procesadores baratos trabajando simultáneamente.

En la empresa tuve ocasión de trabajar en una cantidad de atractivos proyectos, pero probablemente el que resultó más útil fue un sencillo invento para conectar un conjunto de pequeños discos de bajo coste. Uno de los mayores problemas con los superordenadores es conseguir que el enorme caudal de datos empleados en sus cálculos entren y salgan de la

máquina con suficiente prontitud. Utilizar un grupo de discos baratos y diseminar los datos entre ellos, en lugar de depender de un único disco rápido pero costoso, era el complemento perfecto para el ejército de procesadores baratos que estaban efectivamente manejando los datos. Mi contribución fue inventar un conjunto de discos "autorregenerable", o sea, resolver cómo distribuir la información en un cierto número de discos de forma que si uno fallase, los datos contenidos en el defectuoso se regenerasen automáticamente en uno de recambio.

Hillis era una persona estupenda con

la que trabajar, porque estaba sinceramente más interesado en construir máquinas capaces de *pensar* que en convertirse en un próspero hombre de negocios. Había reunido a un notable grupo de ingenieros y científicos, y con frecuencia las cosas ocurrían de una forma impredecible.

Un domingo por la noche, por ejemplo, Danny y yo nos encontramos con que queríamos algo de la máquina dispensadora de refrescos pero estábamos fuera del recinto. Danny recorrió el edificio buscando la llave, que finalmente encontró, pero ambos decidimos que conseguir la llave cada

vez que quisiéramos un refresco no era una respuesta óptima al problema. Nos parecía que podíamos inventar una solución permanente: sencillamente colocaríamos un interfaz a la máquina de refrescos para poder controlarla desde un ordenador conectado a Internet. Nos llevó apenas media hora poner en funcionamiento un interfaz serial que permitiese tal control y además acreditar el cambio desde un ordenador de mesa. Nuestro sistema iba un paso más allá del dado por la clásica máquina de Carnegie Mellon, que estaba conectada a la Red sólo con objeto de proporcionar información sobre cuántas latas

quedaban en la máquina y si estaban frías.

Pasé un verano estupendo en Thinking Machines, abordando sencillamente cualquier problema que me pareciese interesante, y cuando volé de regreso a Caltech, en el otoño de 1984, la idea de volver a ser un estudiante me atraía todavía menos que cuando salí de allí en junio.

Había recibido una oferta para trabajar con Steve Chen, el arquitecto de ordenadores de Seymour Cray, quien más tarde fundaría Supercomputer Systems, Inc. Visité a Chen en Cray Research y jugué con la idea de aceptar

la oferta, pero el estar fijo en una empresa se parecía en cierto modo a estar confinado en el colegio.

Al mismo tiempo, además, había recibido una llamada por parte de un equipo de investigadores que habían abandonado Caltech por el Laboratorio Nacional de Los Álamos, en Nuevo México, para construir un ordenador paralelo especializado para investigación en física. ¿Me interesaría ir a trabajar allí incorporándome a un innovador proyecto de ordenador paralelo? Parecía extraño que se lo ofrecieran a alguien no graduado habiendo tantos graduados entre los que

escoger, pero me di cuenta de que la amplitud de mi experiencia en informática tenía su valor. Estuve un tiempo sopesando mis perspectivas y fui en busca de Feynman. Quería su consejo sobre si debía seguir como estudiante.

Le encontré una tarde cruzando el *campus* a pie. Le expliqué que mis calificaciones me habían colocado en una situación problemática con la dirección, y que de todas formas no sabía si deseaba quedarme. Me respondió que si había cualquier cosa que él pudiera hacer para mejorar mi situación en Caltech, estaría encantado de hacerla. Le conté lo de la oferta que

había recibido para Los Álamos y le pedí su opinión. Él no iba a tomar ninguna decisión por mí —protestó— pero yo tuve la sensación de que pensaba que lo mejor sería que me lanzara por mi cuenta. Resolví que era hora de abandonar el colegio para siempre.

Llegué a Los Álamos a fines de 1984 con un nombramiento de investigador de posdoctorado, pese a no haberme graduado en bachillerato ni en la universidad. A los diecinueve años fui el miembro más joven incorporado a la división teórica de Los Álamos desde el ingreso de Feynman al Proyecto

Manhattan en los años cuarenta. Siendo el laboratorio de armas nucleares más antiguo de la nación, éste estaba inmerso en la burocracia gubernamental y plagado de burócratas, algunos de los cuales eran supervisores míos. Al mismo tiempo había en los laboratorios un espíritu de "poder hacer" que me resultaba refrescante, y espacios de libertad intelectual en los que era posible dedicarse a cuestiones de interés científico.

Aunque había llegado a Los Álamos en medio del creciente desarrollo de la guerra fría de Reagan, en el término de pocos años el presupuesto de defensa de

la nación iba a alcanzar su máximo para luego empezar a declinar, forzando a los diseñadores de armas, muchos de ellos antiguos prodigios en física, a justificar su existencia por primera vez en sus carreras. Entretanto, a mí me regocijaba saber que estaba trasegando fondos del presupuesto para armas al área, mucho más interesante intelectualmente, de la investigación básica en física. En lugar de devanarme los sesos en problemas como el de la forma más eficaz de volar por los aires al enemigo, yo trabajaba con un grupo que dedicaba su tiempo a explorar los fundamentos mismos de la informática, vinculado sólo teóricamente

con las armas, y que, por tanto, nos colocaba fuera de la corriente mayoritaria del laboratorio.

Aunque mi misión original en Los Álamos fue contribuir al diseño de un nuevo tipo de superordenador paralelo, acabé formando parte del equipo de visualización y simulación científicas de la División Teórica, dirigido por un brillante físico llamado Brosl Hasslacher, que era veinticuatro años mayor que yo y fue en todos los sentidos mi mentor. Fue Brosl quien me reclutó sacándome de Diseño de Ordenador Paralelo para volver a la física y juntos trabajamos en provechosa colaboración.

Si bien Brosl poseía una reputación internacional como físico, muchos de sus superiores jerárquicos en el laboratorio no apreciaban la importancia de su trabajo. Un invierno, nuestro equipo fue exiliado a una virtual Siberia, una caravana-gulag en el exterior del edificio principal del laboratorio. No nos molestaba que la jodida caravana no estuviera diseñada para aguantar un montón de terminales de ordenador y que necesitara ser equipada de forma improvisada para asegurarnos la adecuada energía eléctrica. Pero puesto que era esencial mantenernos en contacto con el mundo

exterior, tuvimos que tender un cable coaxial de ordenador hasta otra caravana que ya estaba firmemente conectada a la red principal del laboratorio y a Internet.

Como en Los Álamos puede nevar abundantemente, después de que el cable quedase enterrado por una tormenta y para protegerlo de daños accidentales, colocamos algunas señales de carretera fluorescentes de color naranja a lo largo de su extensión y alertamos al departamento de mantenimiento sobre su existencia. No sirvió de mucho. Al día siguiente vino una máquina quitanieves del Laboratorio y lo cortó limpiamente.

Tendimos un cable nuevo y volvimos a llamar a mantenimiento, pero la siguiente vez que nevó, la máquina nos dejó aislados una vez más.

Se imponían claramente medidas más fuertes. Se me ocurrió la idea de envolver el cable en kevlar, el material a prueba de rotura que se emplea en los chalecos antibalas y para amarrar los submarinos. Cogí una cuerda de kevlar, aseguré un extremo a una columna de hormigón, la enrollé a lo largo del cable y luego até el otro extremo de la cuerda al costado de la caravana vecina. "Ya está", dije para mí.

La cosa funcionó, aunque demasiado

bien quizá. La siguiente vez que una quitanieves tropezó con nuestra línea, el kevlar, actuando como el cable que contiene a un aparato que aterriza en un portaviones, la retuvo, y la máquina arrancó el costado de nuestra caravana vecina. De todos modos, a partir de entonces los conductores de las quitanieves fueron más cuidadosos.

En el verano de 1985 Brosl pasó varias semanas con el físico teórico Uriel Frisch en la campiña francesa próxima a Niza. Los dos estaban colaborando en un enfoque básicamente nuevo de la informática, que llamaban autómatas de matrices de gas. En los

años treinta, el matemático Alan Turing había presentado un sencillo dispositivo secuencial para resolver ecuaciones matemáticas que vino a conocerse como Máquina Turing. La virtud de la Máquina Turing es que puede simular cualquier otro esquema informático, y en consecuencia se ha convertido en la herramienta estándar para la reflexión en ese campo.

No obstante, tanto Brosl como Frisch eran físicos antes que matemáticos, y dieron con un nuevo modelo de informatización en paralelo a partir de la visión del mundo de un físico. Se dieron cuenta de que era

posible describir teóricamente el flujo de los fluidos de una forma completamente diferente a como lo había sido hasta entonces, y se pusieron a pensar en el diseño de los ordenadores que harían falta para simularla. El resultado obvio es que operando con ordenadores en paralelo es posible conseguir sensibles incrementos de velocidad. En su modelo, en lugar de procesar secuencialmente una fórmula compleja, el flujo de un fluido es simulado por un sistema compuesto de numerosos componentes simples que interactúan localmente. En otras palabras, un algoritmo, o receta, para

informatizar secuencialmente un problema es reemplazado por muchos agentes independientes que reciben el nombre de autómatas celulares.

Tradicionalmente, por ejemplo, el flujo de los fluidos ha sido descrito por una compleja ecuación conocida como de Navier-Stokes. Ahora Brosl y Frisch proponían la idea de una disposición hexagonal en cada uno de cuyos puntos se podían representar las partículas en colisión y en movimiento. Un conjunto de sencillas reglas de colisión para cada punto del conjunto basta para describir teóricamente todo lo que requería una compleja ecuación, y es capaz de

simular el flujo de fluido en dos o en tres dimensiones.

Frisch y Brosl eran buenos amigos y los dos comprendían que se hallaban a punto de dar un importante paso adelante, pero Frisch era sobre todo un francés, profundamente nacionalista, por lo demás. Al cabo de unos días Brosl se dio cuenta de que al final de la jornada su amigo se iba solo y entablaba una conversación telefónica con un equipo de cuatro o cinco programadores en París. ¡Estaba intentando ganarle por la mano y dar a los franceses la ventaja de ser los primeros en llevar a cabo una versión práctica del modelo de

autómatas de matrices de gas!

Brosl resolvió que él también podía jugar sucio, de modo que una noche me telefoneó a Los Álamos y me describió detalladamente el modelo teórico básico. Yo propuse algunos cambios secundarios y le dije que creía poder trabajar en ello rápidamente. La máquina con la que tenía que trabajar se llamaba Celerity, un terminal científico Unix con una visualización de alta resolución de 1280-por-1024-pixels. Trabajé un par de días codificando para poner en ejecución la teoría de Brosl en un programa que mostrase gráficamente el flujo de un fluido según emergía de

las decenas de millones de pequeñas colisiones de partículas. Debido a que sólo estaba representando un pequeño conjunto de reglas locales sobre el comportamiento de las partículas, el software era muchísimo más sencillo que las versiones existentes. Los elementos esenciales de la simulación podían describirse en unas docenas de líneas de código, y era mucho menos complejo que los varios centenares de ellas que normalmente se requieren para ejecutar cálculos de hidrodinámica bidimensional y tridimensional.

Cuando Brosl regresó de Francia una semana después yo tenía algo para

mostrarle en el visualizador, y la cosa estaba casi lista, pero algo no iba totalmente bien. Él planteó unos pocos cambios y luego se fue a su casa mientras yo me quedaba realizándolos. A eso de medianoche le telefoneé.

"Brosl, más vale que venga a ver", dije. "Está pasando algo raro en la pantalla".

En el monitor del ordenador una línea delgada que representaba un plato insertado para perturbar el flujo del fluido pasando a su alrededor estaba rodeada por un halo de colores que cambiaban lentamente. Brosl reconoció al instante que habíamos dado en el

clavo; la imagen se transformaba gradualmente a medida que el ordenador registraba los millones de colisiones de partículas y los remolinos surgían con claridad. Dejamos la imagen congelada en la pantalla y a la mañana siguiente, cuando regresamos al laboratorio, el recinto estaba lleno de expertos en hidrodinámica sorprendidos de ver que estábamos calculando algo cientos de veces más rápidamente que con los algoritmos secuenciales tradicionales.

No obstante, la teoría de Brosl no tuvo una aceptación inmediata. Imperios enteros se habían construido sobre los viejos modelos secuenciales y la

publicación de su artículo acerca de los autómatas de matrices de gas, en agosto de 1985, ocasionó una fea disputa en la comunidad científica. Algunos científicos intentaron de entrada cuestionar la exactitud de la técnica, pero pronto pudimos confirmar nuestros resultados. Era una prueba sobresaliente de que las controvertidas técnicas de la informática en paralelo podían proporcionar tremendas aceleraciones sobre los enfoques existentes.

A pesar de su triunfo intelectual, el trabajo de Brosl continuaba estando fuera de la actividad dominante, y a mediados de 1988 resolvimos alejarnos

de la política y las peleas internas del laboratorio armamentístico. Nos trasladamos a San Diego a preparar una sede alejada para la División Teórica del laboratorio. Con el fin de la guerra fría los laboratorios armamentísticos iniciaban ya su declive, y con el agotamiento de los fondos la burocracia se estaba volviendo cada vez más restrictiva. Roger Dashen, un físico a quien yo conocía bien, estaba tratando de convertir el departamento de física de la Universidad de San Diego en un lugar animado y ecléctico, y me ofreció un puesto allí como investigador. Ese verano, Brosl y yo terminamos una

noche de cargar en un semirremolque de 18 ruedas nuestro equipo informático y partimos hacia el oeste, en medio del fresco de la noche desierta.

5. Recogiendo datos

A la mañana siguiente en que Andrew y yo llegamos a San Diego tras el ataque a mis ordenadores, la sala 408 del Centro de Superordenadores se convirtió en nuestro centro de operaciones de guerra.

Situado en la planta superior, el amplio salón tuvo en un tiempo una vista al océano, recientemente bloqueada por el nuevo edificio de la Escuela de Asuntos Internacionales, y actualmente

obstaculizada aún más por un par de monitores, una cámara y otros aparatos para videoconferencias que cubrían parcialmente los ventanales de aquel lado del recinto. Pero por lo demás, los diversos elementos con que contaba —una extensa mesa de conferencias, tableros blancos contra las paredes, y conexiones con la red para nuestros ordenadores portátiles— eran perfectos para nuestros propósitos.

Nuestro grupo de urgencia empezó a organizarse a eso del mediodía. Aunque estábamos en la semana de Navidad y no había clases, siempre quedaban en el Centro algunos investigadores,

estudiantes, posgraduados, e incluso algunos funcionarios y técnicos, de modo que pudimos reunir un improvisado equipo investigador para tratar de recrear la intrusión. Con el fin de añadir un pequeño incentivo encargamos la comida a la Thai House, una de nuestras favoritas, como a diez kilómetros del *campus*. Yo había decidido que si Sid iba a soltar dinero para los gastos, debíamos intentar hacer algo útil con él, como alimentar a la gente.

Mediante una ronda de llamadas telefónicas había logrado reunir un ecléctico escuadrón de personas

dispuestas a dedicarme parte de su tiempo. Debido a las prisas del planteamiento, era una especie de ejército anárquico, y mientras que algunos de sus integrantes asumían tareas específicas, otros estaban allí simplemente para prestar su apoyo moral, o por curiosidad. Rama Ramachandran era un antiguo estudiante de la UCSD que ahora estaba en la escuela empresarial de la Universidad de Chicago y se encontraba de visita por vacaciones. A mí me seguía desconcertando aún el extraño mensaje de error de sintaxis del intérprete PostScript X-NeWS que había estado en

el visualizador de la consola de Ariel el día anterior, y como Rama era un verdadero *gurú* en PostScript, le pusimos enseguida a trabajar examinando el intérprete a ver si había sido empleado para lograr el acceso.

Entre quienes se unieron a nosotros estaban John Moreland, programador científico de visualización, y Henry Ptasinski, un estudiante en ingeniería eléctrica e informática graduado en la UCSD. Por entonces, Henry era asimismo uno de los administradores de sistema en CERFnet, un proveedor de servicio de Internet estrechamente vinculado al Centro.

En el Centro había además un encargado de la seguridad de las redes. Tom y yo generalmente nos llevamos bien siempre que no tengamos que trabajar juntos, pero le gusta intervenir en todo y a veces me refiero a él como "obstáculo ambulante". Puede que parezca una desconsideración, pero nunca he sido capaz de encontrar la manera de ser tolerante con los responsables del mantenimiento de las normas y reglamentos burocráticos que al parecer hacen que cualquier vasta organización funcione. Julia dice que mi palabra favorita es "payaso", y sostiene que debería tratar de ser un poco más

diplomático. Lo intenté esta vez, cuando se presentó a ver si podía hacer algo útil. Le entregué un fragmento de código llamado *rpc.ttdbserverd*[15] —que facilita la comunicación de algunos programas a través de una red de ordenadores— y le pedí que se lo llevara para analizarlo en busca de vulnerabilidades ignoradas por nosotros. Nos había entrado la sospecha de que aquello podía haber jugado un papel en el forzamiento, porque en uno de nuestros archivos de registros de actividad figuraba un acceso inusual al mismo en una noche de Navidad.

Cuando él abandonó la sala, uno de

los estudiantes graduados se volvió hacia mí y preguntó: "¿Por qué le has encargado una cosa como ésa? Siempre te estás quejando de él".

Andrew y yo nos miramos, y yo repliqué: "Básicamente para mantenerle tranquilo y que no nos moleste".

"Tú sabes que no va a dejarte en paz", dijo el estudiante.

"Bueno", dije yo, "al menos esto lo va a tener un buen rato ocupado".

A esas alturas todavía estábamos recopilando datos, y las cosas aparecían bastante negras, lo cual me puso todavía más malhumorado. Ya había extraído información de Rimmon y Astarte, las

máquinas de casa. Por entonces podíamos asegurar que Osiris había sido interferido, pero no cómo. En cada uno de estos ordenadores habíamos hecho comprobaciones para ver si algún archivo había sido alterado y si se habían dejado atrás cualquier programa dudoso. Al no ver ninguno inmediatamente empecé a preocuparme todavía más, porque eso indicaba que nuestro incursor conocía algún otro modo de meterse, y que creía poder volver sin ser detectado. Yo no podía pensar en volver a estar conectado hasta hacer una estimación sobre el riesgo de una nueva intrusión. Todo el mundo se

enfrascó en su respectiva tarea, dejándonos a Andrew y a mí en los ordenadores portátiles que habíamos instalado.

Los progresos resultaron esporádicos. Debido a la edad de Ariel, obtener datos útiles del ordenador era un proceso frustrante que nos llevó buena parte del día. En un ordenador moderno, la mayoría de los componentes están conectados por un haz de líneas conocido como bus de datos. Microprocesadores, memoria, disqueteras, visualizadores gráficos y periféricos varios, todos conectan a través de esta autopista principal, que en

realidad no es sino un conjunto de cables paralelos que permiten que la información circule en ambos sentidos con increíble rapidez. Ariel era tan antiguo que utilizaba un bus llamado VME, inventado en los años ochenta para los miniordenadores. Sus disqueteras se basaban también en un estándar anticuado, de modo que no había forma de poder conectar los discos de Ariel directamente a mis ordenadores portátiles, que utilizaban disqueteras SCSI más modernas. En consecuencia, teníamos que copiar primero todos los datos necesarios extraídos de Ariel para luego poder

trabajar con seguridad en él.

Anduvimos los dos explorando el edificio buscando algunos discos extra para almacenar aquella enorme cantidad de información, y por fin, ya avanzada la noche, conseguimos arrancarle a la gente de CERFnet un disco de dos gigabytes. (Para entender cuánta información representan dos gigabytes, piénsese que uno de esos discos podría almacenar cómodamente la *Enciclopedia Británica* entera, texto e ilustraciones, todo en la palma de una mano). Empleamos varias horas tratando de resolver cómo trasladar toda la información de forma que estuviese organizada exactamente

como estaba almacenada en Ariel.

A las 10 de la noche tuve toda la información de Ariel transferida al disco duro y lista para ser examinada en mi RDI portátil. Para entonces casi todos los demás habían abandonado el Centro, y Andrew y yo sentimos la necesidad de hacer un paréntesis para cenar. Bajamos en el ascensor y nos alejamos del campo en coche hasta Rubio's, un local barato de pescado y tacos que a ninguno de los dos nos gustaba especialmente. "Oye, tenemos una cuenta para gastos y en realidad deberíamos comer algo mejor que esto", le dije a Andrew. "No quiero

presentarle a Sid una nota de 4.95 dólares por una cena". Pero después de las diez de la noche no hay en aquella parte de San Diego muchos lugares donde elegir. Comimos rápidamente, deseosos de regresar al Centro a ver qué nos diría la información de Ariel.

De vuelta en la sala 408, me llevó cerca de un cuarto de hora ejecutar los programas de detección que, como con Rimmon y Astarte en casa, desvelaron a cuáles archivos de Ariel alguien había accedido y cuáles había modificado o corrompido. Por primera vez supe realmente qué habían robado de Ariel: virtualmente todo lo existente en mis

directorios. Gran parte era valioso para mí y mi trabajo, incluyendo decenas de miles de mis mensajes del correo electrónico, el código fuente para programas que yo había escrito y delicada información privilegiada. Pero de aquella lista de elementos no podía extraerse ninguna conclusión, pues el ladrón o los ladrones habían sido tan poco selectivos que habían empleado también horas en copiar programas libremente disponibles en cualquier parte de la Red, incluyendo diversas herramientas que yo mismo había bajado de la Free Software Foundation.

Nuestro análisis de los datos de

Ariel produjo por cierto una noticia: los intrusos habían estado robando archivos apenas dos horas antes de que Andrew descubriese la intrusión. De modo que ahora teníamos un cuadro bastante completo de lo que había ocurrido y cierta noción de cuándo. Pero seguíamos sin responder a la pregunta que, para mí, era la más importante: "¿Cómo lo hicieron?".

Yo sabía que a Osiris, la máquina de la cabecera de mi cama, habían accedido antes que a Ariel, en mi oficina del SDSC, pero no sabía cómo habían llegado a una y otra, ni si habían utilizado una para llegar a la otra. Y

luego estaba aquel mensaje de error del programa intérprete XNeWS PostScript en Ariel, que parecía indicar un intento de sondeo desde Colorado SuperNet. ¿Era significativo… o era una pista falsa? Si nuestro atacante sabía realmente lo que hacía, la desinformación era una posibilidad que teníamos que tener en cuenta.

Había asimismo otros elementos aislados que formaban un rompecabezas que yo todavía era incapaz de resolver. Uno de ellos era un misterioso programa, Tap, que yo había visto el día anterior mientras examinaba la memoria de Osiris. Era un programa temporal que

alguien había creado y colocado en la memoria de mi ordenador para una tarea específica. Cuando el ordenador fuese apagado o vuelto a arrancar, se borraba para siempre. ¿Y qué pasaba con el fantasma del archivo *oki.tar.Z*, cuya creación sugería que alguien andaba detrás del software del teléfono móvil, no obstante la ausencia de selectividad en el saqueo?

El examen de la información de Ariel dio lugar a otro descubrimiento crucial: el intruso había tratado de escribir encima de nuestros registros comprimidos, en los que conservábamos una relación detallada de los diversos

paquetes de datos enviados a nuestras máquinas, o recibidos por ellas, a través de Internet. Los archivos de registro borrados revelaron que al intentar sobreescribir en ellos el intruso no había tapado enteramente los originales. Era como si hubiese tratado de ocultar sus huellas en la arena arrojándole encima más cubos de arena: en algunos lugares todavía quedaba a la vista un talón, un dedo gordo, incluso un pie entero. Al parecer, teníamos nuestras primeras pistas. Puede que no tuviésemos enteramente la ruta de escape, pero al menos sabíamos en qué dirección comenzar a rastrear.

De hecho, aunque ninguna de las piezas del rompecabezas encajaba aún, el registro compacto nos proporcionó una forma potencial de comenzar a ordenar nuestros indicios. La alteración por el intruso de aquel registro de actividad aislado había sido lo primero que había alertado a Andrew sobre el ataque. Ahora, la chapucera sobreescritura del archivo de registro compactado nos daba la posibilidad de recrearla, gracias a la tecnología empleada para encaminar fragmentos de datos —paquetes— por Internet.

Esta tecnología se llama "transferencia de paquetes" y, como la

propia Internet, es el resultado directo de una idea concebida a comienzos de los sesenta por un investigador de la Rand Corporation llamado Paul Baran. En aquellos días, en plena guerra fría, los militares estaban obsesionados por el problema de sobrevivir a una guerra nuclear, de manera que uno de los encargos asignados a sus *think tanks* o gabinetes de estrategia fue inventar un sistema de comunicaciones que continuase operando incluso si algunos de sus enlaces resultaban destruidos.

Baran concibió la idea de una red de ordenadores que fuera capaz de reconducir automáticamente el tráfico.

La técnica, la transferencia de paquetes, consistía en fragmentar cada mensaje en un gran número de paquetes pequeños. Cada paquete contenía únicamente una pequeña porción del mensaje, acompañada de un packet header o guía direccional provisto de información suficiente para que en cada punto de la ruta durante su pasaje por la red cada uno de aquellos pequeños paquetes de datos pudiera ser reconducido en caso necesario y arribar con seguridad a su destino final. Los ordenadores router estaban dotados de suficiente inteligencia como para que aunque los paquetes tomaran rutas diferentes y

llegasen desordenadamente, o incluso se perdiesen, fuera posible reconstruir el mensaje en el orden correcto y requerir el reenvío de los paquetes extraviados.

La de Baran fue una brillante concepción, y a fines de los años sesenta la Agencia de Investigación de Proyectos Avanzados (ARPA) del Pentágono financió un proyecto experimental para desarrollar una red de ese tipo. El primer mensaje —"Watson, venga aquí. Necesito su ayuda"— circuló en 1970 entre el Instituto de Investigación de Stanford (actualmente SRI International), en Menlo Park, y un grupo de investigadores informáticos en

la UCLA. A partir de entonces, las cosas se han salido un poco de madre: de las dos primitivas localizaciones de ARPAnet, la red Internet se había expandido a más de 6,6 millones de máquinas y seguía creciendo en proporción geométrica.

Pero al tiempo que la multiplicidad de máquinas y usuarios está sobrecargando Internet en varios sentidos, y suministrando cobertura a gente dedicada a hacer daño, cada uno de los billones de paquetes flotando a través de la red sigue llevando esa etiqueta informativa, que dice no sólo adonde va el paquete, sino de dónde se

supone que viene. Y puesto que yo sabía que un filtro de paquetes puede tomar debida nota de toda esa información, tenía la esperanza de que los registros de paquetes de Ariel pudieran oportunamente ayudar a recrear las acciones del intruso.

Pero había una complicación: aunque el intruso no había logrado suprimir la escritura anterior del archivo de registros compactado al escribirle encima, su esfuerzo por borrarla iba a dificultar la lectura. La forma en que la información se almacena en un disco duro se asemeja al modo en que una biblioteca organiza sus fondos. Lo que

uno realmente quiere de una biblioteca es poder dirigirse al bibliotecario, pedir un determinado libro y que se lo entreguen; no le importa dónde esté colocado. Del mismo modo, la información sobre los archivos que uno crea en un ordenador está toda almacenada en un lugar en el disco duro —cabe considerarlo como el fichero de una biblioteca— pero la información en sí se conserva en otra parte, generalmente diseminada en pequeños bloques por toda la superficie del disco.

Como los bibliotecarios, los sistemas operativos de los ordenadores se encargan de la tediosa labor de

almacenar y localizar la información. Cuando el sistema operativo borra un archivo, lo que hace en realidad es borrar los indicadores que conducen a la información, la tarjeta del fichero, más bien que la información en sí, que permanece hasta que todo el espacio disponible en el disco duro está lleno y llega un momento en que nuevos datos almacenados se sobreescriben sobre los datos borrados. (Tratar de impedir esa sobreescritura fue uno de los motivos por los que hice detener el funcionamiento de Ariel y las otras máquinas tan pronto como me enteré del forzamiento).

De modo que aunque el archivo de paquetes había sido borrado, era efectivamente posible que sus datos pudieran aún reconstruirse a partir del disco; sólo que la tarea era ímproba. Como primer paso de procedimiento, Andrew sugirió: "Creo que puedo escribir un programa que localice el punto del archivo donde acaba la corrupción y luego busque el sitio donde empieza la información real". Sería un punto de partida útil, pero que no necesariamente nos permitiría dar con todos los diferentes fragmentos de datos que estábamos buscando, pues aquello sólo pondría de manifiesto la

información escrita en el archivo después de haber sido manipulado.

Se me ocurrió que podría haber una forma mejor y menos obvia de encontrar la misma información. Como físico pienso mucho en conceptos como entropía y caos, y he pasado mucho tiempo construyendo herramientas que detectan esquemas o estructuras que de otra manera podrían pasar desapercibidas. Un cuerpo de datos puede parecer ruido, pero de hecho puede poseer una estructura oculta. El reto consiste en revelar esa estructura, que puede existir en forma clara o en una que requiera el filtro adecuado para

verla.

En cierto sentido me enfrentaba al mismo problema que un criptógrafo romano intentando descifrar un antiguo lenguaje codificado conocido como clave de César. En este procedimiento, los mensajes militares se escribían en la superficie de un pergamino envuelto alrededor de un cilindro o un cono. El único modo de decodificar el mensaje era encontrar un objeto del mismo tamaño y forma y envolver el papel alrededor hasta alinear la escritura.

De un modo semejante, yo necesitaba encontrar un esquema en los diminutos fragmentos de datos

diseminados por la superficie de nuestros discos. Como todos los datos informáticos, estaban en forma de código binario: hileras de unos y ceros que pueden representar dígitos, letras y otros tipos de información. Cada fragmento de hilera era un eslabón de una cadena de información; el problema era descubrir el esquema según el cual aquellos eslabones individuales habían sido diseminados, para poder encontrarlos y rehacer la cadena. Yo lo había dejado para más tarde, porque parecía una apuesta arriesgada. Pera lo que hasta entonces habíamos conseguido a través de otros análisis era

insuficiente, de modo que se nos presentaba como el necesario siguiente paso.

"Veamos quién es capaz de conseguirlo el primero", le dije a Andrew a eso de la una y media de la mañana. Convinimos en que él escribiese su programa convencional para recuperar la información del paquete mientras que yo escribía uno para buscar esquemas en el disco y después intentar reordenarlos en algo que se pareciese al archivo original. Nos instalamos delante de nuestras estaciones de trabajo en una mesa de conferencias, el uno frente al otro,

Andrew tecleando en su RDI portátil y yo con mi nueva versión del mismo ordenador, una máquina en la que cada vez depositaba más confianza a pesar de tratarse de un prototipo no probado.

Escribí un programa llamado Hunt para investigar el disco que puse en funcionamiento por primera vez alrededor de las 2:45 de la mañana, y un segundo programa llamado Catch, diseñado para organizar lo que Hunt encontrase. Gané efectivamente la carrera por un pelín, cuando mis programas terminaron su tarea a las 4, apenas antes que el de Andrew. Al final, los dos tuvimos éxito recuperando datos,

y el archivo parcial de Andrew fue útil para contrastar mi botín de datos relevantes: 14 millones de bytes que habían estado esparcidos entre cerca de otros 2 billones, y que ahora nos permitían por fin recrear las acciones de nuestro intruso.

Saboreando el momento, me eché atrás en el asiento y exploré someramente nuestro reconstituido archivo de paquetes de registros. Con aquella información podríamos tener la oportunidad de repetir su mismo tecleado, algo muy semejante a rebobinar una cinta de vídeo para volver a ver un programa de televisión. Ahora

teníamos la ocasión de reconstruir el rompecabezas. Era la primera vez en tres días que me sentía bien.

El intruso había supuesto que sobreescribiendo en la información la haría desaparecer. Debió haber sabido que no era así. "Probablemente, es un usuario de MS-DOS", murmuré. Si intentaba ser invisible no debió haber sido descuidado. Empecé a preguntarme cuán bueno era en realidad. Una de las estrategias estándar en el submundo informático es compartir recetas de "cocina" para efectuar ataques y luego utilizar esos programas paso a paso contra objetivos en Internet. Ocurre con

frecuencia: alguien roba un código fuente de una empresa de hardware o software, o tropieza con software corriente de seguridad de ordenadores como el que había habido en mis archivos robados, o estudia revistas de informática y encuentra cómo introducirse en un sistema. Si tiene éxito hace correr la voz entre su amigos por la red, o hace figurar los detalles del cómo en cualquiera de las numerosas tablas de anuncios que funcionan como punto de encuentro de granujas en Internet. Tal vez nuestro intruso fuera simplemente otro niñato que había aprendido a leer manuales técnicos o tablas de anuncios,

y no se había percatado de que ocultar las huellas en el mundo digital no es siempre tan fácil como parece.

Por prometedores que fueran los indicios, era la tercera noche que yo dormía poco, de modo que acordamos abandonar la búsqueda. Me fui a casa, y mientras el Acura se deslizaba por las calles desiertas yo paladeaba la satisfacción de saber que aún si en el archivo de paquetes de registro no encontrásemos suficiente información como para iniciar decididamente la persecución de nuestro intruso, cuando menos deberíamos poder enterarnos de cómo había entrado y, por tanto,

encontrar la forma de mejorar nuestras defensas. Cuando llegué a casa las primeras luces del alba se filtraban en mi dormitorio, pero a pesar de mi agotamiento físico no tenía sueño. Me senté con las piernas cruzadas en mi futón ante Osiris, examinando nuestros sistemas en busca de otros indicios. Estuve tecleando distraídamente con *rpc.ttdb-serverd*. ¿Por qué lo habían dejado funcionando la noche de la intrusión? ¿Poseía el intruso algún programa inteligente que recorriese una red de ordenadores entera para violar la seguridad? El tema me preocupaba, pero al cabo de otra hora de búsqueda

infructuosa pareció un callejón sin salida.

Mientras mi coche ascendía por la colina hacia el SDSC a última hora de esa mañana, en lugar de sentirme abatido yo experimentaba por anticipado la excitación del desafío que tenía por delante. Andrew ya había llegado a la sala 408, al igual que la mayoría de los otros, y habían vuelto a ordenar que trajesen la comida. Mientras comíamos, sonó el teléfono en la sala de conferencias.

Era Mike Bowen, a quien yo conocía de la CERFnet. Ayudante técnico y un

gurú en cierto tipo de tecnología digital conocida como tecnología telefónica ISDN, se mantenía también atento a los rumores del submundo informático. Yo había hablado con él el día anterior sobre la posibilidad de que hubiese oído comentar algo sobre nuestro problema. Él me había dicho que conocía a un tío llamado Justin Petersen, de quien yo había oído hablar, que estaba en prisión en Los Ángeles por estafa con tarjetas de crédito y tratando de llegar a un trato con los fiscales federales. Petersen había estado intentando persuadir a Mike para que utilizara sus contactos en la comunidad de la seguridad

informática con vistas a que alguien pudiera convencer a los federales de escuchar su coartada: que Kevin Mitnick lo había hecho caer en una trampa mientras él —Petersen— intentaba ayudar al FBI a atraparlo. ¿Querría yo tal vez charlar con Petersen?. "Desde luego", le había dicho yo a Mike, "¿por qué no?".

Ahora Mike volvía a llamar para decir que había arreglado las cosas. Como Petersen estaba en la cárcel, sólo le permitían llamadas telefónicas de una lista restringida de personas. Para que él hablase con cualquier otra persona, alguien de la lista hacía la llamada y

luego le hacía intervenir en la conversación. Mike dijo que eso estaba a punto de ocurrir y que estuviese atento. Y colgó.

Pocos minutos después sonó nuevamente el teléfono. “Hola, estoy con la persona de la que esperabas noticias”, dijo una voz que no reconocí.

“¿Quién habla?”, pregunté.

“¿Por qué no me llamas Eric?”, respondió otra voz en la línea. Petersen había decidido utilizar uno de sus numerosos alias, aunque el más conocido era el de Agente Robo.

Justin Tanner Petersen era un personaje curioso. Nativo de Baja

California, había sido detenido por primera vez en Dallas en 1991 acusado de estafa con tarjeta de crédito y otros delitos informáticos. Gracias a un acuerdo con el Servicio Secreto y el FBI, fue puesto en libertad para trabajar bajo supervisión federal ayudando a perseguir a delincuentes informáticos, mientras otros cargos contra él se sustanciaban en los tribunales californianos. Al parecer Petersen había puesto al FBI sobre la pista de Kevin Mitnick en 1992, forzando a éste a andar ocultándose. Y también había colaborado con los representantes de la ley en reunir pruebas contra Kevin

Poulsen, un programador de Silicon Valley que había sido detenido en 1991 y acabó confesándose culpable en junio de 1994 de hacerse electrónicamente con el control de una centralita telefónica de una oficina central de la Pacific Bell para amañar concursos en dos estaciones radiofónicas de Los Ángeles, en los que ganó dos Porsche, más de 200.000 dólares en efectivo, y al menos dos viajes a Hawai. (Si usted controla la centralita de la oficina central de la compañía telefónica puede convertirse cuando quiera en el afortunado número noventa y cinco en llamar). Entretanto, el FBI poseía un

extenso expediente contra Poulsen por otras actividades en informática y telecomunicaciones, tales como escuchar las conversaciones telefónicas de su ex-novia, interceptar las de funcionarios de seguridad de la compañía telefónica que lo investigaban a él e incluso las comunicaciones electrónicas de los agentes del FBI que seguían los pasos a la hija de Imelda Marcos en Woodside, California.

Pero mientras trabajaba para el FBI parece que Petersen reincidió en el delito informático. En octubre de 1993, en una reunión en el juzgado con un fiscal de la oficina legal del distrito de

Los Ángeles confesó una estafa con tarjeta de crédito. A continuación, en plena reunión, le dijo a su abogado que necesitaba un descanso, salió de la habitación y huyó. Vivió a salto de mata hasta que volvieron a capturarle, en agosto de 1994, y ahora, más de cuatro meses después, estaba a punto de ser condenado y esperaba que yo le ayudase a hacer un trato y rebajar su sentencia a cambio de colaborar con nosotros en la captura de Kevin Mitnick. Aunque había estado tratando de negociar con el Departamento de Justicia, sus perspectivas parecían oscuras. Como yo conocía a Scott Charney, el principal

fiscal contra los delitos electrónicos, Petersen mantenía cierta esperanza de que pudiese ayudarle a hacer un trato.

Creía que Mitnick era quien lo había entregado a los federales en su detención más reciente, y eso no parecía gustarle. Tenía el acento llano de los oriundos de Baja California y me dio claramente la sensación de que no estaba siendo muy sincero.

"Ni siquiera sé si fue Kevin Mitnick el que se introdujo en mis ordenadores", dije.

"Parece ciertamente el *modus operandi* de Kevin", respondió Petersen.

Yo desconfiaba. Había potencialmente miles de personas que podrían andar tras mis máquinas. "¿Qué necesitaría para encontrarle?", pregunté. "Tengo entendido que se encuentra en una situación difícil, dado que se burló de los federales al menos una vez".

Él se mostró vago. "Yo sé cosas que obviamente no quiero decir por este teléfono", replicó.

Petersen empezó a proponer que nos viésemos personalmente y entonces él podría contarme más. Dijo que creía estar muy cerca de pescar a Mitnick, que eso llevaría tal vez un mes. Habló de dinero para gastos. Era difícil formarse

una idea del hombre, y yo seguía intentando sacar en limpio si realmente tenía o no algo que ofrecer.

Después de hablar durante cerca de tres cuartos de hora, dije finalmente: "Si tengo ocasión, le mencionaré esto a la gente de la ley, pero no creo que eso lleve a alguna parte". Agregué que si yo estaba en Los Ángeles le visitaría en la prisión. Colgamos, y llamé a Mike Bowen para decirle "¿Debo creer algo de todo esto?".

"No lo sé, es posible", respondió Mike. Tal vez Mitnick le había realmente tendido una trampa a Petersen. "Pero existe otra posibilidad",

prosiguió. “Puede que a Justin le preocupe que Kevin Mitnick tenga suficientes datos sobre él para ponerle fuera de juego por mucho tiempo”.

Decidí que por ahora, al menos, me beneficiaría más analizar los datos de Ariel que confiar en gente como Justin Petersen.

Poco después de las cinco de la tarde, Andrew y yo estábamos listos para empezar a reconstruir una crónica segundo a segundo de los sucesos de la irrupción en uno de los grandes tableros situados a lo largo de la pared. Habíamos atraído a una pequeña

audiencia de buscadores de curiosidades que se habían enterado de nuestro proyecto, incluyendo a Jay Dombrowski, el gerente del Centro encargado de redes y comunicaciones.

Nos encontrábamos en el punto álgido de nuestra investigación, y hacerlo tan públicamente implicaba un cierto riesgo: no causaríamos una gran impresión si salíamos con las manos vacías. Pero la oportunidad que todos nosotros teníamos de enterarnos de algo superaba el riesgo de pasar vergüenza.

Durante la tarde yo había maquillado el archivo de paquetes de registro reconstruido con un programa escrito

por mí, llamado Cook, que lo despojó de todo lo extraño. También había ordenado los diversos datos de investigación que habíamos reunido —en primer término, los registros de los archivos que habían sido violados— y los había combinado en un archivo, organizado cronológicamente, que nos proporcionaba una línea temporal única de todos los hechos. El archivo de paquetes de registros estaba organizado de este modo de antemano. Todo cuanto habíamos hecho los últimos días había sido una preparación para esto: ahora compararíamos sistemáticamente los registros de paquetes, que nos

mostrarían exactamente lo que el atacante tecleó o transmitió, con los datos de la investigación que revelarían las consecuencias de cada una de dichas acciones.

Andrew se situó de pie ante el tablero con un marcador especial, y yo me senté ante mi estación de trabajo RDI. Empecé a decir en alta voz cada acción según la extraía de las listas que habíamos compilado y combinado.

Comencé por la tarde del día de Navidad, poco después de pasar junto al ordenador de la entrada en Toad Hall y se me ocurrió comprobar el correo en mi red.

“14:09:32”, canté en voz alta. Por el reconstruido paquete de datos vimos que Ariel recibió por Internet la siguiente orden, una sonda exploratoria:

```
finger —1 @ariel.sdsc.edu
```

Finger es una utilidad estándar de Unix que despliega información sobre cada usuario registrado, y Ariel respondió proporcionando información básica, diciéndole al que sondeaba que existían conexiones ordinarias con Astarte, Rimmon y Osiris, y que mi ordenador había estado desatendido durante varios días. En los siguientes tres minutos del tiempo disponible de

nuestro ordenador ejecutó otros seis sondeos, cada uno dirigido a diferentes aspectos de mi red.

"14:11:49", leí. "Eh, han operado una llamada de procedimiento remoto a Osiris".

Andrew rodeó la mesa y estudió la pantalla de mi portátil. Era experto en llamadas de procedimiento remoto —Remote Procedure Call o RPC—, una función de sistema operativo que permite que un programa solicite a un ordenador remoto que haga una determinada cosa. El resultado que estaba estudiando estaba expuesto en formato hexadecimal, el sistema de

numeración de base 16 que los buenos operadores aprenden a leer como un segundo idioma. “Eso es un showmount -e[16] para mostrar sistemas de archivos exportados”, dijo. En otras palabras, era una orden que permitía a la persona que la emitía determinar qué discos duros eran compartidos por los otros ordenadores de mi red. Alguien trataba de construir lo que se denomina un trust model de mi red, para ver cuántos ordenadores tenían una relación especial, con pocas barreras de seguridad entre ellos. Era un intento de ver qué ordenadores de mi red “confiaban” entre sí, como lo hacían

Osiris y Rimmon, por ejemplo.

Examiné más de cerca los sondeos e hice un sorprendente descubrimiento: Todos provenían de *toad.com*.

"Esto es muy extraño", le dije a Andrew. "Yo estaba en Toad Hall cuando se hicieron estos sondeos, a menos de diez metros de la máquina de la que vinieron". Vi que la RPC había venido del puerto fuente 721 en *toad.com*, lo que quería decir que había sido emitida por alguien que estaba enraizado en Toad. Yo sabía que no había habido nadie más físicamente presente en Toad Hall en aquel momento aparte de Julia y yo, y me daba cuenta de

que el ataque podía haber sido organizado desde cualquier parte de Internet. Aun así, no pude dejar de preguntarme si el intruso era alguien a quien yo conocía.

Estaba intrigado, pero no había nada que hacer más que lanzarse hacia adelante.

Seis minutos más tarde vimos en la corriente de datos una prueba de que alguien intentaba iniciar una conexión de Internet: una solicitud llamada SYN (de sincronizar, en inglés *synchronize*).

"14:18:22", dije. "Veo una conexión de acceso remoto desde 130.92.6.97 con Rimmon… Un momento, ¡hay un montón

más!”. Aquello me sorprendió. Normalmente, una solicitud SYN debería haber iniciado una secuencia de saludo de ordenador individual, el breve saludo e interrogación entre dos máquinas antes de convenir en comunicarse por Internet. Eso requiere que el par de ordenadores creen e intercambien una secuencia de números de un-solo-uso para asegurarse de que esa conversación no se confunda con ninguna otra de las conversaciones que cualquiera de los dos puede estar manteniendo simultáneamente.

Pero en este caso era como si aquella máquina remota estuviera

diciendo “hola”, “hola”, “hola”, “hola”, en rápida sucesión, sin escuchar la réplica de Rimmon. ¿Por qué ocurría aquello?

Me detuve y traté de descubrir de dónde había venido aquella rápida descarga de SYNs. Los dígitos 130.92.6.97 eran la dirección en Internet del ordenador remoto, y la respuesta requirió varios interrogatorios a diversas bases de datos de Internet, pero finalmente la conseguí: en la actualidad no había tal ordenador. Los mensajes a Rimmon parecía haber venido de una red en Suiza:

University of Berna (NET-UNIBE)
Institute of Informatics and Applied Mathematics
Laenggassstrasse 51
CH-3012 Berne
SWITZERLAND

Netname: UNIBE
Netnumber: 130.92.0.0

Coordinator:
Buetikofer, Fritz (FB61) btkfr@ID.UNIBE.CH
+41 31 65 3843
Domain System inverse mapping provided by:
ARWEN.UNIBE.CH 130.92.9.52
SWIBE9.UNIBE.CH 130.92.1.1
SCSNMS.SWITCH.CH 130.59.1.30

Esa red existía, como lo indicaban los primeros cinco dígitos: 130.92. Pero parecía que el ordenador que había intentado conectar con Rimmon, la máquina designada por la dirección completa, 130.92.6.97, no contestaba, o no existía, al menos no ahora. El ordenador podía haber estado apagado desde el ataque, supuse, y, por tanto, no sería visible en la base de datos. Había otra posibilidad: la dirección podía haber sido falsa.

Continué con la cronología: "14:18:25". Eran precisamente tres segundos más tarde en nuestra línea temporal de datos. Y ahora había otro

SYN, esta vez a Osiris desde un ordenador llamado *apollo.it.luc.edu*. Volví a interrogar la base de datos de Internet y me encontré con que *luc.edu* era la Universidad Loyola, en Chicago. Como había ocurrido con Rimmon desde la misteriosa máquina en Suiza, Osiris estaba recibiendo una serie de solicitudes de conexión de acceso desde la máquina de Loyola.

"Esto es muy raro", murmuré. ¿Qué estaba pasando? Osiris estaba recibiendo una serie de SYNs, cada cual con un número secuencial para iniciar el saludo. Pero una vez que Osiris respondía —SYN-ACK— incluyendo

un segundo número secuencial, la máquina de Loyola no daba el siguiente paso normal. En vez de replicar con un tercer número secuencial, el ordenador de Loyola iniciaba el proceso de nuevo emitiendo el mandato RST, restaurar. Esto ocurrió veinte veces en rápida sucesión. ¿Por qué?

Continué buscando a través de los datos, y entonces vi algo que de entrada no tenía ningún sentido. Todos los paquetes de datos que estábamos analizando eran paquetes que habían venido de Internet a través de Ariel, que se hallaba en el armario de cableado aquí en el Centro de Superordenadores.

Pero ahora, nuestros registros habían empezado a mostrar un tráfico que parecía discurrir directamente entre Osiris y Rimmon, dentro de mi casa. “Un momento, ¡yo no debería estar viendo esos paquetes!”, exclamé. “¿Cómo es que estoy viendo el tráfico local entre Osiris y Rimmon?”.

Pero de repente me asaltó la respuesta que había estado buscando continuamente los últimos tres días. El ordenador remoto se había aprovechado del hecho de que Osiris “confiaba” en Rimmon y había falsificado una conexión de sentido único con Osiris que parecía provenir de Rimmon pero

en realidad venía directamente del intruso.

"Ah, ya entiendo", dije. Se hizo el silencio en el recinto, mientras yo miraba a Andrew. "De modo que es así como entraron".

Todos aquellos saludos abortados cobraban ahora sentido. El atacante había necesitado poder predecir el número secuencial que Osiris estaba enviando con cada SYN-ACK. Un número secuencial, en este caso, era simplemente un autentificador, muy semejante al número que te dan cuando estás en la cola de la tienda para que cuando te llegue el turno de dirigirte al

hombre que está detrás del mostrador, él y todas las demás personas reconozcan tu derecho a hacerlo. Nuestro intruso planeó disfrazarse de Rimmon, un ordenador en el que Osiris confiaba, y para conseguirlo tenía que poder responderle a Osiris con el número secuencial —o sea, el de la cola de la tienda— que éste esperaba de Rimmon.

Y ahora comprendía por qué el intruso había enviado aquella primera tanda de mensajes a Rimmon. Habían tupido la cola de entrada, amordazando de hecho a Rimmon para que no pudiese responder cuando llegara el momento de presentar su número secuencial. Una vez

atado y amordazado Rimmon, el atacante había enviado aquella serie de veinte SYNs a Osiris, para enterarse de la fórmula mediante la cual Osiris generaba sus números secuenciales —cada uno sumaba 128.000 al anterior— y de esa forma estar listo para deslizarse en el lugar de Rimmon en la cola de la tienda y responder con el número secuencial adecuado. Después, el intruso dio el número secuencial que Osiris estaba esperando y lo utilizó para abrir un canal de comunicaciones.

Andrew se había acercado y estaba observando la pantalla por encima de mi hombro. Una vez que hubieron entrado,

¿qué hicieron? Simulando ser Rimmon, el atacante en el ordenador de Loyola había enviado el siguiente breve mensaje a través del canal de sentido único: "echo ++ >/.rhosts". Este simple mandato dio lugar a que el propio Osiris suprimiera todas sus defensas posibilitando que cualquiera conectase con él sin una contraseña. El intruso había convencido a Osiris de que estaba abriendo una conversación digital con su fiable servidor de archivos, Rimmon, situado en el cuarto contiguo.

Eran ya casi las seis, y Andrew había vuelto al tablero para escribir la secuencia. Jay Dombrowski, que estaba

siguiendo parte pero no toda la cronología creada por nosotros, se excusó cortésmente para irse a casa a cenar.

Después de pensar un momento me di cuenta de que el estilo del ataque me era familiar. Con un hábil juego de manos el atacante había logrado que paquetes provenientes del exterior de nuestra red pareciesen proceder del seguro ámbito interno. Era un ataque "parodiando el IP", un tipo que había sido descrito teóricamente en la literatura de ciencia informática pero, que yo supiese, nunca había sido llevado a cabo como operación hostil.

El ataque se basaba en un fallo en el conjunto de instrucciones para las comunicaciones técnicas para el tráfico de Internet, conocido como Protocolo de Control de Transmisiones/Protocolo Internet (TCP/IP, sus siglas en inglés), que habían sido desarrolladas a finales de los años setenta y principios de los ochenta. Parodiar el IP, o sea manipular los números secuenciales de salutación para hacer pasar un ordenador por otro, era posible porque los procedimientos de saludo, creados en una era en la que a nadie preocupaba mucho la seguridad en Internet, habían sido diseñados simplemente para clarificar quién era

quién en la Red, no para verificarlo.

Yo conocía un artículo técnico sobre los problemas de seguridad en el TPC/IP, escrito en 1989 por Steve Bellovin, investigador en seguridad informática de Laboratorios Bell, en el que había descrito el procedimiento de ataque llamado IP-spoofing.[17] Pero el potencial de usar un IP-spoofing para hacerse pasar por un ordenador "de confianza" ya había sido expuesto a la atención de la comunidad informática con anterioridad, en un artículo escrito en 1984 por un estudiante llamado Robert Tappan Morris mientras estaba como interno de verano también en

Laboratorios Bell. En la última página de su informe, Morris había dado una descripción pormenorizada de cómo funcionaba ese ataque. Más de diez años después, el artículo parecía profético: "Laboratorios Bell posee una creciente red TCP/IP que conecta máquinas con diversos requerimientos de seguridad; tal vez deberían darse pasos para reducir la vulnerabilidad entre ellas mismas".

Con la caída de la noche, la sala 408 se bañó de una fría fluorescencia mientras nosotros continuábamos siguiendo el rastro digital del ataque. Una de las cosas que yo había

descubierto el martes era que tanto en Ariel como en Osiris, el atacante había insertado un programa directamente en la memoria del sistema operativo del ordenador. El Unix de Sun Microsystem tiene un elemento estándar que permite modificar el centro mismo del sistema operativo estando éste en funcionamiento, para añadir nuevas funciones. Estos programas se llaman "módulos de núcleo" y pueden colocarse directamente en "ranuras" del software en el sistema operativo mientras el ordenador continúa funcionando. Normalmente se podría usar uno si se estuviera añadiendo un

periférico al ordenador. El que estaba en Ariel parecía no ser más que basura, pero yo había tratado de analizar el que había encontrado en la memoria de Osiris y no pude de entrada sacar mucho en limpio acerca de para qué había sido diseñado. No obstante, tenía un nombre ciertamente sugestivo: Tap 2.01.

En el momento me pregunté si era un programa *sniffer* o "fisgón", que permitiese al atacante supervisar a continuación el tráfico por mi red, buscando cosas tales como contraseñas que pudieran favorecer subsiguientes intrusiones en mis máquinas o en los ordenadores de otras personas que se

comunicasen conmigo. Pero ahora veía, en los rastros de nuestros datos compactados, lo que había ocurrido. Tras instalar y hacer funcionar un programa clandestino en Osiris, el intruso regresó a través de su puerto de red secreto, un canal aparte que era precisamente uno de los que nuestros registros de paquetes no estaban controlando, y en consecuencia perdimos el rastro directo de sus pulsaciones en el teclado. Pero durante ese punto ciego en nuestro archivo de paquetes de registro todavía podíamos seguir sus actividades, las consecuencias de tales pulsaciones,

consultando nuestros datos de investigación sobre dicho periodo de tiempo.

Vimos que había insertado un programa de módulo de núcleo llamado Tap en una ranura del sistema operativo de Osiris. Casi inmediatamente después observamos que la actividad del intruso saltaba de Osiris, en casa, a Ariel, en el Centro. Si bien Osiris y Rimmon mantenían una relación de confianza que les hacía vulnerables a un IP-spoofing, no la había entre Osiris y Ariel. Iniciar una sesión de comunicación con Ariel habría requerido un conjunto de procedimientos mucho más complicado,

incluyendo una contraseña. El atacante había necesitado otra estrategia, y ahí fue donde entró Tap. Como él vio con finger, la máquina de mi casa tenía ya en marcha y en pantalla una sesión abierta con Ariel. Al parecer, ese Tap le había permitido literalmente apoderarse de aquella ventana abierta en la pantalla de Osiris, y usarla para controlar a Ariel. Tap fue el programa que proporcionó al ladrón un poder de gran titiritero, permitiéndole enviar sus pulsaciones a través del portal tal como si hubiese estado sentado en mi cama.

Era pasada la medianoche, y Andrew y yo éramos una vez más los

únicos trabajando a deshoras en la sala 408. Los inactivos terminales de videoconferencia junto a las ventanas me dirigían su mirada opaca, y de pronto recordé cómo dos días antes me había intrigado la ventana vacía en el visualizador de Osiris. Ahora estaba claro: el intruso había violado aquel portal-pantalla de forma muy semejante a como un ladrón forzaría una ventana para introducirse por ella. Y una vez dentro de Ariel, pudo disponer a gusto de mi software y mis mensajes de *e-mail*, y después llevárselos a quién sabe dónde en Internet.

6. Mis vacaciones de Navidad

En los días inmediatamente posteriores a desentrañar el ataque por IP-spoofing, mi vida no volvió a la normalidad, pues había mucho trabajo de limpieza y reconstrucción pendiente. Pero sí encontré tiempo para patinar al sol invernal de Baja California y hablé regularmente por teléfono con Julia, sopesando la posibilidad de que viniese

a visitarme a San Diego. Buena parte de mi tiempo la dediqué a construir un router más seguro para mi red, que no sólo rechazara a los agresores sino que almacenara detallados archivos de registros y nos alertase rápidamente si éramos atacados. También Andrew trabajó largas horas descifrando los programas que los ladrones de datos habían dejado atrás, y juntos pasamos varios días completando los últimos detalles e intentando asegurarnos de que entendíamos perfectamente cómo habían violado nuestra seguridad.

Llamé a Toad Hall para preguntarle a John Gilmore por los primeros

sondeos desde *toad.com*. Él se encontraba cada vez más incómodo debido a mi relación con Julia. Fue una conversación tensa. Le conté lo del ataque contra mis ordenadores y los primeros sondeos desde el suyo. Él examinó los registros de contabilidad que llevaba su ordenador y me informó que no había ninguna actividad sospechosa.

"Sabes tan bien como yo que si alguien irrumpió en *toad* podría haber alterado tus archivos de registros para ocultarse", dije.

Más tarde hablé con Julia y ambos decidimos que el ataque era una

asombrosa coincidencia. Sabíamos que yo no había estado implicado, pues había estado arriba lejos de los ordenadores, y nos dimos cuenta de que al plantear el asunto podíamos estar abriendo la caja de los truenos. ¿Había alguien tratando de tenderme una trampa a mí, o acaso a John? ¿O se trataba de algo del todo diferente? Resolvimos que lo mejor era no hacer nada, habiendo tantas posibilidades de que la gente se precipitase a extraer conclusiones erróneas.

En San Diego Andrew y yo empezamos a trabajar en la mejora del perímetro defensivo de mi red. Para

muchas personas, la seguridad en Internet no requiere actualmente más que salir a comprar un sistema de los llamados firewall o cortafuegos, una solución tipo caja negra que sólo sirve para limitar el tipo de paquetes de información que puede entrar desde el mundo exterior. Yo nunca he creído que el mero hecho de reforzar los muros del castillo ofrezca una mejor defensa, de modo que lo que nosotros hicimos en cambio fue instalar trampas y alarmas en la red, para que nos resulte más fácil detectar y rechazar futuras intromisiones. Ariel fue mejorado una vez más, ahora con la instalación de

unidades de disco más modernas. También escribimos un software que nos protegiese contra cualquier acción de IP-spoofing o ataques similares. Queríamos tener inmediata constancia de cualquier futuro intento de manipulación, y nos pusimos a modificar el software de nuestra red de forma que fuera imposible engañar a nuestras máquinas con una falsa dirección de Internet.

Diseñamos nuestro nuevo router de seguridad para examinar la dirección de cada paquete que circulase desde Internet a nuestra red. En caso de descubrir una dirección que al parecer

proviniese del interior diría: “Un momento, esto no debería ocurrir”, y a continuación no sólo rechazaría el paquete, sino que además activaría simultáneamente una alarma.

Revolviendo por ahí rescaté una cantidad de piezas de recambio y configuré el router para instalarlo entre el mundo exterior y mi sector de la red del Centro de Superordenadores. Lo construimos de una SunSPARCstation que requisamos para ello en su emplazamiento del armario de cableado al lado de Ariel. Le dimos tres nombres. Si queríamos enviar paquetes al mundo exterior los mandábamos “al caos”. Si

se enviaban paquetes a mis ordenadores se dejaban “a la casualidad”; al distribuidor en sí le pusimos “el abismo”.

En el meollo de nuestra defensa estaba una tecnología básica de red informática llamada filtración de paquetes. La posibilidad efectiva de escrutar y capturar paquetes individuales mientras se desplazaban por un cable surgió por primera vez a principios de los ochenta, porque los diseñadores de redes necesitaron una herramienta de diagnóstico para chequear sistemáticamente y poner a punto sus sistemas. Más recientemente,

empero, la filtración de paquetes se ha convertido en una poderosa herramienta muy susceptible de ser mal utilizada. Ni la primera red de área local Ethernet ni las primera redes de ordenadores de Internet fueron construidas teniendo en cuenta los factores intimidad y seguridad. Eran simplemente proyectos de investigación diseñados para permitir a los científicos e ingenieros informáticos explorar la idea de enganchar ordenadores dentro de una oficina y entre ciudades y estados. Pero en el periodo comprendido entre los últimos años sesenta y el presente, las redes informáticas evolucionaron, hasta

el punto de haberse convertido en parte integral del tejido de nuestra sociedad y no ser únicamente herramientas de investigación. Ethernet funciona anunciando cada paquete por toda la línea. Lo normal es que los ordenadores que están en la red escuchen los anuncios de los paquetes y simplemente cojan los que están dirigidos a ellos. El problema con la tecnología de Ethernet es que alguien puede hacerse con el control de un ordenador en la red y sencillamente vaciar todos los paquetes, estén o no dirigidos a él. Por lo general esa información no está cifrada y constituye un tremendo fallo de

seguridad porque el sniffing o husmeo es una actividad pasiva. No hay forma de saber con certeza si los paquetes dirigidos a nuestro ordenador están siendo ilícitamente cogidos y examinados por otra persona.

Según fue aumentando el flujo de información por las redes de ordenadores, en cierto momento los malos de la película empezaron a utilizar filtros de paquete o sniffers, como se los llamó, para observar todo el tráfico que discurría por una red, reservándolo para más tarde extraer contraseñas y cualquier otro dato que circulase entre dos ordenadores.

Pero así como el filtrado de paquetes puede ser usado para invadir la intimidad, también puede ser utilizado para proteger y su seguridad por parte de los operadores de las redes, que de otro modo estarían inermes ante quienes atentan contra sus sistemas. Uno de los proyectos en los que he trabajado durante años ha sido el crear mejores filtros de paquete para estar al día con unas redes de ordenadores cada vez más rápidas. Como resultado, he sido criticado por los defensores de la intimidad en las comunicaciones informáticas a cuenta de haber mejorado una tecnología que en malas manos

puede ser peligrosa. Algunos han sugerido incluso que estaba creando tecnología para Big Brother. Obviamente, lo mismo que numerosas tecnologías en este mundo, se puede hacer uso y abuso del filtrado de paquetes, pero en sí mismo no es más que una herramienta. Y las herramientas son únicamente eso, herramientas. La posibilidad de un mal uso no basta para disuadirme de desarrollar una herramienta, especialmente cuando tiene un papel así de vital.

La primera oportunidad que tuve de poner en acción esta tecnología contra un oponente real en la Red se presentó a

comienzos de 1991 cuando recibí una llamada de Castor Fu, un ex-condiscípulo de Caltech. Castor había trabajado conmigo en Los Álamos continuando los estudios para graduarse en física en Stanford. En enero de aquel año advirtió que Embezzle, una de las estaciones de trabajo en el departamento de física de Stanford, mostraba un comportamiento extraño.

Investigando, descubrió que un intruso se había hecho con el control de una cuenta llamada *Adrian*, en desuso desde hacía tiempo, y la estaba utilizando como emplazamiento desde el que lanzar ataques a toda clase de

ordenadores del Gobierno. Introduciéndose a menudo por teléfono en la red de Stanford, el pirata utilizaba seguidamente Internet para lanzar sus incursiones desde los ordenadores de la universidad. Irritado, Castor fue a notificarlo a los encargados de la seguridad informática de la universidad. Supo así que ellos estaban enterados del ataque pero habían decidido no hacer nada porque consideraban que era mejor dejar que el intruso continuase, para de ese modo tener alguna idea sobre sus propósitos, en lugar de quedarse totalmente a oscuras.

La falta de preocupación por parte

de la universidad aumentó la de Castor, que me pidió que le ayudase en su labor de vigilancia. Instalamos software de control en su red y yo escribí un software que nos permitiese reconstruir a la manera de un vídeo los paquetes que capturásemos durante las incursiones. Al repetir la secuencia de datos podíamos ver exactamente lo que veía el intruso y observar cada uno de sus golpes en el teclado exactamente como los ejecutaba.

En esa época Stanford poseía un banco de modems de libre acceso que permitían a cualquiera conectar con los ordenadores de la universidad.

Finalmente, descubrimos que el intruso era un joven holandés que parecía disponer de una cantidad considerable de tiempo libre para dedicarse a atacar a diversos ordenadores —sobre todo militares y del Gobierno— en torno a Internet. Castor supuso que era holandés porque usó la palabra *probeeren*, "intentar", en holandés, como nueva contraseña creada para la cuenta robada. También notamos que los ataques se producían en correspondencia con las horas de los programadores en Europa. Durante varios meses vigilamos de cerca sus actividades, tratando de que no hiciera nada destructivo. Cuando

efectivamente atacaba a otras cuentas de la Red alertábamos a la gente sobre los ataques.

Resultó que no éramos los únicos en mantener a Adrian bajo vigilancia. Más o menos por la misma época en que nosotros empezamos a seguirle los pasos, Bill Cheswick, un investigador en seguridad informática de Laboratorios Bell advirtió que alguien estaba usando a Embezzle en Stanford para husmear en el sistema de Laboratorios Bell en Murray Hill, Nueva Jersey. El lugar de limitarse a rechazar el ataque, Cheswick decidió jugar como el gato y el ratón. Creó un falso ordenador, al que él y sus

colegas se referían como “nuestra cárcel”. Instaló el ordenador pasarela especial fuera de la máquina “cortafuegos” de Laboratorios Bell y creó un software de “cuarto de juegos” en el cual podía vigilar cada movimiento y cada golpe de teclado del intruso.

El holandés a quien llamábamos Adrian era conocido por el equipo de Cheswick como Berferd, por el nombre de la cuenta que había usurpado en Laboratorios Bell. Durante varios meses Cheswick estudió las actividades de Berferd, le proporcionó información falsa y trató de ayudar a la gente de

seguridad informática de otros sitios que intentaba seguirle el rastro. Entretanto, se permitía alguna travesura de su cosecha: en el software que escribió para disfrazarse de sistema de Laboratorios Bell, insertó varios estados de "espera" con objeto de simular un sistema de ordenador ocupado. El atacante holandés debe haberse quedado muchas veces tamborileando en el escritorio con los dedos mientras esperaba, pero al parecer nunca se percató.

El intruso intentó alguna vez hacer algo abiertamente destructivo. En una ocasión Cheswick lo vio teclear la

orden *rm -rf /&*, tal vez la más devastadora en el vocabulario de Unix. Cuando se la emplea desde una cuenta raíz hace que el ordenador recorra sistemáticamente todos sus directorios borrando todos los archivos. Aparentemente, Berferd quería cubrir sus huellas, sin importarle el daño que causaba. Dentro de los confines de la "cárcel" de Laboratorios Bell, aquella orden podía hacer poco daño. Pero la voluntad de usarla por parte de Berferd le demostró a Cheswick que el intruso estaba lejos de ser inofensivo. En un artículo sobre el ataque escrito unos meses después, Cheswick escribió:

“Algunos piratas informáticos defienden su actividad con el argumento de que no causan ningún daño real. El nuestro lo intentó sin éxito con nosotros (borrar nuestros archivos) y lo logró con esa orden en otros sistemas”. Adrian y algunos compatriotas suyos con quienes daba la impresión de actuar pertenecían aparentemente a un tenebroso bajo mundo informático que compartía información sobre los diversos microbios y vulnerabilidades en los sistemas que atacaban. Es una ironía que sus incursiones provocasen el benéfico efecto de poner de manifiesto el deplorable estado de muchos

ordenadores que deberían haber tenido verdaderos cerrojos en sus puertas. En un ordenador de la NASA Adrian intentó registrarse como “noticia” —una rutina en muchos ordenadores Unix para manejar transacciones Usenet entre diferentes ordenadores de la red—. El ordenador respondió que “noticia” carecía de contraseña ¡y le pidió que crease una propia!

Otra vez le observamos utilizar con éxito el famoso microbio “sendmail” de Robert Tappan Morris. Sendmail es el programa estándar de Internet para el manejo del correo, y en 1988 Morris había escrito un programa que

aprovechando una insuficiencia en sendmail afectó a más de seis mil ordenadores en Internet. La insuficiencia era ampliamente conocida desde hacía tres años, y Sun había distribuido software para subsanarla. Fue evidente que algunos responsables de sistemas fueron demasiado perezosos para asegurar sus máquinas y pagaron las consecuencias.

También observamos la vez en que Adrian penetró en los ordenadores del Pentágono correspondientes al Comando de la Flota del Pacífico y leyó el correo. Utilizó un mandato de búsqueda para captar todas las instancias en que

aparecía la palabra “Golf”. Nuestra impresión fue que en realidad él había estado buscando la palabra “Gulf”, porque en ese mismo momento los militares estaba movilizando sus fuerzas en la región del golfo Pérsico. De hecho, una noche ya muy tarde Castor estaba siguiendo a Adrian, que hurgaba y husmeaba por Internet, cuando alguien se asomó por la puerta y dijo “¿Sabes una cosa?: estamos en guerra”.

Castor le dirigió por un segundo una mirada inexpresiva y luego dijo: “Lo sé, es como una guerra”.

El tío pareció igualmente desconcertado. Finalmente dijo: “No, es

una guerra *de veras*. Los aliados acaban de bombardear Bagdad".

A pesar del hecho de que ahora Adrian estaba leyendo impunemente incluso el correo electrónico militar no reservado era difícil conseguir que los burócratas en las diversas agencias gubernamentales hicieran algo al respecto. Cuanto más le observábamos, más nos percatábamos Castor y yo de que Adrian/Berferd no era realmente un experto operador de Unix, sino apenas uno persistente. Una vez se puso a teclear "mail-a", "mail-b", "mail-c", y así hasta "mail-z", y luego repitió el proceso en mayúsculas, buscando una

determinada vulnerabilidad que nunca encontró. Mucho de lo que estaba haciendo caía en la categoría de la mera imitación. Puesto que parecía no saber tanto y que simplemente copiaba las técnicas que veía decidí llevar a cabo un experimento propio. Dedicamos cierto tiempo a "enseñar" a Adrian nuevas vulnerabilidades debilitando a propósito alguna parte de la defensa de un ordenador que él estuviera sondeando, haciéndole por un momento accesible la entrada. A continuación restaurábamos la defensa, dejándole efectivamente fuera. Sin percatarse de la estratagema, él repitió el mismo truco por toda la red;

si bien fracasó en todas partes, nos dio una especie de firma muy clara por la cual identificarle cuando entrara en acción.

Una noche dejé abierta una sesión de comunicación a distancia en la Embezzle de Stanford. Yo me había conectado con un ordenador del Laboratorio Nacional en Los Álamos y luego había abandonado la sesión. Con eso dejé una vía hacia el laboratorio expedita para que Adrian la retomase, aunque indicaba un lugar en el que yo estaba muy seguro de que él no podría penetrar. Puesto en antecedentes por Castor y yo, Los Álamos se había interesado en Adrian,

pero para tomar medidas al respecto necesitaba disponer oficialmente de un motivo.

Al día siguiente, al activar el comando ps para ver qué programas estaban en ejecución en el ordenador de Stanford, Adrian encontró mi abandonada sesión con Los Álamos —*lal.gov*— y mordió el anzuelo. Empezó a intentar introducirse en los ordenadores del laboratorio de armas. Yo llamé a los funcionarios de seguridad del laboratorio y les informé que Adrian estaba atacando su red. Aunque no tuvo éxito, Adrian se había convertido oficialmente en un asunto de

la incumbencia del Departamento de Energía.

En última instancia, el rastreo telefónico se demostró imposible, porque en esa época no existía en Holanda una ley contra los delitos informáticos y la compañía telefónica holandesa no iba a colaborar ante las solicitudes de rastreo de los funcionarios de Estados Unidos. No obstante, en abril, un experto holandés en seguridad informática llamado Wietse Venema se puso al habla con colegas americanos y les informó que había detectado a un pequeño grupo de programadores holandeses que se

estaban introduciendo subrepticiamente en sistemas informáticos de Estados Unidos. Estaba en condiciones de identificar a Berferd con nombre, dirección, teléfono e incluso número de cuenta bancaria. Más o menos por la misma época yo recibí una llamada de John Markoff, el periodista del *New York Times*. Nunca nos habían presentado, pero Markoff se había enterado de que yo estuve vigilando de cerca al intruso holandés. Yo le describí nuestra vigilancia, y el 21 de abril el artículo de Markoff apareció en la primera página del *Times*:

BANDIDOS INFORMÁTICOS HOLANDESES SE INFILTRAN IMPUNEMENTE EN SISTEMAS AMERICANOS

por John Markoff, especial para el *New York Times*

Fuera del alcance de las leyes americanas, un grupo de intrusos informáticos holandeses ha desafiado abiertamente a las autoridades militares, espaciales y de inteligencia de los Estados Unidos durante casi seis meses. Recientemente violaron la entrada en

un ordenador militar estadounidense mientras les filmaba una estación holandesa de televisión.

Los intrusos, empleando líneas telefónicas locales que les permitían acceder a redes informáticas americanas prácticamente sin costo, no han causado prejuicios graves, según los investigadores federales. Ni han violado los sistemas informáticos gubernamentales más seguros. Pero han entrado en una amplia variedad de ordenadores, incluyendo los del Centro Espacial Kennedy, el Comando de la Flota del Pacífico en el Pentágono, el

Laboratorio Nacional Lawrence Livermore y la Universidad de Stanford, utilizando una red informática internacional conocida como Internet.

Si bien la información en dichos sistemas no es reservada, los ordenadores almacenan una gran variedad de material, que incluye memorandos de rutina, informes no publicados y datos relativos a experimentos. Funcionarios federales declararon que el grupo había manejado parte de la información almacenada en los sistemas en los que se introdujeron

ilegalmente.

Funcionarios del Gobierno de los Estados Unidos declararon haber estado rastreando a los intrusos, pero que no se han efectuado detenciones porque en Holanda no existen restricciones legales que prohíban el acceso no autorizado a los ordenadores. Nuestras llamadas telefónicas a funcionarios gubernamentales holandeses en Holanda y en Estados Unidos no han obtenido respuesta.

Aunque convino en no mencionar mi nombre, como fondo de la historia

Markoff incluyó una referencia a mi participación:

El grupo holandés fue detectado el pasado año después que un investigador informático excepcionalmente hábil del Gobierno de Estados Unidos rastrease en un laboratorio nacional cada uno de los movimientos del mismo utilizando avanzadas técnicas de seguridad informática y notificase de las intrusiones a las autoridades federales.

Dicho investigador ha podido efectuar registros informáticos de las

acciones de los intrusos en el momento en que hurgaban electrónicamente en ordenadores militares, de la NASA, universitarios y otros muchos en los Estados Unidos. Con esa información grabada le fue posible luego obtener una representación exacta de la pantalla del ordenador tal como se le aparecía a los intrusos en Holanda.

El artículo del periódico y el clamor subsiguiente que provocó generaron interés por mi trabajo por parte del Gobierno, y a su debido tiempo expuse

ante diversas agencias el tema de Adrian y sus ataques. Como parte de esas conferencias preparé una videocinta de algunas de las sesiones de Adrian, para que las personas no familiarizadas con la informática pudieran comprender exactamente cómo trabajaban los piratas y experimentar cómo era observar una pantalla de ordenador por encima del hombro de uno de ellos. Podrían ver y oír, incluidos los timbres que sonaban en su terminal, lo que él veía y oía en tiempo real. Yo había planeado originalmente utilizar las bandas sonoras extra de la cinta, una para comentarios maliciosos sobre las técnicas de Adrian

y la otra para las risas de apoyatura. Lamentablemente, nunca conseguí tiempo ni presupuesto.

El incidente Adrian me proporcionó además una útil lección cívica. En el otoño de 1991 yo estaba en Washington D.C. para mostrarles mi vídeo a unos investigadores en la Oficina de Contabilidad General, a la cual el Congreso había encomendado investigar las violaciones. Pero cuando estaba a punto de iniciar mi intervención, unos abogados del Departamento de Justicia se enteraron del acto. Telefonearon a la OCG y exigieron que yo no presentase la cinta, argumentando que formaba parte

de las pruebas en el caso que tenían planteado ante el Gobierno holandés. Mientras yo permanecía sentado esperando en el interior de una sala de conferencias sin ventanas, tres abogados del Departamento de Justicia atravesaron velozmente la ciudad en un taxi para enfrentarse a los de la OCG, al parecer preocupados porque yo iba a poner en evidencia a la burocracia. Todo aquello me parecía ridículo: los burócratas tratando de tapar sus fallos. Al final no se me permitió efectuar la presentación hasta varios meses después… y entonces sólo en presencia de funcionarios del Departamento de

Justicia y del FBI.

La conmoción originada por el asunto Adrian contribuyó a mi interés por la investigación en seguridad informática, y éste a su vez me condujo a la búsqueda de mejores herramientas. Una de las que modifiqué para mi tarea fue un sofisticado elemento de software llamado Berkeley Packet Filter. Escrito originalmente en 1990 por Van Jacobson y Steven McCanne en los Laboratorios Lawrence de Berkeley, financiados con fondos federales, tenía por objeto la sencilla tarea de controlar el rendimiento de redes de ordenadores y depurar los errores en las mismas. El

inconveniente era que había sido creado para la generación de redes de ordenadores entonces existentes. La mayoría de los negocios y centros de investigación utiliza todavía Ethernet. Sin embargo, Ethernet es un estándar envejecido, y para 1994 me pareció necesario crear software capaz de estar a la altura de las redes de ordenadores mucho más avanzados, como los que emplean cables de fibra óptica y pueden alcanzar velocidades de al menos un orden de magnitud más rápidas que Ethernet. Hoy en día la mayoría de los grandes servicios comerciales online[18] tienen redes internas de fibra óptica para

manejar los billones de bytes de información que circulan diariamente entre sus máquinas. La versión modificada del BPF que yo escribí era capaz de filtrar más de cien mil paquetes por segundo, aun cuando estaba funcionando en una estación de trabajo Sun de varios años de antigüedad. A diferencia del BPF original, mi versión estaba preparada para sepultarse en el interior del sistema operativo de un ordenador y estar alerta a determinada información en el momento en que ésta fluía por el ordenador desde Internet. Cuando un paquete desde una dirección determinada, o bien cualquier otra

información deseada por el usuario pasara como un relámpago, BPF intervenía y la colocaba en un archivo donde pudiera conservarse para ser revisada después.

Yo había desarrollado mi versión inicial del BPF más rápido con la expectativa de recibir de la Agencia de Seguridad Nacional fondos adicionales para mi trabajo de investigación. La Agencia había empezado a respaldar mi trabajo con una subvención de los Laboratorios Nacionales de Los Álamos en 1991, y había prometido prorrogar su respaldo, pero los fondos no llegaban nunca. Yo desarrollé la herramienta,

pero una vez completado el trabajo, a principios de 1994, los burócratas de la Agencia se echaron atrás con la financiación

La idea de trabajar con la Agencia de Seguridad Nacional suscita controversias en la comunidad de profesionales de la seguridad y de las libertades civiles, muchos de los cuales la consideran una fortaleza oscurantista de la alta tecnología.

Libertarios por inclinación o por influencia de sus colegas, los mejores expertos informáticos de la nación tienden a poseer una marcada sensibilidad, incluso hacia la más leve

insinuación de una violación de las libertades civiles. Contemplan con gran desconfianza el trabajo de la Agencia de Seguridad Nacional, que tiene las misiones gemelas del espionaje electrónico alrededor del globo y la protección de los datos informáticos del Gobierno. Esta desconfianza se extiende a cualquiera que trabaje con la agencia. ¿Estoy yo contaminado porque acepté financiación de la ANS para mi investigación? La situación me recuerda la escena de la película *¿Teléfono rojo? Volamos hacia Moscú* en la que el general Jack D. Ripper está obsesionado por la idea de que sus fluidos corporales

están contaminados. Creo que la idea de culpa por asociación es absurda.

Mi punto de vista es muy diferente. En primer lugar, no creo en la investigación reservada y, por tanto, no la hago. Se suponía que la tarea que yo había acometido sobre filtrado de paquetes estaba financiada por la agencia para hacerse pública. Las herramientas iban a estar ampliamente a disposición de cualquiera, para utilizarlas contra las malas personas que ya estaban empleando herramientas similares para invadir la intimidad de los demás y comprometer la seguridad de las máquinas en Internet.

Pero lo que es aún más pertinente, yo creo que la agencia, más que ser inherentemente civil, es esencialmente inepta. Muchas personas temen a la ASN, sin darse cuenta de que es como cualquier otra burocracia, con todas las debilidades de los empleados de una burocracia. Como el personal de la ASN vive en un mundo reservado, los sistemas normales de comprobación y balance no les son aplicables. Pero eso no significa que su tecnología supere a la del mundo informático abierto; sólo significa que son atrasados y pedestres.

En cualquier caso, estoy convencido de que herramientas como el BPF son

absolutamente imprescindibles para que haya seguridad en Internet y para que podamos rastrear en ella a los vándalos. Las personas cuya preocupación es que esté en riesgo la intimidad de las comunicaciones personales probablemente deberían preocuparse menos sobre quién debe tener el derecho de supervisar las redes, y en cambio centrar sus esfuerzos en conseguir que el software criptográfico fuera ampliamente asequible. Si la información está cifrada no importa quién la vea si no sabe interpretar la clave. La criptografía es otro ejemplo para mi argumento de que una

herramienta no es más que una herramienta. En realidad, hasta hace únicamente dos décadas fue utilizada fundamentalmente por reyes, generales y espías. Después, la labor realizada por los científicos en Stanford, el MIT y la UCLA, coincidente con el advenimiento del ordenador personal de bajo coste, pusieron el necesario software al alcance de cualquiera. Como resultado, el equilibrio de poder está cambiando de forma notable, a expensas de la NSA y en favor del individuo y de la protección de nuestras libertades civiles.

En San Diego, mientras nos preparábamos para volver a situarnos on-line, nuestro intruso continuó importunándonos, poniéndonos una segunda llamada la tarde del 30 de diciembre. Cuando regresé a mi despacho y escuché mi buzón de voz allí estaba de nuevo mi antagonista. El sistema me dijo que el mensaje había sido efectuado sólo minutos antes, a las 2:35 de la tarde. Empezó por algo semejante a un fuerte maullido —¿o era un gallo cacareando?— y terminó tras un curioso gimoteo decreciente.

"Su técnica de seguridad acabará

vencida", empezó el mensaje, en una voz que sonó como la de una persona distinta a la de la primera llamada. "Su técnica no sirve". Lo siguiente fue una frase inconexa: la escuché una y otra vez sin poder desentrañar su sentido.

Al parecer el intruso había calculado que ahora estábamos fuera de la Red, y estaba tratando de irritamos para conseguir acceso. "Estos se están volviendo bastante insolentes", le dije a Andrew cuando le hice escuchar el mensaje. "¿Por qué no dejan de bobear?" Quienquiera que fuese —él, ellos— la intención era sacarnos de quicio, pero yo no veía claro el porqué.

Parecía una cosa pueril. Al mismo tiempo sentía cierto alivio, pues era obvio que creían haber salido indemnes, y cabía la posibilidad de que ese exceso de confianza los hiciera más vulnerables en el futuro.

La noche de fin de año estuvimos los dos en el Centro trabajando en el router de seguridad. Hicimos un breve paréntesis para ir al apartamento de Andrew, donde su esposa, Sarah, y un pequeño grupo de amigos estaban de fiesta. Tenían la televisión puesta, había champán, y finalmente el reloj dio las doce. Nos quedamos un rato más y luego regresamos al trabajo. Estuve

codificando afanosamente un par de horas más y pasadas las 3 de la mañana me fui a casa dormir, con mi parte del filtro distribuidor casi acabada.

Julia me preocupaba cada vez más, pues cuando hablábamos me parecía más deprimida. Había pasado días sin salir de Toad Hall, y aunque repetía que vendría a visitarme, había perdido un par de vuelos. De modo que al día siguiente, ya que Julia seguía discutiendo con John sobre la idea de su venida a San Diego, decidí ir al norte.

A eso de las 8 de la tarde Andrew me llevó al aeropuerto y yo le dejé una lista de cosas que terminar y cabos

sueltos de los que ocuparse. Él dijo que tenía la esperanza de regresar al trabajo esa noche y adelantar en su labor. Pero al final nuestro ritmo de trabajo pudo con él, ya que habíamos venido durmiendo a un promedio de cuatro horas diarias durante cinco días. Andrew se fue a casa, directamente a la cama, y durmió todo el día siguiente.

Yo volé a San José, donde cogí un coche de alquiler y fui a San Francisco, con una parada en casa de Mark Lottor para recoger el equipo de esquiar que había dejado allí la mañana del veintisiete. Mi idea era sacar a Julia al aire libre, ya fuera de excursión o a

esquiar en las montañas, confiando en que lejos de Toad Hall tendría la oportunidad de pensar las cosas desde una nueva perspectiva. Hacía mucho tiempo que éramos íntimos amigos, y yo le había prometido que si alguna vez se sentía presa de la rutina o el decaimiento vendría a pasar un tiempo a su lado lejos de la ciudad. Ella me había prometido otro tanto.

Para cuando llegué a la ciudad eran ya las 11 de la noche. Julia y yo nos reunimos en nuestro punto de encuentro convenido: el apartamento de Dan Farmer en el Panhandle, en el distrito de Haight-Ashbury. Dan y yo éramos

amigos desde hacía mucho tiempo y ambos teníamos poco respeto por el convencional mundo de la seguridad informática. Él es un discutido experto que obtendría la atención internacional en 1995 mientras trabajaba como especialista en seguridad para Silicon Graphics, Inc., una empresa fabricante de estaciones de trabajo de Mountain View, California. La controversia al respecto se debió a un programa de control de la seguridad llamado SATAN (Security Administrator Tool for Analyzing Networks) del que fue autor con Venema, el experto en seguridad holandés. SATAN fue diseñado para

controlar automáticamente vulnerabilidades de sistemas informáticos ampliamente conocidas, para que los encargados del sistema tuviesen un modo rápido de identificar y estimar los puntos débiles de sus propias redes. Esperando sacar de su autocomplacencia a los profesionales informáticos, Dan planeaba que el programa fuera accesible a todo el mundo en Internet. Esto significaba que todos los piratas dispondrían de una forma fácil de husmear en la Red en busca de puntos débiles, y que todos aquellos encargados de sistemas informáticos lo bastante perezosos como

para no haber protegido sus sistemas estarían en peligro.

El inminente lanzamiento de la versión final de su programa en Internet, fijado para abril de 1995, daría lugar a un intenso debate. El mantener la información sobre seguridad informática a buen recaudo o distribuirla libremente ha sido siempre un tema candente en los círculos profesionales. Era obvio que Dan había esperado aumentar la temperatura al dar a su programa un nombre tan demoniaco: SATAN.

Dan, un ex *marine*, tiene además un estilo personal que choca con el más formal de la gente de Silicon Valley. De

complexión liviana, pero con una roja cabellera rizada que le cae más allá de los hombros, una preferencia por las camisetas y la ropa de cuero negras, y una inclinación por diversos objetos de metal que le perforaban diversas partes del cuerpo, Dan no casa con el estereotipo del fanático de los ordenadores. A comienzos de 1995, Silicon Graphics, en un arranque de cobardía y miopía empresariales, decidió echar a Dan poco antes de que tuviese lista la versión final de SATAN. Unas semanas después fue contratado por la Sun, competidora de la SGI, pero el asunto provocó tal conmoción en

Silicon Valley que lo que consiguió la SGI fue perder doblemente, al ser criticada duramente y quedarse sin Dan.

Julia y yo conversamos hasta muy avanzada la noche; y ella me habló de la profundidad del rencor y el sufrimiento entre John y ella. Las cosas se habían vuelto mucho más tensas en la última semana. Julia empezaba a ver claro que la relación no funcionaba, pero yo empezaba a preguntarme si había algo autodestructivo en su renuencia a poner fin a todo aquello.

Planeábamos realizar una excursión por Marin Headlands al día siguiente, pero John llamó por la mañana

preguntando por Julia. Después de hablar con él, Julia pareció todavía más tensa y desasosegada. Fuimos los dos hasta un puesto de *burritos*[19] en Haight Street, donde yo pensaba que íbamos a comprar comida para nuestro viaje, pero Julia insistió en llevarle a John. Compramos la comida, fuimos a Toad Hall, y yo aguardé en el coche comiendo mi *burrito*. Poco después salieron los dos y partimos para nuestra excursión.

Yo había creído que para Julia el objetivo era alejarse del ambiente por el que se sentía asfixiada, pero esto lo dejaba todo sin sentido. Parecía que los tres íbamos a tener que pasar una

incómoda tarde juntos, y yo me preguntaba, "¿por qué hace esto?" Durante el trayecto hacia Marin yo iba conduciendo con Julia a mi lado y John en el asiento trasero. Los dos no pararon de intercambiar réplicas mordaces hasta que por fin les interrumpí diciendo: "Haced el favor de tranquilizaros".

Para un extraño la situación puede resultar muy rara, pero los celos nunca han intervenido en mi relación con Julia. A pesar del enfriamiento cada vez mayor de nuestra amistad, John había declarado que él no era celoso, pero yo había acabado por descartar la afirmación como un esfuerzo por ser

políticamente correcto, pues pensaba que estaba actuando de forma posesiva. Tenía claro desde hacía largo tiempo que nada de lo que yo hiciese cambiaría al final la relación entre ellos. Yo quería que Julia pudiera decidir por sí misma lo que quisiera hacer con su vida. Si honradamente no me sentía amenazado, era porque en mi fuero interno creía que la decisión le correspondía a ella, no a mí.

Al llegar a los Headlands aparcamos el coche y salimos andando del Tennessee Valley Trail hacia la playa. Julia y yo habíamos caminado muchas veces por allí, y ahora me puse a

contemplar cómo rompían las olas y a escuchar el oleaje, mientras Julia y John caminaban a lo largo de la orilla. Estaba nublado, ventoso y frío, lo que se sumaba al talante gris que parecía impregnarlo todo. Al final del día regresé a casa de Dan a pasar la noche, solo.

No obstante, a lo largo del par de días que siguieron Julia y yo pasamos un montón de tiempo juntos. Uno de los días hicimos una caminata por las proximidades de Cliff House, en un lugar llamado Land's End, un sitio salvaje al borde del océano, con rocas, leones marinos y majestuosos cipreses.

Disfrutamos de nuestra mutua compañía, y ella empezó a escapar de la situación en la que se había sentido atrapada. Aun así, yo veía que temía provocar la hostilidad de John y me di cuenta de que no podía hacer mucho más para ayudarla. Como yo seguía con ganas de ir a esquiar, lo arreglé con Emily Sklar para volver con ella a la montaña al día siguiente.

Esa noche fui a Menlo Park a visitar a Mark Lottor. Me reuní con él en el aeropuerto de San Francisco, donde entregué el coche alquilado, y a continuación salimos en busca de una comida rápida sin grasa y relativamente

sana. Yo no había abandonado el propósito de correr un montón de carreras de esquí de fondo durante el invierno, así que trataba de comer razonablemente bien, incluso cuando viajaba. Pero después de las diez de la noche en la península, eso resultaba imposible. Finalmente, encontramos un sitio en Redwood City. Yo quería un sándwich de pescado, que como si no hay más remedio, pero no estaba en la carta, de modo que acabé tomando unas patatas fritas. No muy saludable, pero a esas horas no importaba. Cuando llegamos a casa de Mark estaba exhausto, pero él necesitaba su router de

seguridad para protegerse contra el tipo de ataques con manipulación de IP que yo le había descrito y estaba obligado a ayudarle. Estuvimos los dos trabajando hasta el amanecer.

A la mañana siguiente, martes 5 de enero, me desperté sobresaltado a eso de las once y vi que en el busca tenía varios mensajes de Emily, que vive en Palo Alto. Estaba alarmada por no encontrarme y necesitaba coger la carretera para Truckee, donde iba a dar clases de esquí de fondo ese fin de semana.

Diez minutos después se presentó en una camioneta cargada de leña para

calentar la cabaña. Arrojamos mis esquís atrás y partimos hacia la sierra. Por el momento me alejaba de la preocupación por Julia, y me libraba del intruso. Como amigos, Emily y yo nos sentíamos cómodos hablando de toda clase de cosas, y como hija de dos terapeutas, ella poseía útiles conocimientos acerca de la naturaleza íntima de las relaciones. Su sugerencia en este caso fue que me apartase de la situación por un tiempo: consejo que me pareció razonable y que, dadas las circunstancias, era fácilmente practicable.

Llovía durante el trayecto de

ascenso por Sacramento, y a la altura de Auburn, al pie de la montaña, la lluvia se había convertido en nieve. Era inevitable un control de cadenas, pero la tormenta estaba empezando a amainar. Nos detuvimos a por vituallas en Ikeda, un restaurante de comida rápida con tienda de comestibles, al lado de la carretera, donde hay hamburguesas —que yo no como—, pero también buenos batidos de leche, patatas fritas, así como fruta fresca y frutos secos, que sí como. Cuando arribamos a Trucke, compré en el pueblo una pizza para cenar, que estaba fría como una piedra cuando llegamos a la cabaña, quince minutos

más tarde. Como era tarde, desempaquetamos únicamente lo esencial del material para esquiar y del equipo informático. El interior de la cabaña estaba helado, de modo que encendí un fuego, calenté la pizza en el horno y me la comí mientras Emily, que es alérgica a los productos lácteos, se preparaba su propia cena.

El viernes apenas si esquiamos, pero el sábado, cuando finalmente la tormenta acabó, aprovechamos la nieve fresca para pasar el día en las pistas. Fue un gran entrenamiento después de un largo periodo de no hacer ejercicio y dormir poco, y me sentí agradecido por la

oportunidad de olvidar las dos semanas anteriores.

No había comprobado regularmente mi buzón de voz de San Diego porque el teléfono de la cabaña no funcionaba cuando llegamos, pero cuando por fin hice la llamada, había un mensaje telefónico de Becky Bace, una científica informática de la NASA. A esas alturas, la agencia tenía para mí nula credibilidad, debido a su incumplimiento en proveer fondos para un grupo de seguridad informática que me había instado a formar. Pero Becky, mi principal contacto en la sección de seguridad informática de la agencia, que

parecía hallarse atrapada en medio de una organización insensible, seguía tratando de conseguirlos.

Durante meses había estado asimismo tratando de convencerme de que asistiera a la Conferencia sobre Abusos en la Informática y Detección de Anomalías (CMAD en inglés), una reunión anual sobre seguridad informática y la detección de intrusiones, que la agencia copatrocinaba todos los años con el Centro de Guerra Informativa de la Fuerza Aérea. Yo me había estado negando, porque no quería hablar y porque estaba harto de tratar con la

agencia. Pero ella había continuado dorándome la píldora, y ese año, en lugar de celebrarse en el *campus* David de la Universidad de California como las dos anteriores, la conferencia tendría lugar en la Sonoma Mission Inn Spa and Resort[20].

Por lo general las discusiones académicas y teóricas sobre seguridad informática me aburren rápidamente, pero esta vez, con nuestra intrusión reciente, parecía haber una oportunidad de hablar de algo más interesante, y lo que es más, de usar nuestros datos para describir exactamente lo que había sucedido. Una de las áreas de la

detección de delitos informáticos que se halla todavía relativamente en pañales es la de la metodología. Durante cientos de años la gente ha estado investigando delitos de orden físico, y aunque en parte sigue siendo una actividad oscura, existen métodos firmemente establecidos para investigar la escena del crimen y descubrir pruebas. En cambio en el mundo digital todavía hay muy poco en materia de metodología formal de detección.

Llamé a Becky y ella volvió a invitarme a la conferencia. "¿Por qué no vienes simplemente a disfrutar de las aguas termales?", dijo. "Ni siquiera

tienes que dar una charla, simplemente conversar con gente". Yo le dije que no tenía interés en unas vacaciones gratis, pero que ahora pensaba que después de todo podría interesarme asistir y hablar. Ella quedó encantada, y concluyó la conversación diciendo que no había renunciado a la idea del equipo para investigar en seguridad informática, a lo que añadió que estaban a punto de conseguir la aprobación de los fondos. "Sí, claro", respondí yo.

Pero ella estaba dispuesta al menos a pagar mis gastos e incluir unos honorarios. Yo no le había dicho de qué planeaba hablar, sino que lo ultimo que

dije fue que aportaría “una sorpresa”.

Ese día, más tarde, hubo otro mensaje en el buzón de voz del UCSD. Consistió en una melodía, como si alguien estuviese pasando la banda sonora de un *thriller* de suspense que no reconocí. Duró treinta segundos y se cortó abruptamente. Era la clase de música que hace que uno se vuelva para ver si alguien lo acecha. ¿Había alguien? ¿Estaba todavía el intruso allí fuera esperando a que yo bajase la guardia? No tenía cómo saberlo, pero él parecía estar recordándome que no había abandonado la cacería. Si era así, iba a tener que encontrar un truco

todavía más sofisticado para colarse en mi sistema.

Después de irme de San Francisco, Julia y yo hablamos a menudo y no me costó trabajo darme cuenta de que ella necesitaba salir del ambiente en el que se encontraba atrapada, así que la invité a reunirse conmigo en la CMAD. Un balneario de aguas termales le brindaría una oportunidad para desconectar. La conferencia se inició en medio de las mayores inundaciones habidas en un siglo en California, especialmente en el condado de Sonoma. Llegamos a Sonoma Mission Inn en jueves 10 de enero, a tiempo para una recepción

nocturna, y dimos unas vueltas probando comida de un bufé mexicano y charlando con gente a la que no había visto hacía tiempo. Además de profesionales de la seguridad informática había representantes del estamento militar y de la comunidad gubernamental de inteligencia. Estar con gente del mundo del espionaje es siempre una extraña experiencia, porque uno nunca está seguro de que sean quienes dicen ser. En el resto del mundo generalmente hay chequeos de cordura que te avisan cuando estás divagando, pero en el mundo de reserva y fantasía de la inteligencia esas pruebas no existen, y es

fácil que algunas de esas personas se alejen considerablemente de la realidad.

Le presenté Julia a Blaine Burnham, que trabaja en la sección de protección de la información en la NASA. Él le estrechó la mano y sentenció en tono significativo: "He oído muchas cosas sobre usted", como si fuera razonable esperar que alguien que trabaja en una agencia de espionaje poseyera un expediente de cada una de las personas presentes en un cóctel. Ella se puso inmediatamente en guardia y desconfiada, y rápidamente nos apartamos.

El mundo de la seguridad

informática es en realidad una comunidad notablemente cerrada y endogámica, y muchos de los grandes nombres en el ambiente estaban en la conferencia. No es un mundo del que yo forme parte directamente, sino en el que me gusta aparecer de vez en cuando, dejar caer unas bombas y alejarme. El problema de las conferencias como CMAD es que son en general representativas del triste estado de la seguridad informática. En cualquiera de estos acontecimientos, los asistentes se inclinan casi siempre por enterrar la cabeza en la arena y negarse a reconocer que perciben una creciente sofisticación

en los ataques. Son numerosos los usuarios poseedores de sistemas informáticos anticuados que, en lugar de realizar modificaciones básicas para hacerlos más seguros, deciden comprar una caja negra que, colocada entre sus ordenadores y el mundo exterior, les proporciona la ilusión de estar protegidos. Como resultado, se gasta un montón de dinero en sistemas "detectores de intrusiones" automatizados, derivados de un software de inteligencia artificial que busca lo que sospecha es un "comportamiento anómalo" de parte de un usuario y suelta la alarma. También se invierten muchos

esfuerzos en tratar de reemplazar a los muy costosos funcionarios de seguridad que actualmente examinan los registros, por un programa que intente desarrollar las mismas funciones.

Nos encontramos con Bill Cheswick, el investigador de Laboratorios Bell que unos años atrás había vigilado a Adrian/Berferd y que es un reconocido experto en protección de ordenadores. Yo lo conocía a través de conversaciones telefónicas y del correo electrónico, pero nunca nos habíamos encontrado personalmente. Tiene una cara redonda, cabello rizado, y es algo robusto sin ser realmente grueso. Le

gasté una broma sobre su presencia en aquel sitio elegante y él me respondió que era más divertido que estar clavado en su despacho de Nueva Jersey en mitad del invierno.

Siempre he experimentado un gran respeto hacia Ches —como le llaman—, que tiene un gran sentido del humor y mucho entusiasmo. Los dos nos habíamos criado en el ambiente de los fanáticos de la informática, en el que un juego de aventura llamado Zork fue uno de los primeros basados en un texto que surgieron en los ordenadores de gran formato a fines de los setenta. Como muchos de esos juegos, Zork creó una

serie de imaginarias cuevas subterráneas a través de las cuales uno cazaba pulsando en el teclado unas órdenes que significaban Este, Oeste, Norte, Sur, Arriba y Abajo. No tenía gráficos, pero eso realmente no importaba, puesto que los mejores gráficos son los que están en nuestra cabeza. La moneda de Zork eran los Zorkmids, y fue Ches quien me inició en la noción de pensar en los Zorkmids como representación genérica del dinero, en lugar de los dólares. Según su razonamiento, hay demasiada emoción vinculada a los dólares, pero no a los Zorkmids. Las personas podían ser avaras con los dólares, pero nunca con

los Zorkmids. Ches había señalado (sólo en parte en broma, creo) que para los hackers las grandes empresas servían para suministrar los suficientes Zorkmids como para poder continuar jugando al Zork.

Ches fue asimismo autor del texto más importante en seguridad informática sobre los firewalls, escrito con Steve Bellovin, quien, irónicamente, fue también el autor del influyente artículo que describió el ataque IP-spoofing en 1989. Ches me comentó que en su propia intervención de aquel día había mencionado el tema, señalando que nunca había sido visto "al natural".

Otra persona con quien me encontré esa primera noche fue Tom Longstaff, uno de los mejores técnicos integrantes del Equipo Informático de Respuesta de Emergencia, una organización financiada por el Gobierno con base en la Carnegie Mellon University, de Pittsburgh. El CERT, como se le conoce, fue formado en 1989 tras el episodio del microbio de Robert Tappan Morris en Internet. Su misión es reunir y propagar información oportuna sobre problemas de seguridad relativos a Internet, pero tienden a operar con unas precauciones burocráticas que contradice lo de la "Emergencia" del título. Siempre he

tenido la sensación de que él es una persona que quiere hacer lo correcto pero con frecuencia tiene las manos atadas por la organización para la que trabaja. Yo había intentado ponerme en comunicación con él en diciembre, después del ataque a mis sistemas, pero no nos habíamos encontrado. Al describirle el ataque con manipulación del IP quedó claramente intrigado, y yo le prometí que le daría la descripción técnica completa en mi charla del día siguiente.

A la mañana siguiente me presenté abajo con mi RDI PowerLite y mi piolet.

El ordenador portátil tenía mis notas para la charla, y de hecho iba a utilizar el hacha de hielo como puntero para hacer comprender mi afirmación de que las herramientas son sólo herramientas. No iba a referirme al piolet, sino que esperaba en cambio que su mera presencia hiciera preguntarse a la gente para qué era aquella herramienta, y puede que captaran mi idea. Yo había querido conectar mi ordenador directamente a un proyector y al sistema audiovisual del hotel, pero los organizadores de la conferencia no habían podido encontrar ningún equipo audiovisual en tan corto tiempo. Estaba

programado que yo interviniese después del primer descanso, y durante éste me las arreglé para crear unas transparencias a partir de las cuales hablar, aunque en su mayor parte eran sólo tomas cinematográficas de directorios o listas de comandos.

Titulé mi charla "Lo que hice durante mis vacaciones de Navidad", un chiste implícito para quienes me conocían. No soy una persona que de mucha importancia a la Navidad, a la que suelo referirme como "descanso invernal".

Aun cuando el tema de la manipulación del IP estaba posiblemente

obsoleto, sentí que el interés en el recinto aumentaba, porque yo era el primero que en la reunión describía un ataque real y no un problema teórico de seguridad informática. Yo quería mostrar cómo había sido llevada a cabo la investigación, describiendo con detalle cómo había seguido la pista. Señalé que el ataque parecía seguir un guión o estar automatizado, basándome en el cálculo del tiempo de ocurrencia de los hechos que nosotros habíamos realizado. Había sido un factor importante, pues si el ataque estaba empaquetado como programa, era probable que pudiera ser utilizado por

personas sin una cualificación técnica especial, que simplemente formaran parte de la red de boletines de anuncios y sistemas de conferencia de Internet del submundo informático que trafica con esa clase de información. No se trata de que exista una conspiración muy bien organizada ahí fuera; es sólo que los piratas hablan entre sí y no están constreñidos por las reglas de una burocracia con mentalidad de "cubrirse". Su existencia asegura que cualquier nueva debilidad o fallo de seguridad que se descubre es conocido por el bajo mundo informático con mucha mayor rapidez que por el ámbito

oficial de la seguridad informática, donde la gente no se comunica con la misma eficacia.

El hecho de que reconstruir la intrusión me hubiera exigido una gran cantidad de análisis detallado fue algo que claramente impresionó a la audiencia. La situación que yo describía era el tipo de ataque que podría haber estado ocurriendo todo el tiempo bajo sus propias narices sin ser detectado. La implicación de mi charla era que la gente puede tener enormes candados en las puertas, pero entre la puerta y el suelo existe un estrecho espacio por el que los delincuentes pueden deslizarse

tranquilamente.

A continuación hice escuchar los dos mensajes del buzón de voz que había almacenado como archivos digitales en mi ordenador agenda. Cuando el altavoz del ordenador emitió aquel acento desagradable, la distorsión era tal que era difícil discernir las palabras exactas, pero la gente captó la idea de que alguien me había escogido deliberadamente. Muchos profesionales de la seguridad informática han metido de tal forma la cabeza en la arena que han olvidado que los verdaderos enemigos está ahí fuera. “Yo y mis amigos, te liquidaremos”. Delante de

una audiencia de profesionales de la informática, aquella voz resultaba escalofriante. Hubo silencio en la sala mientras yo esperaba que me hicieran preguntas.

Mi argumento era que se trataba de una vulnerabilidad que afectaba a buena parte de Internet, debido a lo mucho que la red confiaba en una autenticidad basada en las direcciones. Si yo envío, por ejemplo, un mensaje por correo electrónico, ¿cómo sabe el receptor que el remitente soy realmente yo? Es lo mismo que si uno recibe una postal por correo: puede que reconozca la escritura, pero es el único indicio en el

que fundarse para discernir si el mensaje ha sido falsificado. El método de las direcciones que subyace en Internet no fue en ningún momento pensado como elemento de autentificación. Es posible burlarlo de muchas maneras haciéndose pasar por un ordenador conocido. La función de Internet es simplemente la de asegurarse de que los paquetes van de aquí para allá, no la de proporcionar autenticación, y aquel ataque demostró que el sistema era demasiado vulnerable a la subversión. Sencillamente, confiamos en que la dirección es correcta y el remitente aquel que dice

ser. El ataque a mis máquinas demostraba que el carácter elemental de los protocolos de Internet, que sustentan básicamente las comunicaciones por la red, los convierte en sumamente abiertos y susceptibles de abusos. Impedir por completo ese tipo de subversión requeriría una reelaboración exhaustiva de aquellos protocolos básicos.

La última pregunta formulada desde la audiencia fue: "¿Tiene usted alguna idea de quién le hizo eso?"

"En realidad, no", repliqué.

Después de la sesión se me acercó una mujer que se presentó como Martha Stansell-Gamm. Yo la recordaba de un

suceso ocurrido años atrás relacionado con el cumplimiento de la ley. Con el cabello rubio atado en un moño detrás de la cabeza y vestida de forma muy conservadora, Marty tenía el aspecto de alguien práctico y eficiente. Trabajaba en la unidad contra el delito informático del Departamento de Justicia y me preguntó si le había comunicado el ataque sufrido por mí al FBI. Le dije que no, y le expliqué que en el pasado no había tenido mucha suerte en mis tratos con el Bureau. Ellos habían mostrado desinterés y, por tanto, esta vez no se me había ocurrido el llamarles.

"Me sorprende oír eso, Tsutomu",

dijo ella. “Me ocuparé de que en lo sucesivo seamos más receptivos”. Prometió hacer que alguien hablase conmigo sobre el incidente. Por más que dijo que no había sido capaz de seguir todos los detalles técnicos de mi descripción, tuve la sensación de que poseía una mente alerta y de que no iba a actuar como un burócrata.

Tras la charla con Marty tropecé con Jim Settle, un fornido agente del FBI que estuvo al frente del equipo de delitos informáticos del Bureau. Lo había abandonado y ahora trabajaba para I-Net, un contratista de seguridad informática de la zona de Washington

D.C. En 1991, cuando él estaba aún en el Bureau, yo había intervenido en una de sus sesiones de entrenamiento para agentes y les había mostrado mis cintas de Adrian para que se hicieran una idea de cómo es un ataque. En aquella ocasión tuve la impresión de que quedaba algo desconcertado y no sabía cómo catalogarme. Ahora se mostró amistoso y dijo que pensaba que tal vez él tuviese alguna idea sobre quién estaba detrás del ataque. Yo mencioné el software telefónico Oki y comenté nuestras sospechas de que se tratase de Kevin Mitnick porque estábamos bastante seguros de que él había

intentado robárselo a Mark Lottor. Pero Settle dudaba de que fuera Mitnick, debido a la competencia técnica necesaria, y en cambio sugirió que podrían ser algunos piratas informáticos de los que había oído hablar operando fuera de Filadelfia.

Después de mi intervención, mientras hablaba con integrantes de la audiencia, empecé a darme cuenta de que los asistentes a la conferencia parecían tomarse seriamente aquella vulnerabilidad, pero presentí que no sería fácil que sus respectivas organizaciones hicieran lo mismo. Tuve una larga charla con Tom Longstaff,

quien reconoció que el IP-spoofing era un problema importante pero que dudaba de poder persuadir al CERT de emitir una advertencia, debido a la política en torno a la cuestión de dar publicidad a las vulnerabilidades. Como agencia financiada por el Gobierno, el CERT siempre había sido tremendamente conservador y temeroso de ofender a alguien. Si emitía una advertencia sobre el peligro de la manipulación de direcciones tendría que mencionar los nombres de los fabricantes cuyos equipos fueran vulnerables, un paso políticamente muy delicado.

Más tarde, después de la cena y de

abundantes libaciones, estaba yo hablando con Bill Cheswick y Marcus Ranum —otro eficaz especialista en seguridad informática— sobre la pasividad del CERT, y Marcus planteó la idea de no esperar al CERT, sino adelantarse a publicar los detalles de la vulnerabilidad por nuestra cuenta. Vi a Longstaff y me acerqué a él.

"¿Qué harían ustedes si lanzásemos un boletín falso del CERT detallando el problema y advirtiendo sobre el mismo?", le pregunté.

"Supongo que tendríamos que efectuar una rectificación", replicó, para luego añadir, con una sonrisa: "Si el

texto es realmente bueno, puede que simplemente lo distribuyésemos".

Me explicó que una buena falsificación sería verdaderamente difícil porque el CERT firmaba digitalmente cada boletín con un número de identificación generado mediante el PGP[21], el sistema criptográfico creado por Philip Zimmermann. Yo señalé que aun cuando todo el mundo supiera que era una falsificación, un anuncio apócrifo lograría el mismo efecto de alertar a la gente sobre el problema. Al final de nuestra conversación tuve la impresión de que a Longstaff no le importaría que lo intentásemos, pero que

no había forma de que fuera a alentamos a hacerlo.

Julia y yo hicimos novillos durante buena parte del último día de la conferencia, porque el estar en la Sonoma Mission Inn era una ocasión demasiado buena para desperdiciarla pasando todo el tiempo en un oscura sala de reuniones. Donde sí estuve fue en una charla que dio Marty sobre cómo la Ley de Telefonía Digital, firmada por el presidente Clinton el pasado octubre, había otorgado a los usuarios del servicio online y a los proveedores de Internet la posibilidad de monitorear el tecleado de las personas que se

comunicaban a través de sus sistemas. Era un anatema para los grupos defensores de los derechos a la intimidad, pero una herramienta importante que resultaba absolutamente vital para rastrear intrusos.

Por la tarde decidimos meternos en los baños calientes, y volvimos a encontrarnos con Marty. Para entonces su aspecto no tenía nada de conservador, con su bañador azul de una pieza. De entrada estuvo un tanto cohibida porque, al igual que nosotros, sabía que la conferencia no había terminado aún, pero igual que nosotros estaba probablemente muerta de aburrimiento.

Nos explicó que estaba tomando aquel baño para sentirse plenamente relajada, porque iba a volar directamente a su casa, en Washington, donde tendría que lidiar con sus hijos, incluido un bebé enfermo, y con su esposo, que estaba cansado de cuidar a la familia en su ausencia.

Llovía ligeramente, con lo que toda la zona de aguas termales cobraba un estupendo aspecto neblinoso. Charlamos sobre las intervenciones del día. Marty dijo que en febrero el Departamento de Justicia planeaba un seminario en San Diego sobre las cuestiones legales relativas al delito informático. El

departamento quería reunir a todos los ayudantes de fiscal a quienes había adjudicado responsabilidades en la materia. Me invitó a una de las sesiones y yo dije que estaría encantado de asistir y hablar de tecnología.

Aunque la lluvia empezó a caer con fuerza, estábamos demasiado a gusto como para movernos, y a través de la neblina de Sonoma nos pusimos a hablar del ataque a mis ordenadores. Marty no podía entender por qué no éramos más activos en la revisión de lo que teníamos registrado del tráfico de paquetes, procedente de Ariel. "Recogimos interesantes indicios apuntando a sitios

como la Colorado SuperNet y la Universidad Loyola de Chicago", le dije. "Pero no tenemos recursos, así que no he podido seguir adelante con nada". Le expliqué que había estado meses tratando de reunir un equipo de investigación en seguridad informática, pero había quedado completamente empantanado por la demora de la NSA en proveernos de fondos. "Estoy cansado de darme de cabeza contra la burocracia y no llegar a ninguna parte", dije. "Estoy harto".

"Pero Tsutomu, este es un ámbito legal nuevo", replicó ella. "Es importante que encontremos casos que

sirvan de prueba y los sigamos hasta el final para sacar algún provecho".

La conferencia estaba casi por terminar y los tres decidimos que debíamos hacer una última aparición en la clausura. Mientras salíamos de los baños me volví y dije: "Me encantaría avanzar en este asunto, pero no tengo pruebas concluyentes. Basado en los datos tomados sospecho que Kevin Mitnick podría estar detrás de esto. Pero carezco de pruebas convincentes. Y por lo que sé, este tipo de ataques se encuentra verdaderamente más allá de su capacidad técnica".

7. Se presenta la prensa

A última hora de la tarde del martes Julia y yo abandonamos la conferencia CMAD, y en el camino de regreso a San Francisco nos detuvimos en Fairfax a visitar a un amigo suyo. Continuaba lloviendo, y yo seguía lamentándome por la nieve de las sierras sobre la que no iba a esquiar, pero por el momento me distraía de la idea el hecho de que el mundo a nuestro alrededor se había transformado en un paisaje fantástico

envuelto en vapor. Para quien ha crecido en el este, buena parte de California tiene siempre un característico aspecto de árido desierto, excepto en lugares como el condado de Marin, donde, al culminar la estación de las lluvias, el mundo se vuelve de un resplandeciente verde esmeralda.

Durante la hora del trayecto hasta Fairfax estuve pensando en la conversación que había tenido con Tom Longstaff acerca de si el CERT emitiría un boletín sobre el IP-spoofing. ¿A quién creía ayudar esa gente omitiendo pasar ese tipo de información a los encargados de sistemas? De todas

formas, lo más probable era que en el curso de un mes los detalles de la violación se hubieran difundido ampliamente por el submundo informático, haciendo inevitables los ataques de los imitadores. Las únicas personas no enteradas serían los responsables de proteger la seguridad de los ordenadores en Internet.

"Es una estupidez", pensé, aunque al parecer yo no podía hacer nada al respecto. Y hasta cierto punto, no era problema mío. Yo me había presentado ante algunos de los principales expertos en seguridad informática del país para hacer un informe preciso sobre el

mecanismo del ataque. Ahora el CERT pretendía obrar sobre CERTezas, actuando con lentitud y cautela, y si yo me sentía frustrado, era debido a una situación desgraciadamente típica.

Tras una comida mexicana en Fairfax, continuamos hacia San Francisco a recoger el coche de Julia, un Mazda descapotable que había estado varios meses aparcado delante de Toad Hall mientras ella hacía *trekking* en Nepal. Ella me siguió hasta el aeropuerto para deshacernos del Oldsmobile alquilado, y en el camino de regreso el motor del Mazda empezó a hacer un ruido ominoso. Llegamos a

duras penas y pasamos la noche en casa de Dan Farmer.

A la mañana siguiente comprobé el aceite, que ni siquiera produjo marca en la varilla, de modo que llevamos despacio el coche a un sitio en Divisadero donde hacen cambios de aceite en el momento. Más tarde supimos que John había prestado el coche a cantidad de gente mientras Julia estaba fuera, y que nadie se había molestado en hacerle el mantenimiento. Ella se puso lívida de rabia. Aunque el Mazda tenía más de 80.000 kilómetros encima, ella siempre lo había cuidado, pero ahora el motor sonaba como si se

hubiera estropeado definitivamente.

A partir de ahí el motor sonaba mal pero siguió funcionando, de modo que cargamos las cosas de esquiar y partimos, con la esperanza de superar el tráfico de los viernes de esquí hacia las montañas. En la cabaña, el sendero de acceso estaba cubierto de nieve fresca, y aunque pasamos media hora paleando antes de poder aparcar el coche, yo estaba contento porque finalmente iba a poder esquiar un poco.

Los tres días siguientes fueron de pura liberación, y Julia y yo esquiamos y hablamos, y pasamos las veladas en copiosas cenas junto con Emily.

Pero el martes por la noche recibí un mensaje telefónico de Tom Longstaff. A la mañana siguiente lo llamé y él me dijo que se habían producido nuevos ataques en Internet, utilizando el truco de la manipulación del IP.

"¿Contra qué objetivos?", pregunté.

"Tsutomo, lo siento, pero ése es un tipo de información que el CERT no divulga. No puedo decírselo".

"Bien, enfoquémoslo de otra forma. ¿Qué tal si le digo *de dónde* han procedido los ataques?". Comprobé mis notas y dije: "Apuesto a que esos nuevos ataques han venido de *apollo.it.luc.edu* en la Universidad Loyola de Chicago".

Estaba en lo cierto —coincidía—, y le pregunté cómo había ocurrido.

Como en el caso del portal abierto entre Osiris y Ariel, habían secuestrado la sesión de alguien. Pero en esta ocasión el usuario había estado sentado a su máquina y vio que alguien se había apoderado de su sesión. El responsable de su red, a quien se había alertado de que el ataque estaba en marcha, pudo capturar todos y cada uno de los paquetes de datos del intruso. Esa información le permitió reconstruir el ataque con exactitud.

Le pregunté a Tom si aquel nuevo incidente había hecho que el CERT

cambiase de opinión, y si estaban ahora dispuestos a sacar un boletín de advertencia. Él sólo dijo que todavía lo estaban considerando, pero estaba implícito que por fin podría haber munición suficiente con la que actuar.

Después de colgar me puse a pensar en lo que los nuevos ataques podían significar. Parecía claro que el ataque IP-spoofing representaba una grave vulnerabilidad para toda la comunidad de Internet. Había miles de emplazamientos informáticos en los que la confianza entre dos ordenadores de una red local era un hecho conveniente y establecido, y ahora todos ellos estaban

en peligro. Yo no podía esperar más tiempo preguntándome cuándo el CERT iba a tomar medidas. Se trataba de algo que la gente debía saber. Pero ¿cómo hacerlo? Me acordé de que John Markoff, del *Times*, me había pedido que lo llamara cuando me enterase de algo que pudiera constituir una historia interesante. A partir de nuestra primera charla en 1991 a propósito de Adrian, Markoff y yo habíamos intercambiado regularmente información sobre la seguridad informática e Internet. Unos años antes nos habíamos conocido personalmente en una de las conferencias de los hackers y habíamos

descubierto que a los dos nos gustaba andar por lugares despoblados, y habíamos hecho juntos un par de largos recorridos en esquí por las zonas rurales. Markoff acabó apoyándose en mis conocimientos técnicos al escribir sobre temas como Internet y la criptografía, y yo encontraba en él una aprovechable fuente de noticias y chismes. Me había dicho que lo que le interesaba no eran las historias de delitos informáticos corrientes sino sólo los casos en los cuales estuvieran implícitas cuestiones más importantes, como el del pirata holandés que operaba fuera del alcance de las leyes

estadounidenses. El IP-spoofing, que era una insidiosa debilidad en la estructura básica de Internet, parecía un tema perfectamente adecuado. Me figuré que, aunque el CERT estuviese limitado por sus normas organizativas, yo era libre de hablar acerca de mi intervención en la conferencia. Eran más de cincuenta las personas que habían asistido a mi charla de la CMAD y cualquiera de ellas podía habérsela comentado a un periodista. Daba igual que yo por mi parte llamase a uno.

Localicé a Markoff en su oficina y tras contarle mi intervención en la CMAD, le expliqué brevemente lo del

ataque IP-spoofing. Le advertí que el CERT estaba todavía considerando si emitía un comunicado, y que probablemente él debería llamarlos para preguntar cuándo lo iban a publicar. Convinimos en que no le diría a la gente del CERT quién le había hablado de mi informe, aunque era improbable que eso se plantease, puesto que él conocía al menos a media docena de los asistentes a la conferencia.

Dos días después, el jueves 19 de enero, Marty Stansell-Gamm llamó para decir que había dado al FBI instrucciones de ponerse en contacto conmigo. Al día siguiente, Richard Ress,

un agente del FBI en Washington, me dejó un largo mensaje preguntando por el ataque a mis sistemas y disculpándose por mis problemas con el Bureau en el pasado. Cuando le devolví la llamada, retomó el hilo a partir del final de su mensaje previo y me soltó un rollo de cinco minutos sobre las dificultades que había encontrado el FBI para afrontar la cuestión de los delitos informáticos y cómo iban a cambiar la forma de tratar el tema. Reconoció que el Bureau se daba cuenta de que no me había prestado atención en el pasado y dijo que ahora querían hacer todo lo posible por colaborar en el futuro. Sonaba

estupendamente, pero yo ya había escuchado antes promesas semejantes.

Ese mismo día, más tarde, Andrew habló con Marty y después con Levord Burns, el principal agente operativo del FBI sobre delitos informáticos. Yo había trabajado con Burns en anteriores casos de intrusiones y le consideraba un buen agente de la ley en el puesto equivocado, porque sabía poco de ordenadores y de tecnología. Andrew le había descrito en su llamada los detalles de nuestra situación y luego le había enviado un fax esbozando en términos generales lo que habíamos averiguado.

Durante la semana, Markoff había

estado trabajando en su artículo y negociando con el CERT acerca de cuándo se publicaría. Al final, ante el argumento de los funcionarios del CERT de que su publicación en viernes daría a los intrusos un fin de semana completo en el que operar mientras los responsables de las redes estaban alejados de sus respectivos sistemas, Markoff aceptó postergarla.

El sábado salí tarde a esquiar. Oscurecía, y la nieve estaba dura, lo que significaba esquiar muy rápido. Sólo los más rezagados se hallaban aún en las pistas más pendientes del ventisquero de Tahoe Donner, y estuve solo durante la

mayor parte del tiempo. Mientras esquiaba se me ocurrió que en la NSA iban a sentirse desconcertados con la publicación del artículo en el *Times*, porque cualquier publicidad suele resultarles ofensiva. Me detuve brevemente en un refugio y llamé a Becky Bace para ponerla sobre aviso, figurándome que con su talante independiente puede que todo el asunto le resultase divertido. En un campo que se distingue por la ausencia de mujeres, ella se refiere a veces a sí misma como "la madre de la seguridad informática". A los treinta y nueve años, da la impresión de haber estado en el

ambiente tanto tiempo como para constituir una especie de parte integral del mismo y conocer a todo el mundo.

La llamé a su casa y, como había sospechado, le divirtió mucho la perspectiva de que la CMAD recibiese un poco de atención. "Fabuloso" comentó; una oscura reunión académica que jamás despierta el menor interés fuera de una reducida comunidad de intelectuales, militares y gentes de los servicios de inteligencia; y de pronto una ponencia presentada en ella va a ser recogida por el *New York Times*. En medio de la decreciente luz del anochecer me fui esquiando a casa

preguntándome cómo acabarían saliendo las cosas.

El artículo de Markoff, que el *Times* dio a conocer en su servicio cablegráfico el domingo por la noche, se publicó en lugar destacado en la primera página del periódico el lunes.

RED INFORMÁTICA EXPUESTA A NUEVA AMENAZA

por John Markoff, especial para el *New York Times*

SAN FRANCISCO, enero 22 —Una agenda federal de seguridad informática ha descubierto que unos

intrusos desconocidos han desarrollado una nueva forma de introducirse clandestinamente en sistemas informáticos, y la agencia planea aconsejar el lunes a los usuarios cómo protegerse ante el problema.

La nueva forma de ataque hace que 20 millones de ordenadores del Gobierno, de empresas, universidades y hogares sean vulnerables al fisgoneo y al robo. Los funcionarios afirman que a menos que los usuarios adopten las complejas medidas que se les indicarán, los intrusos podrían

copiar o destruir documentos, e incluso operar sin ser descubiertos haciéndose pasar por un usuario autorizado del sistema.

Para los usuarios de ordenadores, el problema se asemeja al de unos dueños de casa que descubren que los ladrones tienen llaves maestras de todas las puertas de calle del barrio.

El primer ataque empleando la nueva técnica que se conoce tuvo lugar el 25 de diciembre contra el ordenador de un conocido experto en seguridad informática en el Centro de Superordenadores de San Diego.

Uno de sus ordenadores estuvo más de un día en manos de un desconocido o desconocidos que robaron electrónicamente un gran número de programas de seguridad que su dueño había desarrollado.

Desde entonces se ha informado de varios ataques, y no hay forma de saber cuántos otros pueden haber ocurrido. Funcionarios del Equipo Informático de Respuesta de Emergencia o CERT, financiado por el Gobierno, manifiestan que los nuevos asaltos constituyen una advertencia de que habrá que adoptar mejores medidas

precautorias antes de que el comercio llegue a Internet, una red mundial de ordenadores interconectados que intercambian mensajes, documentos y programas de ordenador electrónicos.

El artículo continuaba identificándome por mi nombre y haciendo referencia a mi charla en la CMAD. Unos años antes, una historia de esta clase, en caso de aparecer, lo haría sepultada en las últimas páginas, pero ahora Internet se había convertido en noticia importante.

Aunque el CERT le había dicho a

Markoff que su propio comunicado sería publicado el lunes por la mañana, el documento, que hacía referencia a los ataques y resumía las medidas defensivas que los responsables de sistemas informáticos debían tomar, no circuló hasta las 2:30 de la tarde, hora del este: casi diecinueve horas después que la historia del *Times* difundida por su servicio cablegráfico. Ese retraso provocó una general consternación en muchos encargados de sistemas, sorprendidos al enterarse de puntos débiles en la seguridad de Internet por los medios de comunicación. No obstante, el hecho de que un asusto

relativamente confuso como el ataque IP-spoofing fuera de repente un tema de primera plana tuvo un efecto colateral beneficioso: habitualmente, las recomendaciones del CERT van a unos administradores de sistemas que de ordinario están demasiado ocupados para hacerse cargo de los problemas, pero en este caso fueron los más altos ejecutivos de las empresas los que se enteraron de la vulnerabilidad de una forma entendible por ellos, con lo que hubo presión de arriba a abajo.

Más tarde descubrí la razón del retraso del CERT. El grupo había hecho circular un borrador del comunicado

antes de pronunciarse públicamente sobre el problema, el cual resultaba confuso para mucha gente que no podía entender cómo el ataque IP-spoofing se diferenciaba de otra clase de problemas denominados “ataques a la fuente de distribución”. Estos últimos implican una vulnerabilidad semejante a la del ataque IP-spoofing que permite a un atacante abrir un sendero a través de Internet para asegurarse que cada paquete de datos procedente de una máquina-blanco pase primero por un ordenador atacante. Al tratarse de una debilidad tan conocida, muchos ordenadores distribuidores de tráfico en

Internet ya no permiten ese procedimiento. De ahí que el CERT necesitara un tiempo extra para revisar el comunicado final.

El documento del CERT, que agradecía a Bellovin, a Cheswick, a mí y a otras tres personas su contribución a la comprensión del problema, comenzaba por una introducción de tres párrafos:

23 Enero de 1995

ATAQUES CON MANIPULACIÓN DEL IP Y CONEXIONES TERMINALES

ATACADAS

El Centro de Coordinación del CERT ha recibido informes de ataques en el que los intrusos crean paquetes con direcciones de fuente IP falsas. Estos ataques sacan partido ilegal de aplicaciones que emplean una verificación basada en direcciones IP. Este abuso conduce al usuario y posiblemente al acceso a la raíz del sistema tomado como blanco. Nótese que este ataque no implica distribución de fuentes. Las soluciones recomendadas se describen en la Sección III del

presente documento.

En el actual esquema de ataque, una vez obtenido el acceso raíz, los intrusos pueden modificar dinámicamente el núcleo de un sistema Sun 4.1.X. En este ataque, que es independiente del ataque IP-spoofing, los intrusos emplean una herramienta para hacerse con el control de cualquier terminal abierta o sesión de registro de los usuarios del sistema. Nótese que aunque la herramienta se está utilizando en este momento principalmente con los sistemas SunOS 4.1.x, los elementos de un sistema que posibilitan este

ataque no son exclusivos del SunOS.

A medida que recibamos información adicional relacionada con este comunicado, la transmitiremos, y sus archivos README asociados están disponibles en FTP desde *info.cert.org*. Os aconsejamos revisar regularmente los archivos README para manteneros al día sobre los comunicados que os conciernen.

El día en que apareció el artículo en e l *Times*, el SDSC se inundó de llamadas telefónicas. Cuando Robert

Borchers, el director de programas de la Fundación Nacional para la Ciencia para los cinco centros de superordenadores —en otras palabras, el santo patrón del SDSC— llamó para saber qué estaba pasando, la persona que atendió el teléfono no sabía quién era, de modo que lo puso con la encargada de relaciones públicas, que tampoco reconoció el nombre. Borchers fue pasando por una cadena de funcionarios del SDSC que tenían instrucciones de no revelar nada, hasta que por fin consiguió dar con Sid. El hombre no estaba muy contento, pero afortunadamente posee sentido del

humor.

A media mañana el SDSC había recibido más de cuarenta llamadas sólo de los medios de comunicación, y yo acabé empleando buena parte del día en mi cabaña contestando a periodistas y personas de la comunidad de Internet ansiosa por saber más sobre el incidente. Hablé por teléfono con Associated Press, Reuters, *USA Today, The Wall Street Journal* y el *Philadelphia Enquirer*, y por correo electrónico con la CNN, una cadena de noticias que siempre he admirado porque es difícil sesgar tus declaraciones cuando te están viendo en

todas partes del mundo. Me ocupé de esos medios y otros más, y le pedí a Ann Redelfs, la encargada de relaciones públicas, que atendiese al resto. Steve Bellovin, el investigador que había escrito el informe original en el que describía los ataques IP-spoofing, pidió más detalles por correo electrónico. Pero también recibí mensajes de muchos ignorantes fabricantes de productos de seguridad informática que, aunque sin la menor idea de qué era un ataque IP-spoofing, se mostraban completamente seguros de que su hardware o software nos protegería. Es muy fácil proponer soluciones sin saber cuál es el

problema.

Por lo que llegó a mis oídos, hubo mucha gente inquieta por la situación entre el personal del Centro, por creer que lo peor del mundo era que una violación de la seguridad apareciese en la primera página del *New York Times*. Sid también estaba preocupado por la publicidad negativa, pero en general se tomó bien el asunto, y me dijo que lo único que lamentaba era no haberlo notificado antes a Bob Borchers. En cuanto a mí, era una buena noticia que hubiera sido capaz de calcular lo que había ocurrido, en contraste con los numerosos casos en los que

probablemente los sistemas habían sido violados sin que sus responsables se enterasen siquiera.

Salí por la tarde a esquiar un poco y a mi regreso Julia y yo resolvimos que con su ayuda —la redacción técnica es una de sus dotes— yo debería escribir algo que describiese detalladamente el ataque en términos técnicos. La cabaña estaba llena de esa luz gris de los atardeceres de mediados del invierno. Afuera nevaba ligeramente, difuminando las luces del telesquí que cruzaba el valle, discernible a través del ventanal del salón. Ninguno de los dos se había molestado en levantarse para encender

las pocas luces que había en la cabaña y yo estaba sentado a la mesa del comedor inclinado ante el débil resplandor de la pantalla de mi ordenador portátil.

Mi busca zumbó, lo cual me sorprendió, porque nunca antes había recibido una llamada en la cabaña, y en cualquier caso yo siempre había supuesto que estaba fuera de alcance. Extendí un brazo, lo cogí, y en la penumbra observé atentamente la pantalla.

Los dígitos eran 911911, o sea, el código de emergencia, repetido.

"Es raro", le dije a Julia, mostrándole la diminuta pantalla. Lo

devolví a su lugar. Unos segundos después volvió a zumbar, y nuevamente aparecieron los seis dígitos.

¿Por qué me buscaría alguien con el 911? Nos miramos en la creciente penumbra. Casi nadie tenía mi número de busca, que cambio con frecuencia, pero entre los archivos robados había una "imagen" de sostén de la memoria contenida en mi teléfono móvil, en la cual había un directorio que incluía mi número de busca. ¿Se trataba de otro aviso de la misma persona que me había estado dejando crípticos mensajes? Coloqué el localizador sobre la mesa y lo estuve observando: más o menos cada

medio minuto zumbaba como un sonajero sobre la dura superficie durante diez o quince segundos, mostrando cada vez aquella misma inquietante hilera de dígitos, 911911, como si alguien me estuviera advirtiendo que pidiese ayuda. Allí estábamos, en medio de las sierras, en una remota cabaña: si sabían el número de mi busca, ¿qué más conocían?

Llamé a PageNet, la empresa de localizadores a la que estoy suscrito, para decirles que alguien me estaba presionando y pedirles que intentasen rastrear las llamadas telefónicas. Julia y yo observamos que el busca continuaba

sacudiéndose sobre la mesa, hasta que finalmente yo estiré la mano y lo apagué. No tenía miedo, sólo la sensación inquietante de que ahora alguien, si quería, podía realmente acosarme.

No empezamos a escribir hasta eso de la diez de la noche, después de cenar, pero hacia las 3:30 de la mañana tuvimos un detallado documento, que me propuse remitir por Usenet. A diferencia del comunicado del CERT, que omitía cuidadosamente mencionar por su nombre a las organizaciones que habían sufrido ataques, yo no iba a cambiar los nombres para proteger a los culpables.

Usenet, que precedió por pocos años

a Internet, comenzó como un anárquico sistema de transmisión de mensajes para muchos de los ordenadores del mundo basados en Unix, que originalmente se conectaban principalmente mediante líneas telefónicas regulares y modems. Desde el principio, Usenet se organizó en grupos de noticias donde la gente podía poner y leer mensajes correspondientes al tema elegido por el grupo. Actualmente existen más de doce mil grupos diferentes donde la gente puede discutir sobre todos los temas imaginables. Yo planeaba, cuando estuviese en San Diego, remitir mi informe a tres archivos en los que

normalmente se discutían asuntos de seguridad: *comp.security.misc*, *comp.protocols.tcp-ip* y *alt.security*.

El título de mi mensaje fue "Detalles técnicos del ataque descrito por Markoff en el NYT". Comenzaba: "Saludos desde el lago Tahoe. Parece que hay abundante confusión acerca del ataque IP-spoofing a direcciones y los ataques de copamiento conexos descritos en el artículo de John Markoff en el NYT del 23/1/95 y el comunicado del CERT CA-95:01. Adjunto algunos detalles técnicos extraídos de mi intervención del 1/11/95 en la CMAD 3 en Sonoma, California. Espero que sirva para aclarar cualquier

malentendido sobre la naturaleza de dichos ataques". Seguidamente, el mensaje detallaba paso a paso el ataque, empezando por los sondeos iniciales desde *toad.com*, el ordenador del sótano de John Gilmore, y terminando por el secuestro de Osiris.

Mientras estábamos trabajando, llamé a Andrew a San Diego. Hablamos sobre su tarea de mejoramiento de nuestro perímetro de seguridad del software y de sus conversaciones con Levord Burns, del FBI, y le conté lo de la aparición de las llamadas con el 911.

Hubo una larga pausa al otro extremo de la línea.

Finalmente, Andrew dijo quedamente: “Tsutomu, he sido yo. Es que te añadí a la lista de alerta de números telefónicos. Hubo un error en el código del router de filtrado que estuve instalando, que hizo que se accionase cuando no debía”. Andrew había estado instalando alarmas en nuestro software defensivo para enviar automáticamente mensajes de busca en caso de intento de intrusión. Los dígitos 911911 eran su inequívoca forma de indicar una emergencia.

En cierto sentido era un alivio conocer el motivo de que mi busca hubiera estado comportándose como un

sonajero, pero me sentí exasperado y pensé: "Andrew, por eso mismo yo soy el consejero y tú el alumno".

El martes por la mañana a primera hora, tras haber dormido unas tres horas, Julia y yo fuimos al aeropuerto de Reno, con un tiempo horrible. Ella cogía el vuelo de la United Express a las 9:35 para San Francisco y yo el de Reno Air a las 11:20 para San Diego. Habíamos disfrutado diez días de trabajo, diversión y mutua compañía, pero ahora tuvimos que despedirnos en su puerta de embarque. Ella regresaba a ver a John, porque le había prometido hacerlo esa mañana. Pero lo hacía sin ganas y me

dijo que aunque sentía miedo, sentía también la necesidad de cumplir su compromiso. Yo no tenía idea de cuándo nos volveríamos a ver y estaba preocupado, puesto que la última vez que ella había estado en Toad Hall lo había pasado fatal y le había sido muy difícil irse. A través del gran ventanal acristalado la saludé con un brazo en alto cuando se encaminaba al avión, y me quedé contemplando el aparato mientras éste se desplazaba hacia la pista de despegue.

Después que su vuelo partió fui a reservar el mío y mientras esperaba saqué mi terminal RadioMail, el modem

inalámbrico conectado a mi ordenador de bolsillo Hewlett Packard 100 que me permite enviar y recibir correo electrónico en cualquier ciudad importante del país. La unidad estuvo casi una hora absorbiendo la cantidad insólitamente grande de mensajes acumulados. Uno era de una lista de correos en la que estoy para un grupo de mis antiguos condiscípulos de Caltech, y mencionaba que había un artículo sobre un tal Shimomura en la primera página de *USA Today*. A continuación otro me mandaba una nota que decía: "¿Ése eres tú?". Yo contesté con otra: "Sí, soy yo, y el que tu nombre aparezca de esa forma

en el *New York Times* es un fastidio cuando ocurre en medio de tus vacaciones de invierno para esquiar".

Una vez en San Diego intervine en una reunión de los altos cargos de SDSC, y luego estuve respondiendo a más llamadas de periodistas. Andrew, entretanto, se entendía con los de seguridad del *campus* y había hablado con el FBI para ver si podíamos conseguir una orden para intervenir el teléfono de mi despacho. Nos figurábamos que probablemente el intruso volvería a llamar, y en ese caso queríamos saber desde dónde lo hacía.

El martes por la tarde me di cuenta

de que había estado todo el día sentado y resolví que si no podía esquiar, al menos iría a patinar, y me fui a hacer una sesión de 25 kilómetros en torno al lago Miramar, donde un grupo informal de patinadores se reúne cada día al atardecer. Si bien cualquier clase de intimidad de la que yo hubiera disfrutado en el pasado parecía estar desapareciendo, entre aquella panda de dos docenas de patinadores podía conservar mi anonimato.

Esa noche, al llegar a casa, decidí añadir un toque final a mi informe sobre el forzamiento antes de remitirlo por Usenet. Con anterioridad había hecho

archivos digitalizados de los mensajes del buzón de voz dejados por mi atacante y ahora los iba a hacer públicos. El SDSC operaba un espacio en Internet que posibilitaba las transferencias ftp de archivos de ordenador. El sitio contenía software gratuito disponible bajo diversos encabezamientos, y yo hice que Andrew pusiera los mensajes del buzón en un directorio al que llamamos *pub/security/sounds*, en referencia no demasiado velada a categorías de distribución de Usenet de un valor de rescate semejante, como *alt.sex.sounds*. Él llamó a los dos archivos

tweedledee.au y *tweedledum.au*[22] respectivamente, con "au" indicando archivos de audio para el disfrute auditivo de los descargadores. Yo añadí una nota sobre los archivos en mi informe sobre "Detalles técnicos", y finalmente lo remití a Usenet a las 4 de la mañana.

Tweedledee.au y *Tweedledum.au* gozaron de una breve popularidad en los ficheros de audio de Internet. El *San José Mercury News* creó un enlace de la página WWW con los archivos de su servicio de Internet *Mercury Center*, y *Newsweek* incluyó citas de los mismos en su artículo sobre la intrusión. Yo

imaginaba que mi atacante, al igual que mucha gente, leía los periódicos y las revistas informativas, y que probablemente estaría muy complacido consigo mismo por la atención que su trabajo estaba recibiendo. Tal vez yo pudiera hacerle morder el anzuelo llamándome otra vez, en cuyo caso tal vez consiguiésemos que cayese en la trampa de nuestro teléfono intervenido.

Había estado jugando al escondite telefónico con David Bank, un periodista del *San José Mercury News* que cubría el tema de las telecomunicaciones, y finalmente hablé con él por la tarde. Me dijo que tenía

dificultades para dar con mi conexión en la red Usenet, de modo que le envié una copia vía correo electrónico y no volví a pensar en el asunto. Varios días después de leer mi informe sobre el ataque *toad.com* inicial, él llamó a John Gilmore para preguntar sobre ello. John le dijo que efectivamente yo había estado en Toad Hall cuando ocurrió el ataque contra mis máquinas en San Diego. Bank se puso a investigar una hipótesis en la cual, como parte de mi disputa por la financiación con la NSA, yo había violado mis propios ordenadores para generar material para la charla en la CMAD. La premisa era

que un falso ataque inventado por mí me daría la oportunidad de hacer gala de mis capacidades ante mis potenciales patrocinadores. La pega en teoría era que todo el mundo sabía que yo era amigo de Julia y John. ¿Por qué iba a ser yo lo bastante estúpido como para fingir un ataque y luego publicar una información que me señalaría casi directamente? Pero Bank, que era un persistente ex cronista policial del *Mercury News*, empezó a seguir mi rastro incansablemente, llamando a toda clase de personas que pudieran conocerme, en un esfuerzo por probar su hipótesis.

La verdadera pista estaba en otra parte, y poco a poco estaban empezando a aparecer sus primeros indicios. El 17 de enero, estando yo en Truckee, el SDSC recibió un *e-mail* de Liudvikas Bukys, administrador de sistemas informáticos en la Universidad de Rochester. El último parágrafo de su nota advertía que el Centro podría verse en graves dificultades si aún no se había enterado de las intrusiones, pues los encargados de seguridad en Rochester habían descubierto indicadores apuntando a mi red mientras investigaban un ataque propio. Andrew había hablado con el grupo de Rochester

y luego también con el personal de seguridad en la Universidad de Loyola, que había sufrido un ataque similar y siendo igualmente notificada por Rochester.

Me había llamado a Truckee para decirme que sin que se supiera cómo mis archivos habían sido transferidos a un ordenador en la Universidad de Rochester desde Loyola, de forma que los encargados de seguridad de allí pudieran examinarlos. A los responsables de Rochester les preocupaba haber perdido algún código fuente del sistema operativo IRIX de Silicon Graphics durante el ataque

sufrido. Sin embargo, cuando los administradores informáticos en Rochester examinaron los archivos robados que habían sido encontrados en Loyola, se dieron cuenta de que eran los míos. Andrew se había desorientado al principio, y por un rato creímos que mis archivos habían sido asimismo ocultados en Rochester por los intrusos, lo cual no era cierto. También nos enteramos de que en el curso del fin de semana alguien más había descubierto que mis archivos fueron a parar a Rochester, posiblemente debido a los artículos que informaron de la intrusión allí. Quienquiera que fuese de nuevo se

había introducido en las máquinas de Rochester utilizando el mismo ataque con manipulación del IP, había vuelto a robar archivos y luego los había borrado. El ataque tuvo éxito en Rochester por segunda vez porque, aunque los administradores de la red en la universidad habían configurado el cortafuegos para rechazar tales ataques, desgraciadamente habían cometido un error cuando estaban cambiando el software del router.

El miércoles, Andrew y yo examinamos los archivos que habían sido recuperados de la Universidad de Loyola. Hubo un indicio interesante: el

que había ocultado los datos robados en el ordenador de la universidad había recorrido mis archivos para ver qué había cogido. Algo que llamó nuestra atención fue que un retrato digitalizado de Kevin Mitnick había sido sacado de mis archivos comprimidos y almacenados aparte. ¿Por qué, me pregunté en voz alta, de entre todo el material el ladrón había dejado la foto de Mitnick suelta por ahí?

¿Era Mitnick nuestro intruso?

"No creo", dijimos casi al unísono Andrew y yo: era demasiado obvio. Además, en una incursión contra los ordenadores del SDSC, en marzo, un

intruso había plantado información para que pareciese que el ataque había sido perpetrado por otro; por tanto, los dos éramos sumamente cautos para dar demasiada importancia a un indicio tan evidente.

Yo había pensado que la atención de la prensa empezaría a aflojar, pero en cambio continuó aumentando durante la semana. Esa tarde, dos periodistas que preparaban un artículo para los periódicos de Gannett en Rochester, habían escuchado las grabaciones en FTP y me llamaron al SDSC preguntando qué se sentía al recibir una amenaza de muerte. Les dije que no la

tomé en serio. El jueves, varias publicaciones enviaron fotógrafos, ocupándome prácticamente el día entero. Añadido al alboroto de la prensa estuvo el hecho de que ese día se inauguraba el nuevo centro atlético universitario vecino del SDSC y Hillary Clinton asistía a la ceremonia, rodeada de periodistas y equipos de filmación. Un fotógrafo de *Newsweek* se presentó en mi despacho con un abundante equipo fotográfico y cantidad de lentes y filtros especiales, y me dijo que sus jefes le habían ordenado tomar fotos "del estilo de las de *Wired*", la revista de San Francisco dedicada a la cultura de la

Red, conocida por su atrevido grafismo e ilustraciones.

Hicimos unas fotos en el Centro y luego el fotógrafo sugirió que fuésemos a tomar otras en el parque estatal de Torrey Pines. Pero llegamos cuando acababan de cerrar las puertas, de modo que nos vimos obligados a aparcar fuera, donde él me hizo posar junto a un montón de rocas. Yo había sido fotógrafo en la secundaria, y ahora por primera vez me daba cuenta de cómo era estar del otro lado de la lente: sentirse completamente tonto allí sentado, fingiendo utilizar uno de mis ordenadores portátiles. Un grupo de

personas que pasaban se detuvo a mirar. Oí que una preguntaba: "¿Qué están haciendo? ¿Es un anuncio de ordenadores?". La "foto" publicada puso obviamente en evidencia la idea de arte de vanguardia que tenía el director artístico: una ridícula foto mía en la que yo estaba sentado con mi ordenador portátil sobre las rodillas, y en un recuadro la foto de mi cara que parecía salir de mi propia cabeza.

Esa noche llamó Julia, y aunque las cosas iban pésimamente en Toad Hall, ella parecía mejor. Durante los días anteriores sólo habíamos hablado brevemente, por haber estado yo tan

ocupado. Le comenté mis aventuras ante el asalto de los medios de comunicación, y lo tonto que me había sentido haciendo de modelo para los fotógrafos.

"Esta vez las cosas empezaron mal y siguieron peor", dijo ella. "Me doy cuenta de que lo que está pasando aquí es malo para mí, y de que tengo que tomar determinaciones difíciles".

Eso era algo que nunca le había escuchado a Julia. Anteriormente ella había tenido miedo de abandonar su entorno conocido.

"Me gustaría estar contigo y sé que eso implica abandonar a John", dijo en

tono quedo. “Pero esto va a ser muy duro, porque llevamos juntos mucho tiempo”.

Todavía no estaba segura de cómo iba a efectuar la ruptura, pero yo estaba alborozado.

“Haré cuanto pueda para ayudarte”, le dije. Nos habíamos echado mutuamente de menos y convinimos en reunimos lo antes posible.

A la siguiente noche me fui a la “patinada” nocturna de los viernes, que se organiza cada semana a las 19.30 en una tienda de bicicletas de Mission Beach. Generalmente son sólo quince o veinte personas: una versión muy

reducida de las Midnight Rollers en San Francisco, que suele atraer a más de cuatrocientas y que procuro no perderme cuando estoy en la zona de la Bahía. La carrera de San Diego, un sosegado acontecimiento social llamado el Dinner Roll, recorre normalmente unos 20 kilómetros por un trayecto que acaba en una parte de la ciudad en la que abundan los restaurantes.

A eso de las 21:30 acabábamos de iniciar el trayecto de regreso del circuito cuando sonó el teléfono móvil que llevaba en la mochila. El aparato está dotado de una combinación auricular-micrófono, que me permite

conversar y patinar al mismo tiempo, de modo que pude escuchar a Sid diciéndome que había revisado el servicio del *New York Times* en American Online y había encontrado un adelanto del artículo de Markoff.

"No te va a gustar lo que dice", me advirtió Sid, que empezó a leerlo, en tono sarcástico: "Fue como si los ladrones, para demostrar su aptitud, hubieran robado el candado. Que es la razón por la cual Tsutomu Shimomura, el guardián de las llaves en este caso, se está tomando el caso como una afrenta personal; y la de que considere una cuestión de honor el descubrir a sus

autores”.

Mientras Sid continuaba leyendo, y yo rodando, no pude evitar sonreír ante la prosa melodramática de Markoff: “El señor Shimomura, uno de los más competentes expertos en seguridad informática de este país, es la persona que instó a una agencia informática gubernamental a emitir el lunes un escalofriante aviso. Unos intrusos desconocidos, advertía la agencia, habían empleado una sofisticada técnica de saqueo para robar archivos del bien protegido ordenador del propio señor Shimomura en su casa de San Diego. Y tanto la cautela del ataque como su

estilo indicaban que muchos de los millones de ordenadores conectados a la red global Internet podían estar en peligro. Hasta ahora ha habido, que se sepa, otras cuatro víctimas, incluyendo ordenadores en la Universidad Loyola de Chicago, la Universidad de Rochester y la Universidad Drexel en Filadelfia".

El artículo me citaba en varios momentos, como: "Parece que los mocosos han aprendido a leer manuales técnicos… Alguien debería enseñarles a tener modales".

Cuando Sid terminó, le dije que el artículo me parecía razonablemente

ameno. Pero él estaba disgustado y temía que la consecuencia del artículo fuera convertir al SDSC en un atractivo blanco. "Tsutomu, esto es deliberadamente cáustico y desafiante", dijo furioso. "Está claro que trata de provocar".

Durante el camino de regreso estuvimos más de diez minutos hablando del artículo y llegamos a la conclusión de que tendríamos que esperar a ver qué pasaba.

Más tarde, pasada medianoche, bajé a buscar un ejemplar del *Times* en el Circle K, una tienda de las que abren 24 horas que en coche queda a unos cinco

minutos de casa, para ver por mí mismo cuán provocativo era el artículo. Al leerlo, me di cuenta de que Sid tenía razón, pero que seguía siendo ameno.

A la mañana siguiente me levanté bastante temprano porque mi casero pensaba vender la casa y vino con su esposa a hacer una revisión. Era mi primera mañana tranquila desde la aparición de la historia del CERT. La vida parecía retornar finalmente a la normalidad y yo preveía un fin de semana en calma.

Estaba en el salón hablando con mis visitantes cuando llamó Markoff y le dije que le llamaría yo enseguida. Cinco

minutos más tarde le telefoneé a la delegación del *Times* en San Francisco.

"Tengo malas noticias", empezó diciéndome. "Tus archivos robados han aparecido en la Well".

8. El hallazgo de Koball

El viernes por la noche, 27 de enero, al acceder a su cuenta en la Well, un conocido servicio de conferencia por ordenador de la zona de la Bahía, Bruce Koball había hecho un descubrimiento intrigante.

Koball, un diseñador de software afincado en Berkeley, es uno de los organizadores de la conferencia anual

sobre “Ordenadores, Libertad y Privacidad”, y Well le había otorgado una cuenta adicional gratuita —CFP[23]— como contribución a los preparativos de la reunión de 1995. Como él no la había utilizado en varios meses, le sorprendió encontrar esa noche un mensaje del personal de mantenimiento del sistema de Well advirtiéndole que debía trasladar los 150 megabytes de material almacenado en aquel momento en la cuenta CFP o se lo borrarían.

Tales mensajes son corrientes en Well, cuyo personal ejecuta rutinariamente un programa para

conocer niveles de uso, con objeto de descubrir "acaparadores" —personas que ocupan un espacio de almacenamiento desproporcionado en los ordenadores del servicio— y Koball fue simplemente uno de los varios suscriptores que recibieron el aviso ese día. Pero como él apenas había utilizado la cuenta CFP, no pudo entender el mensaje hasta que miró su directorio. Era evidente que un intruso se había apoderado del espacio y lo había llenado de unos misteriosos archivos condensados y tandas de correo electrónico.

```
well % ls -l
```

```
total 158127
-rw-r--r--  1 cfp     128273 Dec
26 23:02 bad.tgz
-rw-r--r--  1 cfp     547400 Dec
26 23:07 brk.tar.Z
-rw-r--r--  1 cfp        620 Dec
26 23:07 clobber.tar.Z
-rw-r--r--  1 cfp       2972 Dec
26 23:07 clobber.tgz
-rw-r--r--  1 cfp        734 Mar
14 1991  dead.letter
-rw-r--r--  1 cfp     704251 Dec
26 23:11 disasm.tar.Z
-rw-r--r--  1 cfp    4558390 Dec
26 23:31 file.941210.0214.gz
-rw-r--r--  1 cfp    1584288 Dec
26 23:39 file.941215.0211.gz
-rw-r--r--  1 cfp    2099998 Dec
26 23:47 file.941217.0149.gz
-rw-r--r--  1 cfp    1087949 Dec
27 10:09 kdm.jpeg
```

```
-rw-r--r--  1 cfp     275100 Dec
27 10:09 kdm.ps.z
-rw-r--r--  1 cfp    1068231 Dec
27 10:10 mbox.1.Z
-rw-r--r--  1 cfp     869439 Dec
27 10:10 mbox.2.Z
-rw-r--r--  1 cfp     495875 Dec
27 10:10 mbox.Z
-rw-r--r--  1 cfp      43734 Dec
27 10:10 modesn.txt.Z
-rw-r--r--  1 cfp    1440017 Dec
27 10:11 newoki.tar.Z
-rw-r--r--  1 cfp     999242 Dec
27 10:12 okitsu.tar.Z
-rw-rw-rw-  1 cfp     578305 Dec
28 09:25 stuff.tar.Z
-rw-rw-rw-  1 cfp  140846522 Dec
27 11:28 t.tgz
-rw-r--r--  1 cfp     146557 Dec
27 11:28 toplevel.tar.Z
-rw-r--r--  1 cfp    3967175 Dec
```

```
27 11:31 tt.z
-rw-r--r--  1 cfp         307 Dec
20 1990  xmodem.log
-rw-r--r--  1 cfp      187656 Dec
27 11:31 ztools.tar.Z
```

El listado del directorio mostraba la cantidad total de espacio del disco que ocupaban los archivos, así como sus nombres, fechas de modificación y otros detalles. Entre los archivos había tres nominados “mbox”, la nomenclatura estándar de Unix para el archivo que contiene el correo de un usuario. Cuando Koball examinó algunos de los archivos de correo descubrió que todos los mensajes estaban dirigidos a la misma persona: *tsutomu@ariel.sdsc.edu*.

Aunque Koball y yo habíamos estado juntos en unas cuantas reuniones anuales de pioneros de la industria informática denominadas Hacker's Conferences, el nombre Tsutomu no le sonó inmediatamente. Estaba desconcertado y preguntándose aún qué hacer acerca de su descubrimiento cuando, ya tarde, oyó caer en el umbral de la puerta de la calle el ejemplar del día siguiente del *New York Times*, como ocurre antes de medianoche en muchos hogares de la zona de la bahía. Koball recogió el periódico, lo hojeó, llegó a la primera página de la sección de negocios y allí estaba: el artículo de

Markoff y mi foto en la que aparecía sentado en la sala de operaciones del Centro de Superordenadores de San Diego.

A primera hora de la mañana siguiente llamó por teléfono a Hua-Pei Chen, administradora de sistemas de Well, con sede en Sausalito, en Marin County. Le dio cuenta de su descubrimiento, le habló de su relación conmigo y le pidió que borrase los archivos y cancelara la cuenta CFP.

Poco después recibió una llamada de su amigo John Wharton, diseñador independiente de chips y uno de los principales organizadores de la

exclusiva conferencia Asilomar sobre diseño de microprocesadores, a la que asisten cada año en Monterey muchos de los "veteranos" pioneros de las industrias de semiconductores y ordenadores personales. Wharton, que se encontraba conduciendo su coche por la autopista 101 hacia el Cow Palace de San Francisco, donde había una exhibición de modelos a escala de trenes, quería saber si habría una demostración de un modelo digital de efectos sonoros de ferrocarril que Koball había producido con Neil Young, la estrella del rock, que es también un fanático de los modelos de trenes.

Koball es pionero en una industria que está inyectando "inteligencia" informática en toda clase de productos de consumo y ha desarrollado software para artilugios especialmente buenos como los ciclómetros Avocet utilizados por los ciclistas y los relojes-altímetro preferidos por los escaladores, incluido yo. (Cuando Julia estuvo en Nepal comprobó que el reloj de Koball es el máximo signo de estatus entre los sherpas que acompañan a los escaladores occidentales en el Himalaya).

Koball le dijo a Wharton que no, que su sistema sonoro para modelos de

trenes a escala no iba a ser expuesto, pero acto seguido desvió la conversación hacia el descubrimiento realizado en Well. Wharton quedó fascinado, y en el siguiente cambio de impresiones convino en que liquidar la cuenta CFP parecía la decisión más razonable. Concluida la conversación, Wharton empezó a preguntarse si cualquiera de los dos sabía realmente lo bastante como para llegar a la antedicha conclusión y se le ocurrió que la persona a quien valdría la pena consultar sería su amiga Marianne Mueller, programadora de software de sistemas en Sun Microsystems, que

sabía mucho más que él sobre Unix, Internet y cuestiones de seguridad en general. Telefoneó a su casa y a su trabajo, pero no pudo dar con ella.

De hecho, yo había conocido tanto a Mueller como a Wharton el año anterior en Las Vegas, en la convención anual del submundo informático llamada Defcon —una extraña reunión de majaderos, gente de la seguridad de la industria de las telecomunicaciones, e indudablemente algunos policías—, a la que no sé cómo había permitido que Markoff me arrastrase. Una de las pocas cosas interesantes fue una charla dada por Mueller sobre los hackers, en la que

presentó su propia versión digitalmente equipada de una muñeca Barbie, a la que llamó Hacker Barbe para evitar problemas de derechos con Mattel Inc., el fabricante de Barbie. Fue todo muy gracioso, aunque el humor pasó desapercibido para los adolescentes presentes en la conferencia, que parecían interesados sobre todo en travesuras juveniles tales como burlar las cerraduras controladas por microprocesador de las puertas de los hoteles.

Wharton se aproximaba a la desviación hacia el aeropuerto de San Francisco y recordó que el día anterior

Mueller había mencionado que el sábado alrededor de mediodía estaría despidiendo a una amiga que se iba para Tokio. Tomó la salida al aeropuerto, condujo hasta la planta superior del garaje de aparcamiento, localizó el MR2 de Mueller en la zona de salidas internacionales y pudo aparcar precisamente al lado. Mientras corría hacia la terminal vio en un monitor que el vuelo de JAL estaba ya saliendo. Se detuvo y empezó a examinar la multitud.

Con su abundante cabellera larga y grisácea, sus gafas de montura metálica y su calzado Birkenstock, no había estado mucho rato de pie en el gran

vestíbulo de acceso cuando localizó a Mueller, que vestía un mono de cuero negro y una camiseta Cypherpunks, y corrió hacia ella. Aprovechando las posibilidades clandestinas de aquel encuentro en una terminal de vuelos internacionales, Wharton hizo que Mueller le jurase guardar secreto antes de contarle lo que había sabido por Koball.

"¡Que no vayan a hacer nada con los archivos!", dijo alarmada Mueller. Insistió en que no fuesen borrados ni alterados en forma alguna, pues cualquier cambio podría revelar al ladrón que su presencia había sido

descubierta. En cambio, explicó, el personal de seguridad de Well debía colocar software de control y llevar un registro de todo aquel que intentase acceder a los archivos. Wharton, que seguía disfrutando con el aspecto novelesco de la situación, pero ahora más consciente de la gravedad del asunto, llamó nuevamente a Kobal por su teléfono móvil.

"Líder Perro Rojo", empezó diciendo cuando Koball contestó la llamada. "Aquí Llorón Cósmico. Practicado reconocimiento con Mama Cyber; ¡dice que dejéis en paz los archivos!".

Después de hablar al poco rato con Mueller por teléfono regular, Koball volvió a llamar a Well para rectificar sus instrucciones anteriores. Pero los preocupados superiores de Well ya habían discutido el tema entre ellos resolviendo no hacer nada que comportase el riesgo de alertar al intruso. A continuación, Koball telefoneó a Markoff, quien a su vez me llamó para alertarme y darme el número de Koball en Berkeley.

Era cerca de mediodía cuando hablé con Bruce Koball. Me describió los archivos que había encontrado la noche anterior en el directorio CFP y me leyó

las fechas de acceso, no todas ella de utilidad porque él ya había leído algunos de los archivos. Pero no cabía duda de que se trataba de material robado de Ariel en diciembre: los programas que yo había escrito, el irrelevante software gratuito cuyo robo carecía de sentido y, lo peor, megabytes y megabytes de mi correo, cosa que yo sentía como una tremenda invasión de mi intimidad.

Koball me puso al corriente de las conversaciones que había mantenido más temprano esa mañana, con Pei en Well, con Wharton y Mueller, y luego otra vez con Pei. Un complot muy bonito, pero yo no tenía interés en

historias de espías, a pesar de lo que el artículo de Markoff pudiera haber dicho que yo consideraba "una cuestión de honor" el descubrimiento de la trama delictiva. Era mi correo electrónico el que estaba siendo esparcido por toda Internet y le dije a Koball que quería que borrasen los archivos. Él me dio el número del teléfono móvil de Pei y yo la llamé para decirle lo mismo.

Pei me explicó que los responsables de Well tenían dudas sobre el procedimiento a seguir, pues les preocupaba que al borrar los archivos no sólo alertarían a la persona que se había apoderado de la cuenta CFP, sino

que podía provocar asimismo que el intruso tomase algún tipo de represalia.

"Quiero esos archivos fuera de su máquina", volví a decir. Según Koball, el intruso había establecido los parámetros de "permiso" en la cuenta CFP para "lectura universal", o sea que cualquiera con acceso a Well podía mirar los archivos que contenía. A mí no me hacía gracia hacer público mi correo bajo ninguna circunstancia, y en particular no quería que ninguno de mis archivos personales o profesionales se convirtiese en el material de lectura corriente del submundo informático. De todas maneras, también comprendía las

preocupaciones de Well, de modo que me puse a instruir a Pei sobre una serie de pasos que harían parecer que Koball había respondido simplemente al aviso sobre sobresaturación y había limpiado de archivos el directorio CFP sin tomar nota de su contenido.

En aquel momento yo no sabía mucho de Well. Algunos meses antes, actuando de consultor en Sun Microsystems, había conocido brevemente al propietario de Well, Bruce Katz, que estaba en el mercado de ordenadores nuevos. Recordaba vagamente que Well era un lugar donde se reunían muchas personas, desde

asistentes habituales a las conferencias de hackers hasta Dead Heads[24] provistos de un modem.

Pei, por su parte, parecía más bien confusa acerca de las vulnerabilidades en la seguridad de Well. Como mucha gente, había estado leyendo sobre el forzamiento de San Diego, y desde esa mañana sabía que al menos una cuenta de la Well había sido violada, pero no había relacionado ambas cosas.

"Ah, eso tiene mucho más sentido", dijo, después que le hube explicado cómo mis archivos habían acabado en su sistema. Reconoció que Well sabía que probablemente estaba mal equipado

para manejar aquel problema, y dijo que durante la frenética ronda de conversaciones telefónicas de esa mañana uno de los directores de Well, John Perry Barlow, letrista de los Grateful Dead y uno de los fundadores de la Electronic Frontier Foundation, había sugerido que Well me invitase a ir a Sausalito a ayudarlos.

Yo estaba comprometido a hablar la siguiente semana en una conferencia informática en Palm Springs, donde había convenido en encontrarme con Julia, y le dije a Pei que estaba sobrecargado de obligaciones. "¿Qué tal", sugerí, "si mi alumno Andrew

Gross volaba a Sausalito y echaba una ojeada?".

Pasé varias horas efectuando los arreglos. Andrew y su esposa, Sara, candidata al doctorado en química por la UCSD, estaban en proceso de mudarse a otro apartamento porque el moho causado en su piso de estudiantes por la humedad se había vuelto insoportable, incluso para alguien fascinado por la materia orgánica como ella. No obstante, convinieron en que él estaría libre el martes para volar al norte. A continuación convencí a Sid de continuar pagándole el salario de SDSC e incluso de asignarle algo para gastos

durante su estancia en la zona de la bahía. Yo todavía no estaba empeñado en rastrear al intruso, pero pensaba que yendo a la Well Andrew podría descubrir información adicional de utilidad sobre el despojo a Ariel y sobre qué había pasado después con mis archivos.

Para entonces Kobal me había enviado por correo electrónico los tiempos de creación de archivos y de acceso para los contenidos del directorio CFP (con un mensaje añadido diciendo que le había alegrado ver en la foto del *Times* que yo llevaba puesto uno de sus relojes altímetro Avocet

Vertech). Una vez que supe cuándo habían sido creados los archivos, pude determinar que las copias de mi material habían sido depositadas en Well antes de transcurridas doce horas de haber sido movidas de Ariel. Aunque era posible que los archivos hubieran hecho una o incluso varias paradas en otras partes de Internet antes de aterrizar en Well, el tiempo empleado sugería que el pirata de Well era alguien íntimamente relacionado con la persona que había robado mis archivos… si no el propio ladrón.

El miércoles por la tarde, antes de salir para la conferencia en Palm

Springs, recibí un mensaje telefónico de Andrew, que había llegado a Sausalito la noche anterior. Anticipando la llegada de un comando informático, la Well había alquilado para él un imponente Jeep Cherokee, con el que Andrew estaba absolutamente encantado, pues el coche que tiene en San Diego es un Honda Accord de trece años de antigüedad. Aparte de eso, se sentía frustrado: hasta el momento su estancia entera había estado dedicada a reuniones con responsables de Well sobre unos acuerdos de confidencialidad que querían hacerle firmar antes de permitirle examinar el sistema; todavía

no había dedicado ni un momento a ocuparse de sus problemas. Como Andrew suele ser mucho más flexible y diplomático que yo, su disgusto me impresionó como una mala señal de lo embarulladas que debían estar las cosas en Well.

Tras volar a Palm Springs, me registré en el Westin Mission Hills Resort, donde los patrocinadores de la conferencia corrían con mis gastos y los de Julia. Era casi de noche y ella, que había perdido su vuelo, no había llegado aún de San Francisco. Se había enredado en otra penosa discusión con John, que le juró que si ella se iba a

Palm Springs conmigo, la relación entre ellos había terminado. Julia le dijo que se iba igual, pero que no quería que quedasen peleados. A modo de tregua, había aceptado que se reunirían a la semana siguiente para decirse adiós.

Partí para la recepción a los oradores, dejándole una nota, y finalmente, a eso de las 9 de la noche, ella se reunió conmigo en la cena de la conferencia. Estaba tensa y exhausta después de una espera de horas en Los Ángeles para conseguir un vuelo hacia Palm Springs. Pero lo había conseguido, y a los dos nos encantó vernos.

El acontecimiento era una llamada

Vanguard Conference, parte de una serie de seminarios que la Computer Sciences Corporation, una firma consultora de alta tecnología, llevaba a cabo a lo largo del año para altos ejecutivos responsables de tecnología de la información en sus respectivas empresas. Los asistentes incluían representantes de una larga lista de compañías tales como AT&T, American Express, Federal Express, Morgan Stanley y Turner Broadcasting.

La lista de oradores era asimismo impresionante y variada, e incluía a Bill Cheswick, el experto en seguridad de Laboratorios Bell; Whitfield Diffie,

padre de una técnica criptográfica ampliamente difundida para proteger la intimidad informática; Clifford Stoll, el astrónomo itinerante que a mediados de los años ochenta dio caza a unos jóvenes vándalos informáticos alemanes y luego convirtió la historia en un *best seller* de no ficción, *El huevo del cuco;* Mitchell Kapor, el fundador de Lotus Development y cofundador de la Electronic Frontier Foundation; y Nicholas Negroponte, fundador y director del Laboratorio de Medios del MIT.

A mí me habían invitado como sustituto de última hora de otro orador y

uno de los organizadores de la conferencia, Larry Smarr, director del Centro Nacional de Aplicaciones de Superordenadores, de Illinois, una organización hermana del SDSC con financiación federal. Yo había supuesto que mi súbita notoriedad tenía mucho que ver con la invitación, aunque dudé si sentirme halagado cuando me enteré de que en realidad estaba ocupando el lugar de Mark Abene, un bandido informático neoyorquino convicto, más conocido por Phiber Optic, que tuvo que renunciar porque le negaron el permiso para salir del Estado. Pero me sentí mejor cuando me encontré con Bill Cheswick en la

recepción a los oradores; Ches bromeó que él y yo parecíamos habituales del circuito de los chicos de la seguridad informática.

Eran tantas las personas que se me acercaban comentando "he visto su foto en el periódico", que me inventé una respuesta estándar: "Es mejor que encontrarla entre las de las personas buscadas".

Mi muy publicitado forzamiento había engendrado un sorprendente grado de paranoia entre la gente de empresas allí presente, en su mayoría responsables de las redes de sus respectivas compañías. Al parecer

habían llegado a la conclusión de que si "uno de los más competentes expertos en seguridad informática de este país" podía ser atacado con impunidad, era obvio que ellos eran más vulnerables. "Malos tiempos son estos, si de los problemas de seguridad hemos de enteramos antes en las páginas del *New York Times*", me había escrito en un mensaje por correo electrónico alguien de Morgan Stanley, el gran banco inversor, tras la aparición del artículo de Markoff sobre el CERT la semana anterior. Ahora los ejecutivos presentes venían a preguntarme si estaría dispuesto a acudir a sus empresas a

realizar una revisión de la seguridad y como consultor en la materia.

El jueves ofrecí una versión sólo ligeramente más pulida de mi intervención en la CMAD, demostrando cómo aparece "al natural" un ataque IP-spoofing, pero me temo que mi esfuerzo por subrayar las complejidades del delito informático real no tuvo otro resultado que el de dejar perplejos a muchos de mis oyentes. Ese viernes, en cambio, junto con Ches, hice que la audiencia recorriese con mi vídeo de Adrian los intentos de forzamiento de 1991 en ordenadores gubernamentales y militares, y el grupo no sólo siguió la

exposición sino que pareció satisfecho de ver un caso en el que los "buenos" habían podido detectar, y luego contener, a los villanos.

Después de la charla, Julia y yo estuvimos patinando por los senderos y las calles de Palm Springs, maravillados ante los espacios de césped impecablemente mantenidos allí, en medio del desierto. El jueves acudimos a la fiesta al aire libre amenizada por una banda *country-and-western*; para entonces habíamos finalmente empezado a divertirnos y no nos atraía la idea de irnos al día siguiente. Y eso que las cercanas cumbres nevadas de San

Jacinto eran un recordatorio de que íbamos a volver a Sierra Nevada a reanudar la práctica del esquí que habíamos interrumpido dos semanas antes.

El viernes a primera hora de la tarde Larry Smarr y yo nos pusimos a discutir la posibilidad de un proyecto conjunto de investigación sobre seguridad informática entre el SDSC y el Centro de Smarr. Estuvimos de acuerdo en que una parte excesiva de lo que pasaba por seguridad informática consistía simplemente en adoptar posturas defensivas; nosotros queríamos

enfrentarnos al enemigo desarrollando un modelo mucho más agresivo, acudiendo a los ejercicios de simulacro bélico de la teoría militar y descubriendo hasta qué punto podían ser aplicados al campo electrónico. Si los intrusos informáticos fueran cazados e identificados de forma rutinaria, el porcentaje de incidentes bajaría de un modo dramático.

Había perdido la noción del tiempo, y de pronto me di cuenta de que tenía que encontrar a Julia, a quien encontré hablando de su oficio con un grupo de profesionales de sistemas. La saqué de allí para que pudiésemos coger el vuelo

a Los Ángeles, donde habíamos de enlazar con el avión a Reno. Al final lo logramos por los pelos, retrasados por la hora punta del tránsito en Palm Springs, y acabamos corriendo por la terminal, en una especie de carga de la brigada ligera con ordenadores portátiles, bolsas de patines, equipaje de mano, esquís y demás.

A la mañana siguiente fuimos en coche hasta Mount Rose, a 20 kilómetros al suroeste del aeropuerto de Reno, para realizar una marcha con esquís. Era un día hermoso, soleado, despejado y fresco, y fue estupendo estar nuevamente en la nieve. Pasamos

el día llevando a cabo ejercicios con balizas de avalancha, los transmisores de señales que llevan los esquiadores para ayudar en su búsqueda a los equipos de rescate si quedan sepultados por un deslizamiento. Un grupo salía y enterraba unas balizas, y otros practicaban localizándolas y desenterrándolas. Hubo también otros ejercicios, incluyendo el manejo de sistemas de poleas, prácticas con deslizadores de rescate y equipo médico. El domingo salimos a esquiar sin prisa por nuestra cuenta, y esa noche cuando regresamos a la cabaña estábamos exhaustos por los esfuerzos

del fin de semana.

Dediqué más o menos una hora a devolver llamadas telefónicas y a saludar a amigos, y escuché varias veces que David Bank, el periodista del *San José Mercury*, seguía con la teoría de que yo había fingido el forzamiento como una maniobra publicitaria. También oí que Bank había cenado con John Gilmore la misma noche que Julia voló a Palm Springs para reunirse conmigo y empecé a preguntarme qué le habría dicho éste. Era un hecho que la naturaleza del ataque a Ariel apuntaba a un perpetrador sofisticado, familiarizado con el TCP/IP y Unix. Y

después de todo, aquellas sondas iniciales habían venido de *toad.com*.

Después de haber reflexionado en voz alta sobre mis sospechas mientras comíamos, Julia y yo estuvimos de acuerdo en que, por más furioso que John pudiera estar con cualquiera de los dos, era un cruzado de la intimidad electrónica con demasiados principios como para tener algo que ver con el forzamiento de un ordenador. De todas formas, los rumores y el continuo cuestionamiento de mis motivos despertaban mi curiosidad sobre a dónde conducía ese encadenamiento de sucesos y decidimos escribir una

relación cronológica de los hechos que nos ayudase a entender y explicar lo que había ocurrido.

A eso de las 11 de la noche llamó Andrew. Habíamos estado brevemente en contacto varias veces desde el miércoles, pero ésta era la primera oportunidad para una completa puesta al día. "¿Qué has descubierto hasta ahora?", le pregunté, todavía con la esperanza de que pudiera manejar las cosas por sí mismo en Well.

"Tsutomu, creo que deberías venir a ayudarme", dijo él. "Estoy con el agua al cuello".

Tras pasar varios días atascado en

la burocracia de Well, Andrew había empezado por fin a examinar el software robado guardado en el sistema de Well el domingo por la mañana, y resultó contener mucho más que simplemente mi colección de archivos. Había pasado el día creando un inventario del material robado, cada vez más alarmado ante el valor y el propio volumen del contrabando. “Es evidente que estamos frente a algo que no es el corriente jovenzuelo pirateando sistemas”, dijo.

El software estaba ubicado en una cantidad de cuentas ilegítimas en la Well, y mis archivos robados, tan cuidadosamente borrados una semana

antes, habían vuelto a aparecer, en una cuenta diferente. Este solo hecho sugería que quien se había apoderado de los ordenadores de Well era lo bastante engreído como para creer que podía ir y venir, mudando impunemente las cosas de un lado a otro. Andrew empezó a recitar una lista de lo que había encontrado, pero lo interrumpí diciéndole que quería examinarla sistemáticamente. Rich Ress, del FBI, me había dicho durante aquella llamada de disculpas allá por enero que el Bureau otorgaba prioridad a los casos según su valor en dólares. Resolví que si querían dólares, yo ahora se los iba a

dar.

Mientras Andrew empezaba de nuevo a pormenorizar sus hallazgos, yo me puse a responder con una estimación del valor de cada programa robado, sea en precio de mercado o en coste de desarrollo. Además de mi software, estaba el del teléfono móvil de Qualcomm, una empresa de tecnología de San Diego; cantidad de programas de una casa de software llamada Intermetrics, que crea herramientas de desarrollo de software; el código fuente de Silicon Graphics, el software de estación de trabajo 3-D usado para crear la mayoría de los efectos especiales de

las películas de Hollywood; el software de seguridad informática que se suponía debía proteger contra robo los programas de la compañía; registros del ordenador pasarela de Internet para el Sector de Productos Semiconductores de Motorola, que había captado información encaminada a la red de Motorola, incluyendo contraseñas; varias contraseñas robadas captadas por otros programas de chequeo; un archivo entero de contraseñas de *apple.com*, la puerta de entrada de Apple Computers a Internet; y diversas herramientas de software para forzar de varias maneras la entrada en un ordenador.

Cuando terminé la cuenta el total en dólares ascendía a varios millones en coste de desarrollo de software, cifra que no incluía el que tal vez fuera el trofeo más notable, cuyo valor potencial no podía empezar a calcular: un extenso archivo de datos con el nombre *0108.gz*, que contenía más de veinte mil números de cuenta de tarjetas de crédito de los suscriptores de Netcom On-Line Communications Services Inc., un proveedor de servicios de Internet con base en San José, California. Muchas compañías de redes en conexión permanente piden a sus suscriptores que proporcionen plena información de la

tarjeta de crédito al establecer sus cuentas, si bien la misma generalmente no se almacena en un ordenador conectado a Internet.

La información de las tarjetas de crédito no era la única pérdida de Netcom. El ladrón había hurtado también el archivo de contraseñas de suscriptores, otro paquete de información que normalmente no debería haber sido accesible. La versión del sistema operativo Sun Microsystems instalado en Netcom toma ciertas medidas para proteger ese archivo: las contraseñas están codificadas, lo cual teóricamente las vuelve inútiles para

cualquiera que tropiece con ellas, y el archivo que contiene las contraseñas es inaccesible excepto para quien tenga acceso a sus ordenadores.

Aun así, la posesión de una copia de ese archivo permitiría a un ladrón descodificar algunas contraseñas no muy bien elegidas. El método criptográfico empleado para codificarlas es sumamente conocido. Por tanto, la cuestión sería simplemente utilizarlo para codificar cada palabra de un diccionario amplio y luego comparar las palabras del diccionario alteradas con las contraseñas del archivo. Cada vez que encontrase una coincidencia, el

ladrón podría desandar el proceso para llegar a la palabra sin codificar en el diccionario y ¡zas!: una contraseña válida. Un artista del forzamiento puede emplear un ordenador para ejecutar de una forma rápida y con éxito este tipo de ataque mediante ruptura de código contra aquellas personas lo bastante imprudentes como para utilizar palabras corrientes a modo de contraseñas.

Después Andrew centró su atención en otra categoría de bienes robados: el correo electrónico. Además del contenido de mi buzón, el ladrón (o los ladrones) había robado el correo de otras dos personas. Andrew y yo

reconocimos el nombre de Eric Allman, autor de sendmail, el programa estándar de correo de Internet. Yo supuse que el correo de Allman había sido saqueado en busca de informes sobre nuevos fallos de seguridad en dicho programa, pero Andrew, sensible a las cuestiones de intimidad, no había leído los contenidos. El otro nombre, desconocido para nosotros, era el de un estudiante de Stanford llamado Paul Kocher, cuyo correo electrónico había sido expoliado por motivos que ignorábamos.

Las comprobaciones regulares de la Well había reducido las idas y venidas

del intruso a una falsa cuenta llamada *dono*, utilizando la contraseña "fucknmc", que en sí misma sonaba como una pista. En el mundo de Unix e Internet existe la arraigada tradición de usar las iniciales de tu nombre y apellidos como nombre de entrada de registro, y nos preguntábamos quién sería el "nmc" a quien el ladrón parecía guardar rencor.[25]

Andrew y el personal de Well dedicado al caso sólo podían ver lo que sucedía localmente cuando el ladrón conectaba desde un ordenador remoto, pero rastreando las actividades de *dono* en Well fue posible ver surgir un

esquema determinado y conjeturar razonablemente lo que estaba haciendo en otras partes. Como las herramientas de delinquir y la mercadería robada constituían pruebas que ningún delincuente avisado querría dejar descuidadamente en discos duros en su casa, el intruso de *dono* estaba al parecer utilizando a Well como taquilla electrónica donde almacenarlas. Para cada incursión contra un ordenador en Internet, *dono* sacaba de Well copias de sus herramientas, en una secuencia predecible.

Primero venía a por un programa corriente de forzamiento que le permitía

hacerse raíz en un sistema mal vigilado en alguna parte de Internet. Poco después volvía en busca de un programa "de encubrimiento", que ocultaba su presencia en el sistema en cuestión, cuando menos al observador casual, borrando de los registros del sistema los rastros de sus actividades. Terminada su nefasta tarea, el intruso retornaba a Well en busca de un programa fisgón que podía dejar en el lugar saqueado para recoger contraseñas que más tarde le posibilitaran forzar otras máquinas.

Se trataba de un delincuente muy metódico.

Pero Andrew había visto también

que el pirata, en concordancia con lo mostrado en nuestro forzamiento de San Diego, estaba siendo descuidado. Una vez ejecutado en un ordenador forzado su programa de encubrimiento, que suprimía de los ficheros de estadísticas de utilización la prueba de su presencia, no se preocupaba de cubrir sus huellas al proceder a llevarse los archivos robados. Por ejemplo, podían quedar por cualquier otra parte del sistema registros de la efectiva transferencia de archivos. Puede que un observador casual no advirtiese esas actividades, pero a cualquiera que buscase ese tipo de comportamiento le resultaría

probablemente fácil rastrearlo.

Andrew empleó tres cuartos de hora en describir todo lo que había observado. “Esto tiene proporciones enormes, Tsutomu”, concluyó Andrew. “Ni siquiera tenemos suficientes ordenadores para realizar un seguimiento adecuado”. Lo peor, continuó, era que aun cuando había consentido en firmar todos los documentos sobre confidencialidad que Well le había puesto por delante, sus actividades continuaban siendo estrechamente restringidas por una mujer llamada Claudia Stroud, ayudante administrativa de Bruce Katz, el dueño

de Well.

“Llevo aquí una semana”, dijo Andrew, “he reunido datos. Tengo cierta idea acerca de dónde vienen estos tipos, pero ahora estoy con el agua al cuello. Ahora te toca a ti”.

Me dijo que los ejecutivos de Well querían celebrar una reunión al día siguiente con un pequeño grupo de gente para discutir cómo responder a los ataques. Yo le aseguré que estaría presente, pero le pregunté si podía conseguir que se pospusiera para la noche; quería aprovechar un día más de esquí antes de alejarme de las montañas.

Le dije a Andrew que entretanto

debía reunir algo más de información. Quería datos sobre la hora y la fecha de cada acceso a los archivos, y le pedí que hiciera una lista de las conexiones del pirata con Well. También le sugerí que realizara una búsqueda más exhaustiva de puertas secretas y troyanos. Era importante que él y el escuadrón de seguimiento de Well no estrecharan prematuramente el campo de su vigilancia. No queríamos ser como el borracho del clásico chiste que tras perder las llaves las busca únicamente bajo la farola de la calle porque "es donde hay mejor luz". Andrew había llevado consigo desde San Diego uno de

los ordenadores RDI, y le pedí que cuando llegase a la zona de la bahía recogiese el segundo, que yo le había prestado a Soeren Christensen, un amigo que trabajaba en la Sun. Yo llevaba una tercera máquina para que contásemos con los recursos necesarios tanto para controlar como para analizar los datos.

Después de colgar me senté en el suelo de la cabaña y durante varios minutos estuve contemplando el fuego que bailoteaba detrás del cristal de la panzuda estufa. A pesar de sus protestas de que aquello lo sobrepasaba, Andrew había descubierto pruebas en abundancia. Se estaban cometiendo

verdaderos delitos, sin señales de que fueran a terminar, y ahora había una pista caliente que seguir.

DOS:
LA PERSECUCIÓN

9. Anatomía

El lunes Julia y yo nos despertamos a media mañana.

Me senté a los pies de la cama situada en la parte central del ático de la cabaña a dos aguas y me desperecé. El ático ocupaba la parte trasera, y yo no veía nada excepto una luz grisácea que filtraban las cortinas que cubrían el ventanal. Volví a pensar en la llamada de auxilio de Andrew la noche anterior. Estaba claro que había que ocuparse del

caso y en conciencia yo ya no podía esperar que lo hiciera otro. Por eso, después de hablar con Andrew, me quedé levantado hasta tarde contestando el buzón de voz y el correo electrónico, un ritual de preparación para zambullirme de nuevo en el mundo exterior. Hubo otro mensaje amenazante más, y se lo envié a Andrew con un mensaje adjunto pidiéndole que se comunicase con las autoridades para rastrear la llamada.

Aunque no parecía un gran día para esquiar, estaba decidido a salir una vez más. Caía una nieve ligera, castigada por unas rachas de viento que la

impulsaban de lado y ocasionalmente incluso directamente hacia arriba.

Yo no tenía un plan en especial, pero parecía lógico pasar un par de días en Well para calibrar el problema. Cada vez había más motivos para pensar que nuestro intruso podría ser Kevin Mitnick, no solo por el código fuente de Oki y Qualcomm que habían sido escondidos en la Well, sino también otras indicaciones sueltas, incluyendo la confidencia del pirata Justin Petersen. Pero también existían razones para excluir a Mitnick, especialmente la sofisticación del ataque IP-spoofing y los sarcasmos del buzón de voz, que yo

estaba casi seguro no eran obra de una sola persona (aunque Mitnick, desde luego, podía formar parte de una conspiración). Si era efectivamente Kevin Mitnick, ciertamente suscitaría mucho interés en los tipos de las fuerzas del orden. Levord Burns, el agente investigador con quien Andrew había estado hablando, trabajaba para Rich Ress en el equipo contra los delitos informáticos del FBI en Washington, D.C. El Bureau daba toda la impresión de que iba a ayudar esta vez, pero a partir de la ocasión en que hablé con el FBI sobre el delito informático en su centro de entrenamiento de Quantico, mi

impresión ha sido siempre que incluso el que hubieran decidido tal cosa no era garantía de éxito. Siento respeto por la integridad de los agentes que he conocido, pero incluso ellos admiten que generalmente el delito informático los supera. Por lo general el agente investigador medio ha asistido a una clase de entrenamiento, de forma que sabe cómo reconocer un ordenador en la escena del delito, pero es probable que no sepa cómo ponerlo en marcha.

Yo no tenía ninguna duda, por otra parte, de que el Bureau sabe mucho sobre la psicología del delincuente habitual. En Quantico me enteré también

de las técnicas para rastrear y capturar asesinos seriales y lo frecuente que es que consigan librarse. Los expertos del FBI en delitos reiterados creen que existen semejanzas entre el delito informático y otros tipos de delitos repetidos más violentos y complejos. Es una idea discutible, pero los expertos del FBI aducen que el mismo comportamiento compulsivo y las mismas ansias de poder impulsan a ambas clases de delincuente. Según esa teoría de científicos conductistas, en ambos casos los delincuentes experimentan en cada ocasión la necesidad de un "chute", y ésta se va

haciendo cada vez más frecuente. Más relevante para mi tarea es la aceptación por su parte de que en ambos tipos de delito serial el mayor problema en cuanto a la investigación radica en el manejo de la información, es decir, en ordenar y organizar los datos acumulados. Cuando examinan retrospectivamente un caso de delito serial, con frecuencia descubren que tuvieron la solución mucho antes pero no se dieron cuenta.

Antes de abandonar la cabaña le pregunté a Julia si quería venir conmigo, aun cuando no tenía idea de qué podría ocurrir ni de adonde nos llevarían las

pistas. Pensé que la capacidad organizativa de ella podría resultar útil en nuestra investigación. Ella dijo que no sabía mucho de cuestiones de seguridad informática y que era una ocasión para aprender algo más. Decidió venir a Sausalito, pero al comprobar las malas condiciones afuera optó por pasar del esquí.

Al final, a eso de mediodía emprendí el camino hacia el centro de esquí de fondo de Tahoe Donner. Había poca gente y las máquinas acondicionadoras habían dejado las pistas rápidas. Era bien entrada la tarde y la luz ya empezaba a menguar cuando

llamé a Julia para que viniese a recogerme. Partimos en su Mazda hacia la zona de la bahía sin tiempo para cambiarme de ropa.

El tiempo estaba empeorando y en la Interestatal 80 estaba montado el control de cadenas, lo que retardaba todavía más nuestra salida de las montañas. Apenas llovía cuando nos aproximábamos a San Francisco y cogimos por los caminos secundarios al norte de la bahía hacia Marin County. Alrededor de las 20:30 llegamos al Buckeye Roadhouse, un restaurante de moda en Mill Valley, cerca de Sausalito, donde está la sede de Well. Habíamos

planeado cenar allí como una oportunidad para reunimos con varios directivos de Well y otros amigos de la empresa, con el fin de alcanzar un acuerdo sobre cómo el servicio on-line iba a actuar ante los ataques. Andrew, que estaba alojado en casa de Pei, ya había llegado, y me puso al día antes de habernos sentado. Habían descubierto más software de teléfono móvil y diversos programas comerciales ocultos en otros emplazamientos de Well. Ese mismo día él había encontrado el software de un teléfono móvil Motorola.

Me habló también de un extraño aunque interesante descubrimiento. Una

de las cosas con las que se había encontrado era una extraña puerta trasera que el intruso empleaba en la Well. Dado que el atacante podía hacerse raíz en la Well siempre que quisiera, podía examinar libremente el correo electrónico de cualquier otro usuario. El equipo de seguimiento le sugirió revisar una cantidad de buzones, incluido el de Jon Littman, el escritor autónomo de Marin County, que poseía una cuenta legal en la Well. Littman estaba trabajando en un libro en el que detallaba las actividades de Kevin Poulsen, el pirata informático de la zona de la bahía a quien Justin Petersen había

implicado en el fraude de la estación de radio y que se hallaba todavía en prisión acusado de espionaje por la posesión de cintas de ordenador clasificadas como secreto militar. El año anterior había escrito también un artículo sobre Kevin Mitnick para *Playboy*.

Mientras Andrew había estado vigilando la red, había observado al intruso hacerse raíz y copiar un archivo de un ordenador remoto, una carta escrita por Kevin Ziese, oficial a cargo del Centro para la Guerra Informativa de la Fuerza Aérea en San Antonio, Texas. Después el intruso se registró como Littman y, en la propia cuenta de éste,

empezó a componer un mensaje que dirigió al escritor, con una nota en la línea correspondiente a Tema: "*Here you go:-) A visión from God*"[26]. A continuación intentó copiar el archivo de Kevin Ziese en el mensaje a Littman, pero se atascó, al parecer porque no pudo resolver cómo usar el software de edición de correo de Well.

Entonces abandonó el programa de correo y en cambio volvió nuevamente a la Well como raíz y simplemente añadió el archivo de Ziese al del buzón de Littman. La carta de Ziese contenía una larga exposición sobre los peligros propios del ataque IP-spoofing, y hacía

referencia a una conversación que mantuvo conmigo en la conferencia del CMAD. Al final de la carta, encima de la línea de la firma de Kevin Ziese, el intruso insertó una línea única que decía, "***_Hey john_ (sic), _Kevin is a good name:-)_"[27].

Andrew estaba convencido de que aquella era la pista definitiva que apuntaba hacia Kevin Mitnick. Yo vacilaba aún en alcanzar esa conclusión. Después de todo, en este mundo abundan los Kevin. Pero sin duda los dos nos preguntábamos lo mismo: ¿era consciente Littman de aquel canal privado creado por el intruso? No había

prueba de que lo supiese, o de que, en caso de haberse dado cuenta, aquello fuese algo más que una mofa del intruso, no un indicio de complicidad.

Entramos en el restaurante a reunimos con Bruce Katz y los directivos de Well. Nos habían reservado una larga mesa en la parte trasera. Bruce Koball, el programador de Berkeley, era uno de los invitados, al igual que varios veteranos miembros de la comunidad Well. Viejo amigo de Julia y de John Gilmore, Koball le dirigió una mirada de extrañeza cuando ella se presentó conmigo. Pero el estruendo en el Buckeye era tal que uno

apenas oía al que tenía al lado, de modo que Julia tenía pocas posibilidades de explicar tranquilamente lo que había ocurrido. En cualquier caso, yo no estaba conforme con lo ruidoso del lugar de reunión, tan escasamente propicio para celebrar una discusión confidencial en grupo. Parecía que desde el arranque mismo de la investigación estábamos violando los principios operativos básicos de la seguridad.

El Buckeye era bávaro, decorado con cornamentas de ciervo en las paredes. Yo pedí salmón y Julia un pastel de pastor, mientras que Andrew, aprovechando evidentemente el menú,

optaba por una ración de carne notablemente grande.

Bruce Katz estaba sentado a mi lado. Empresario cuarentón que había fundado y dirigido la compañía de zapatos Rockport antes de comprar Well, Katz tenía el cabello largo y escaso y su vestimenta informal lo hacía parecer un veterano de los años sesenta más que un hombre de negocios. A pesar del estrépito intenté ponerle al tanto de lo que habíamos descubierto. Como para enfatizar la urgencia de la situación, poco después de habernos sentado un empleado de Well que estaba haciendo el seguimiento del sistema allá en la

oficina llamó a Pei para decirle que el intruso acababa de utilizar a Well como punto de apoyo para forzar su entrada en Internex, otro servicio comercial de Internet con base en Menlo Park, California.

Yo conocía a Bob Berger, el ingeniero informático fundador de Internex, porque en varias ocasiones él había suministrado conexiones ISDN Internet para Sun Microsystems. Sabía también algo más acerca de Internex: le proporcionaba el correo electrónico de Internet a Markoff. Se me ocurrió que aquel podía ser el motivo del ataque, pero decidí no manifestar esa sospecha

hasta que pudiera investigar. Cuando Andrew y Pei resolvieron que llamarían a Internex por la mañana, procuré convencerles de que había que alertar a la compañía inmediatamente. Pero nadie pareció dispuesto a renunciar a la cena para localizar a un administrador de sistema de Internex que, encima, probablemente resultara difícil de encontrar a esas horas.

Katz quiso saber si el intruso era una persona que potencialmente podría dañar el sistema de Well. Como nosotros todavía no estábamos seguros de quién era, no le dimos una buena respuesta, y puesto que no teníamos la

menor idea de cómo reaccionaría si detectaba nuestro seguimiento, le dije a Katz que la posibilidad de represalias no podía excluirse.

La cuestión de los perjuicios está en el meollo del asunto. En el hampa informática se suele argumentar que el forzamiento de sistemas es moralmente defendible porque lo que los transgresores hacen es mirar, no revolver. A los piratas les gusta asimismo proclamar que en realidad, al poner de manifiesto la condición vulnerable de los sistemas, están contribuyendo a que los operadores mejoren la seguridad de los mismos.

Para mí esos razonamientos son ridículos. Puede que en otro tiempo, cuando las redes de ordenadores eran sistemas de investigación utilizados únicamente por ingenieros y estudiosos, esa actitud haya sido defendible, aunque no muchos de los ingenieros y profesores que conozco estuvieran de acuerdo con ello. En cualquier caso hoy, cuando empresas e individuos utilizan redes informáticas como elemento esencial en sus negocios y sus vidas, el razonamiento de los piratas equivale a afirmar que sería admisible que yo forzara la entrada en su casa y anduviese por ella, siempre que no tocase nada.

Aunque no se robe y sólo se copie, un material como el software de un prototipo de teléfono móvil sigue siendo una propiedad intelectual que fácilmente podría otorgar a un rival industrial una importante ventaja en el mercado competitivo. En los casos en que el pirata daña efectivamente el software, y aun el hardware, cuando fuerza su entrada, las empresas se ven obligadas a gastar decenas de miles de dólares en reparar los desperfectos. En un ordenador especialmente complejo suele requerir mucho esfuerzo el determinar simplemente qué ha sido dañado o qué se han llevado. No existe modo de

justificar la circulación clandestina en Internet, y lo peor de todo es que provoca que los usuarios de la red levanten fuertes barreras, destruyendo el espíritu de comunidad que ha sido por mucho tiempo carácter distintivo de la Red.

La conversación derivó al tema de la actividad del hacker y el pirata informático y de si la posibilidad de un daño efectivo era mucho mayor de lo que tendíamos a creer. Yo señalé que entre los delincuentes informáticos por lo general sólo cae el tonto. Katz no parecía satisfecho con esta línea de razonamiento, pues en realidad él quería

creer que estábamos ante una travesura inofensiva. Pero a mí el intruso de Well no me parecía inocuo. Le expliqué a Katz cómo funcionaba el husmeo de contraseñas, que podía permitir que un transgresor obtuviera el acceso no sólo a un único sistema sino a sistemas por toda Internet. También intenté explicarle que la única seguridad real consiste en el uso extensivo de la criptografía. El problema es que la mayoría de los criptosistemas actuales hacen a las redes más difíciles y costosas de usar, y en consecuencia la gente tiende a evitar su adopción.

Era evidente que Katz quería hacer

lo adecuado y que estaba dispuesto a aprender sobre seguridad informática. El problema era que como no entendía los detalles técnicos, según él mismo admitía, no estaba seguro de qué era lo adecuado. La Well maneja algunas conferencias privadas utilizadas por grupos consultores y otras organizaciones privadas. Él quiso saber si era posible al menos blindar esas conferencias y garantizar su seguridad.

Admití que desgraciadamente no. Le mencioné el uso de plásticos digitales, dispositivos del tamaño de una tarjeta de crédito que producen a cada minuto una contraseña nueva, pero cuando le

dije el precio reconoció que eran económicamente inaccesibles.

"¿No podríamos simplemente dejarlo fuera?", preguntó Katz. Quería saber si no bastaría con hacer que los once mil usuarios de Well cambiaran de contraseña.

"No creo que se pueda asegurar", respondí. A estas alturas, puesto que el intruso había sido raíz durante un lapso desconocido —de al menos muchos meses—, la Well tenía que suponer que todo el software de su sistema operativo había estado expuesto a riesgo. Además, no había forma de saber con certeza si todas las cuentas creadas por el pirata

habían sido identificadas. Puede que él hubiese escondido un puñado de cuentas dejándolas secretamente instaladas en reserva por si era detectado y necesitaba usarlas más tarde. Peor aún, estábamos bastante seguros de que podía hacerse raíz desde una cuenta normal.

"Si intentan cerrar las puertas cambiando las contraseñas y clausurando sus cuentas, es casi seguro que él habrá ocultado en alguna parte un programa "troyano" que le permita volver a entrar", dije. "Sólo que esta vez no sabrán dónde está".

Hice un resumen del software robado que Andrew y los demás habían

encontrado, y admití: “Todavía no sé exactamente qué está pasando, pero lo que sí sé es que hay una enorme cantidad de datos de gran valor comercial que alguien está ocultando allí”.

Empecé a comprender que los directores de Well buscaban soluciones fáciles y seguridades que yo no podía darles, porque aún no había siquiera visitado la Well. Les advertí que aquello era algo que quizá no pudiese lograr yo solo. Probablemente, requeriría también el auxilio de otros proveedores de servicios de Internet, así como de funcionarios policiales. Reunir datos en la Well era un comienzo, pero

para localizar al intruso posiblemente necesitaría en su momento contar con las compañías telefónicas para las medidas de rastreo. Intenté trasladar mi sensación de urgencia mientras explicaba todo eso, y les dije que en una situación como aquella uno tenía que avanzar a toda máquina o más valía que se olvidase el asunto. Una filtración que advirtiese al intruso de nuestra vigilancia y cualquier huella podría borrarse instantáneamente. La principal cuestión a resolver, para tener la oportunidad de rastrear al intruso, era si los directores de la Well estaban dispuestos a mantener abierto el sistema y no hacer nada que pudiera

revelarle que lo habíamos detectado.

El grupo de la Well escuchó atentamente, pero era evidente que se encontraban en un gran estado de ansiedad sobre cómo reaccionarían los usuarios tanto ante los forzamientos como ante la respuesta de la dirección. La Well ha sido siempre un lugar insólito en el ciberespacio. Además de atraer a un círculo de hackers y deadheads de la zona de la bahía, la Well se ha convertido también en punto de reunión favorito para los *digerati* de los medios informáticos, escritores sobre temas tecnológicos dedicados a la chismografía online y candidatos a estar

entre los críticos más vocingleros de cualquier paso erróneo por parte de la dirección de la Well. Por lo que yo había oído decir, la Well como comunidad posee su propio y arraigado sentido de los valores, y cualquiera que transgreda las convenciones del grupo lo hace a riesgo de convertirse en un paria social. Recientemente incorporado a ese mundo digital, Bruce Katz no podía permitirse ser marginado.

La vicepresidenta de administración de la Well, Claudia Stroud, que había sido la principal lugarteniente de Katz antes de que éste adquiriese la empresa, estaba nerviosa sobre la

responsabilidad que la compañía podría tener que asumir debido a nuestra operación de seguimiento. Aparte de la cuestión de un intruso que leía el correo de otras personas, Claudia señaló que entre los miembros de la Well había activistas del derecho a la intimidad que pondrían el grito en el cielo cuando se enterasen de que los investigadores habían estado filtrando sistemáticamente todo el tráfico de datos del sistema en la red.

"¿En qué sentido el mantener las puertas abiertas por más tiempo y no decir a los usuarios lo que está pasando rendirá mejores resultados?", quiso

saber.

Es probable que Claudia, que en su relación con Katz actuaba con la protectora familiaridad de una hermana mayor, mezclada con un fiel respeto a su mentor, estuviera simplemente haciendo su trabajo. Pero desde mi perspectiva, la única forma segura de que la Well retomase a la normalidad sería que diésemos con el intruso, y al parecer Claudia podría tratar de interponerse en nuestro camino.

“Hasta donde yo sé”, dijo ella, “la Well ha estado a la expectativa durante la última semana y media, y esta investigación tiene poco que mostrar”.

La Well había estado planeando transferir sus operaciones a un nuevo ordenador Sun Microsystems SPAR-Center 1000, y durante toda la cena la discusión estuvo volviendo al tema de con qué rapidez podrían y debían cambiarse al nuevo equipo. El reemplazo de todo el hardware y el software podría mejorar temporalmente su situación en materia de seguridad, pero complicaría nuestra operación de seguimiento.

Al término de la noche, Katz estaba impresionado por la extensión del forzamiento y la propia cantidad de software, información de tarjetas de

crédito y archivos de datos que habíamos descubierto. Parecía haber resuelto que la única forma de lograr seguridad para la Well era cerrarla y transferir su operación a un nuevo ordenador con software fiable. Y no obstante, nosotros habíamos dejado clara, al parecer, nuestra convicción de que la mejor forma de garantizar la seguridad consistía en poner fuera de combate al pirata.

"Les daré un poco más de tiempo", dijo al final Katz.

Después de la cena seguimos a Pei y Andrew, bajo la ligera neblina que

había reemplazado a la lluvia del día, hacia el cercano Holiday Inn de San Rafael, donde íbamos a alojamos Julia y yo. Andrew conducía el Cherokee rojo que la Well había alquilado para él y al cual le había dado por llamar el +4 Jeep de Intimidación, en referencia a las poderosas armas imaginarias que se otorgan a los jugadores en juegos de fantasía y rol como "Dragones y mazmorras"

Mientras seguía al *jeep*, pensé: "¿Por qué habrá creído la Well que nuestra investigación requería un vehículo con tracción en las cuatro ruedas?". Mi segundo pensamiento fue:

“Va a ser difícil aparcar, pero al menos podemos hacerlo sobre lo que sea”.

Levord Burns, el agente del FBI, le había pedido a Andrew que lo llamase después de la reunión para contarle lo que la Well hubiera resuelto hacer. Por tanto, aunque era medianoche cuando llegamos al hotel —y las 3 de la mañana en Virginia, donde vive Burns—, le telefoneé. Atendió medio dormido, pero las llamadas en medio de la noche forman parte de la rutina de un agente de campo del Bureau, así que un momento después ya estaba hablando en el tono formal y un tanto gris al que nos tenía acostumbrados.

Yo le resumí lo que el seguimiento había revelado hasta el momento y le dije que al día siguiente iría al centro operativo de la Well a examinar los datos. Durante la conversación me dijo que a pesar de haber sido designado como principal agente en funciones para delitos informáticos, tanto su formación en materia de tecnología como su experiencia en casos relacionados con el robo de información, eran escasos.

"Generalmente me ocupo de robos de bancos, Tsutomu", declaró.

Concluí la conversación comunicándole que la Well había accedido a permitir que continuásemos

el seguimiento durante un tiempo, y él respondió que esperaría a ver a dónde nos llevaba.

Andrew y Pei se fueron después de la llamada. Antes de dormirnos Julia y yo, ella me dijo que ya no sentía la sensación de tener un hogar, que en las últimas semanas cualquier hotel en el que estuviésemos alojados parecía convertirse en uno. "Y hablando de hoteles", añadió, "éste es decididamente un paso atrás con respecto a los lugares en los que hemos estado alojados últimamente".

Llegamos a la Well alrededor de las once y media de la mañana del martes.

El mediocre edificio de la oficina no se parecía en nada a la vecina sede, ubicada de espaldas a una hilera de viviendas flotantes en un maloliente barrio de Sausalito, donde el servicio online empezó en 1987.

Las oficinas de la *Whole Earth Review* fueron sede original, y la Well —acrónimo de Whole Earth 'Lectronic Link— estaba estrechamente vinculada con Stewart Brand, uno de los Merry Pranksters de Ken Kesey y creador de la revista y del *Whole Earth Catalog*. Brand, primer portador de la antorcha del movimiento de retorno-a-la-tierra en los años sesenta, había escrito en 1972

un artículo para la revista *Rolling Stone* en el cual describía a un loco grupo de investigadores del Centro de Investigación de la Xerox en Palo Alto que estaban intentando reinventar la informática. En pocos años más lo habían conseguido, creando el precursor del ordenador personal.

A finales de los setenta, cuando emergió por vez primera, la industria del ordenador personal era todavía mayormente un conjunto de aficionados con un fuerte sesgo contracultural. A finales de los ochenta la Well reflejaba esa misma mezcla ecléctica de hackers y *hippies*. Los miembros de la Well

empezaron a conectarse primero desde los alrededores de la zona de la bahía, y más tarde desde todo el país, para charlar sobre las cosas que tenían en la cabeza. Cuando se inició el furor de la Autopista de la Información, docenas de periodistas escribieron artículos sobre la Well, otorgándole una importancia desproporcionada en relación al número de sus miembros. De forma que gozaba de un cierto prestigio en 1994 cuando Katz, que era ya inversor de la Well, adquirió el resto del grupo sin fines de lucro que la controlaba y se embarcó en un ambicioso plan para convertir la empresa en un importante y lucrativo

servicio nacional.

Una de sus primeras acciones fue cambiar la sede de la Well del barrio de las casas flotantes a un complejo de oficinas situado a varias manzanas de distancia, adonde llegamos nosotros el martes por la mañana. Pei nos precedió, a Julia y a mí, a través de un amplio recinto en el que el personal de apoyo y el equipo administrativo trabajaban en PCs y Macs, y nos condujo hasta la parte trasera, donde estaban los sistemas informáticos y los servidores de archivos. A lo largo del vestíbulo había un amplio armario abierto con un estante de modems para que los usuarios

pudiesen conectar y desconectar con la Well.

Yo diría que Pei, una mujer de aproximadamente la misma edad de Julia, era competente, brillante y capaz, pero dejaba una cierta impresión de inseguridad. A mediados de 1994, cuando ella empezó en la Well, el trabajo había sido cuestión de una sola persona, pero en poco tiempo se encontró supervisando a cuatro o cinco, y era evidente que se sentía inexperta y falta de confianza en cuanto al aspecto gerencial de su tarea. Se quejó de lo difícil que era conseguir que la Well le prestara atención, especialmente en lo

concerniente a la seguridad. Había sido precisa la llegada de Andrew como experto de fuera para recomendar acciones y proporcionarle el apoyo que ella necesitaba.

Julia y yo nos habíamos presentado a tiempo para la comida —de hecho, para nosotros el desayuno—, que traían en ese momento para el pequeño grupo de personas encargadas de los sistemas que hacían funcionar la Well bajo la dirección de Pei. Con objeto de no dar a conocer a nadie que no tuviese necesidad de saberlo nuestras actividades, habríamos de permanecer ocultos en el pequeño cuarto en la parte

trasera del edificio donde Andrew venía operando desde hacía una semana. Cuando entramos, él estaba pasando por fax a Levord Burns una página con información que el dispositivo captador en la UCSD había detectado entre los mensajes del buzón de voz que habían dejado para mí. Esa misma mañana Andrew había sabido que los mensajes habían venido por las líneas de larga distancia de Sprint; eso quería decir que probablemente el que nos llamaba no estaba en San Diego. Andrew le estaba enviando la información a Burns con la esperanza de que el FBI pudiera conseguir de la compañía telefónica una

localización precisa.

También había seguido trabajando sobre sus sospechas de que nos estábamos enfrentado a Kevin Mitnick. Más temprano había llamado a la oficina local del FBI, que lo remitió a Kathleen Carson, una agente en Los Ángeles al parecer encargada de la investigación del Bureau sobre Mitnick. Ella se había mostrado únicamente dispuesta a decirle algunas cosas, no muy útiles por otra parte, como los nombres de una cantidad de compinches de Mitnick —de antes y actuales—, incluidos Kevin Poulsen, Justin Petersen, Eric Heinz, Lenny DeCicco, Ron Austin y Lewis Depayne.

Dijo que el FBI sabía de una cuenta informática recientemente usada por Mitnick, llamada *marty*, pero no reveló ninguno de los emplazamientos específicos de Internet implicados. Cuando Andrew le citó los emplazamientos que conocíamos relacionados con el forzamiento de la Well, ella se limitó a gruñir un par de veces.

Mientras comíamos las suaves veneras, camarones y guisantes blancos chinos, y el pollo *kung pao* que nos habían servido, empecé a hacer balance de lo que ahora sabíamos. Desde la noche anterior la Well había visto más

tráfico hacia y desde Internex, de modo que llamé a Bob Berger y le dejé un mensaje advirtiéndole que Internex había sido forzada. Después llamé a Markoff y lo alerté de que alguien podría estar leyendo su correo electrónico. Me dijo que hacía más de un año un mensaje privado dirigido a él en la Well había aparecido en un grupo de noticias público, de modo que había dejado en gran parte de utilizarla para el correo y en cambio había dispuesto su cuenta de la Well para enviar mensajes a su cuenta *New York Times*, que era manejada por Internex. Ahora tampoco la Internex parecía muy segura.

Como Internet se había convertido en una herramienta esencial para la mayoría de los periodistas especializados en tecnología y puesto que a todo periodista tiene miedo de que otro se le adelante en las noticias, Markoff estaba naturalmente preocupado porque alguien fuera a mirar por encima de su hombro y leyera su correspondencia. Pero accedió a no hacer nada que pudiera alertar a algún espía y a esperar a ver qué resultaba de mis investigaciones. Tomó, no obstante, una precaución. El ordenador de su despacho en la oficina del *Times* en el centro de San Francisco se conectaba

automáticamente con Internex cada hora para comprobar si había correspondencia nueva. Markoff resolvió aumentar esa frecuencia a veinte minutos, para que el correo en espera en Internex estuviera expuesto por menos tiempo.

Después de las llamadas me puse a atender la operación de seguimiento en la Well, que evidentemente no marchaba bien. Pei estaba recogiendo parte de la información en una estación de trabajo Sun utilizando un programa estándar de husmeo llamado “fisgón”, en tanto que Andrew recogía datos distintos en un RDI portátil que había conectado a la

red interna de la Well. Esa disposición de las cosas me molestó, porque me impedía comparar fácilmente los respectivos hallazgos de las máquinas de Pei y de Andrew. Peor aún, nadie parecía estar haciendo mucho por analizar los datos que iban obteniendo.

Y sin embargo, ya había aparecido cierta información digna de interés. Además de la cuenta Computers, Freedom and Privacy, y la cuenta dono que Andrew había estado vigilando, había al menos otras cuatro que estaban siendo utilizadas por el intruso: fool, fairdemo, nascom y marty; otra indicación de que el intruso podría ser

Mitnick. Todas ellas eran cuentas demo, de modo que no había registros de facturación. Eso sugería que quien estaba detrás de los forzamientos poseía un conocimiento detallado de las prácticas contables de la Well y había establecido cuentas —o se había apoderado de otras— en las que una factura no revelase a los tenedores de las mismas que alguien estaba aumentando sus cuentas con actividades no autorizadas.

Pei y Andrew habían generado también una lista de otros emplazamientos de Internet de los que ahora sabían que el intruso venía o a los

que se dirigía por Internet. Eso incluía a Internex; a Colorado SuperNet, un servicio comercial de Internet con base en Boulder; a Motorola Corporation; a NandoNet, el servicio online de la *Raleigh News and Observer*; y a Intermetrics. Había también conexiones desde un sistema Unix de acceso público con base en la ciudad de Nueva York cuyo nombre parecía sospechoso: *escape.com*.

Había asimismo una lista de idas y venidas desde Netcom de los números de tarjeta de crédito cuyos clientes habían sido ocultados en la Well. El día anterior, Andrew había llamado a

Netcom y les había hecho saber que uno o más intrusos habían estado escudriñando sus sistemas.

Mientras Pei y Andrew hablaban de sus esfuerzos, me pareció que habían estrechado prematuramente el campo de sus respectivas averiguaciones. Parecían decir: "Estamos mirando esas cinco cuentas robadas y observando el uso que se ha hecho de ellas".

Era una actitud que yo había temido la noche anterior, cuando hablé con Andrew desde Truckee.

"¿Cómo sabes que eso es todo lo que hay?", le pregunté. Era obvio que necesitábamos echar una red más

amplia.

Andrew tenía muchos papeles grapados juntos. Algunos tenían las listas de las horas de entrada y de acceso a archivos, pero me resultaba realmente difícil decir qué eran. Nada estaba realmente dispuesto en un orden racional que resultara discernible. Para coger al intruso era necesario que llevásemos a cabo de forma sistemática lo que la comunidad de inteligencia llama análisis de tráfico. Más que mirar lo que había en cada conexión individual a mí me interesaba ver cuándo tenían lugar las conexiones, de dónde venían o adonde iban y qué otra

cosa ocurría simultáneamente. Y antes de poder encontrar el camino hacia el cuadro mayor, yo necesitaría entender la disposición de la red interna de la Well y descubrir un único punto en el que pudiésemos ver toda la información de venida y de ida a Internet. La Well había fijado una reunión para las 2 de la tarde con un abogado del Departamento de Justicia y con el FBI para discutir los forzamientos y el software robado. Yo iba a servir como experto técnico designado.

La reunión tuvo lugar en las oficinas del Rosebud Stone Group, la compañía

de *holding* de Katz situada a sólo un par de manzanas de la Well. Asistimos Julia, Andrew y yo, así como Pei, Claudia y el abogado de la Well, John Mendez. Representando al Gobierno estaban Kent Walker, fiscal adjunto en San Francisco, y dos agentes del FBI de sendas oficinas locales: Pat Murphy, de San Francisco, y Barry Hatfield, de San Rafael. Yo había oído hablar de Murphy, que anteriormente había estado vinculado con asuntos de delitos informáticos y cuestiones criptográficas en Washington, por el Departamento de Justicia. Tenía la reputación de ser duro en materia de delitos informáticos, pero

yo ignoraba totalmente cuál era su preparación técnica. Al conocerle ahora personalmente, un treintañero de uno ochenta y complexión atlética, me impresionó como poseedor de mente ágil y talante agresivo.

Andrew y Pei empezaron a describir algunos de los resultados del seguimiento de tecleo captados durante la semana anterior y hablaron de analizar los esquemas de comportamiento del intruso como si se tratara de estudiar un espécimen. Escuchándolos me puse cada vez más impaciente. Al igual que los que participan en las conferencias

académicas sobre seguridad informática centradas en los resultados teóricos más que en los hechos reales, ellos se estaban interesando más en las clasificaciones que en la acción directa.

"¡Todo eso está muy bien, pero es pura anatomía!", interrumpí, sin poder contenerme más. "¡Y lo que estamos buscando es un ser vivo!".

Por un momento reinó el silencio en la habitación, pero mi explosión tuvo el efecto de volver a centrar la discusión, no en lo que podíamos hacer para proteger a la Well de la amenaza, sino en mi punto de vista, consistente en que la única forma de asegurar a la Well

contra la amenaza era eliminar ésta. En lugar de adoptar una postura defensiva, necesitábamos pasar al ataque.

Empecé bosquejando un plan para establecer una base de operaciones en la Well y luego movernos rápidamente en cualquier dirección a la que nos condujeran nuestras operaciones de seguimiento. En la práctica, mi plan suponía una organización semejante a la de una expedición para escalar una montaña. Tendríamos un equipo de avanzada y un equipo de base. Avanzaríamos impetuosamente por la red hasta identificar al intruso en una localización específica. ¿Y cuando

efectivamente lo encontrásemos? Supuse que eso era problema del FBI.

En situaciones como ésa, cuando intento llevar la batuta, tiendo a hablar muy rápido. Más tarde me enteré de que había abrumado a los agentes del FBI, ninguno de los cuales poseía muchos conocimientos técnicos. "No entendí una palabra de lo que dijo", le contó después a Walker uno de ellos. "Hablaba a 9.600 baudios, y yo sólo puedo oír a 2.400".

Para hacer comprender mi idea de que estábamos combatiendo a un oponente vivo, una forma de vida animal al otro extremo del cable, utilicé un

mensaje de voz para llamar a mi buzón de voz en San Diego. Allí habían dejado un nuevo mensaje, enviado la semana pasada y que yo había escuchado por primera vez el día anterior. Parecía que mi antagonista estaba contrariado por que yo hubiera volcado sobre él los focos de la publicidad exponiendo sus mensajes previos en la Red como *tweedledum* y *tweedledee*.

"Ah, Tsutomu, mi ilustrado discípulo", empezó diciendo con un falso acento asiático, y a continuación se puso a barbotar como quien no ha ensayado perfectamente su parlamento: "Veo que… utilizas mi voz para

Newsweek… la pones en *Newsweek*. Y la pones en la red. ¿No sabes que mi voz *kung fu* es la mejor? ¡Mi voz de *kung fu* es estupenda! ¿Por qué pones mi voz natural en la red?".

"Eso no está bien. ¿No te he enseñado, saltamontes? Debes aprender del maestro. Yo sé… yo conozco todas las técnicas y todos los estilos. Sé el estilo garra de tigre. Conozco la técnica de la grut… de la grulla. Sé la técnica del mono loco".

"Y conozco también rdist y sendmail. Y tú la pones en la red. Estoy muy decepcionado, hijo mío".

Era evidente que había conseguido

la atención de mi intruso. Que era lo que yo había querido. Había acudido al cebo, y con los datos de localización de la llamada tal vez pudiésemos empezar a afinar la puntería para dar con su ubicación. La reproducción del mensaje era asimismo para todos un recordatorio de que íbamos tras un delincuente real, no unas simples líneas de mandatos de Unix.

Al poco rato interrumpió una conferencia telefónica de Netcom, la empresa que había conseguido que un ladrón se llevase la información de las tarjetas de crédito de sus clientes. Había tres vicepresidentes de la misma al otro

extremo de nuestro fichero sonoro y parecieron muy ansiosos por cooperar, dándonos una cantidad de nombres de contacto. Por el tono de voz sospeché que les preocupaba la posibilidad de que les hicieran responsables de los ataques contra la Well y querían dejar claro ante los funcionarios gubernamentales presentes que estaban dispuestos a cooperar en la investigación. Walker y los agentes del FBI dijeron que volverían a estar en contacto.

Ese día, más temprano, mirando la hoja que mostraba los registros de entrada a una de las cuentas

secuestradas de Well, yo había reconocido inmediatamente uno: *art.net*, la máquina de Lile en casa de Mark Lottor. Era la misma que Kevin Mitnick había controlado el otoño anterior. Cada vez eran más los indicios que apuntaban hacia Mitnick, tanto en la Well como en mi caso, y los agentes del FBI, Murphy y Hatfield, empezaron a revisar sus archivos sobre él.

Murphy dijo que el Bureau tenía un montón de información pero que no podía compartir mucha con nosotros, sólo la que era de dominio público. Para determinar lo que podía facilitamos, el agente decidió llamar a la oficina del

FBI en Los Ángeles. L.A. se mostró renuente a soltar nada pero concedió a Murphy autorización para examinar el material que tenía en su portafolios y leernos párrafos "purgados".

Mientras él revisaba el archivo yo me arrimé a mirar por encima de su hombro y vi un documento con el sello "Confidencial" y un póster de Kevin Mitnick con la palabra "Buscado".

Murphy leyó en voz alta los lugares presumiblemente forzados desde que Mitnick pasó a la clandestinidad a fines de 1992: la oficina de SunSoft en Los Ángeles; la subsidiaria de software de Sun Microsystem; la Universidad de

California del Sur; Colorado SuperNet; Novatel, fabricante de teléfonos móviles; Motorola; Pan American Cellular; Netcom; Fujitsu; Qualcomm; Oki; US West; y L.A. Cellular.

Si estaban en lo cierto, Mitnick estaba verdaderamente obsesionado por los teléfonos móviles.

Los documentos del FBI describían también una incursión en Seattle el otoño anterior en el cual el objetivo había evitado por poco ser capturado. Sin saber en aquel momento quién era su sospechoso, funcionarios de seguridad de McCaw Cellular, una empresa privada de investigación, y la policía de

Seattle, habían llevado a cabo una operación de vigilancia para localizar a alguien que estaba haciendo llamadas fraudulentas por teléfono móvil y utilizando un ordenador y un modem. Después de varios días de seguir a su sospechoso fueron a su apartamento, próximo a la Universidad de Washington, como nadie contestó, echaron la puerta abajo. Los funcionarios confiscaron el equipo, que incluía un ordenador portátil Toshiba T4400 y gran cantidad de elementos de telefonía móvil, y le dejaron una orden de registro. Después la policía de Seattle montó guardia en el apartamento

durante varias horas y se fue. El sospechoso, que por los datos de su ordenador fue más tarde identificado como Mitnick, regresó al apartamento, habló brevemente con el casero y desapareció.

"¡Jo!", pensé.

Otro de los documentos del FBI se refería al posible paradero de Mitnick. La oficina del FBI en Los Ángeles poseía información de que, además de en Seattle, había estado en Las Vegas y, últimamente, en Boulder, donde los agentes de Los Ángeles creían que podía encontrarse aún. En efecto —nos dijeron los agentes—, al parecer la oficina de

Los Ángeles estaba trabajando con los operadores de la Colorado SuperNet en un intento de seguimiento de las actividades del intruso y confiaba en estar acorralando a su presa.

Murphy me preguntó si me parecía razonable que Mitnick pudiera estar operando con el modem de su ordenador a través de un teléfono móvil. Le repliqué que no parecía muy posible. Yo lo había intentado, y la fiabilidad de transmisión era bastante pobre, pues las llamadas tendían repetidamente a cortarse. La transmisión de datos habría sido creíble con un potente teléfono de tres vatios, pero con las unidades

manuales de 0.6 vatios que el FBI creía que Mitnick prefería, no parecía muy práctico. Exigiría una enorme dosis de paciencia, porque los modems tienden a trabajar mal con los cortes automáticos que se producen en la red de telefonía móvil mientras los teléfonos pasan de célula en célula.

"Si él continúa con el móvil, su firma será fácilmente identificable, porque tendrá que reconectar una y otra vez", les dije. Tomé nota mentalmente de que debía buscar cualquier señal reveladora de unas conexiones cortadas reiteradamente que pudiéramos haber recogido en nuestros datos de tráfico en

la red.

Por último, el FBI aceptó compartir con nosotros las cuentas y las contraseñas que Mitnick había estado usando en otros sistemas, incluida la cuenta marty. La contraseña para una de estas cuentas era *pw4nl*. Se nos ocurrió que la traducción más obvia era "contraseña para Holanda"[28], país en el que el hampa informática continuaba sumamente activa a pesar del hecho de que el Gobierno holandés había finalmente aprobado leyes contra delitos de esa naturaleza. Por el seguimiento de Andrew nos habíamos enterado ya de que el intruso de la Well tenía en una

máquina holandesa una cuenta llamada *hacktic.nl*, frecuentada por piratas. La operaba un grupo informático de anarquistas holandeses conocido como Hacktic.

Yo no estaba seguro de cuánto crédito dar a cualquier dato del FBI, dado que en gran parte provenían del ordenador confiscado en Seattle, que Mitnick sabía que estaba en posesión de ellos.

Hubo alguna discusión sobre si Mitnick podría ser violento y si la Well corría físicamente algún riesgo.

"Ya saben que John Markoff escribió el libro sobre Mitnick", dije yo.

"¿Por qué no le telefonean y le preguntan a él?".

A los agentes del FBI no les pareció muy adecuada la idea de incorporar a un periodista a la reunión, pero Walker impuso su opinión favorable. Cuando lo tuvimos al habla, Markoff explicó que todo lo que sabía sobre Mitnick se encontraba en *Cyberpunk* o en su artículo del mes de julio en la primera plana del *Times*. Dijo asimismo que él también era escéptico en cuanto a que Mitnick fuera el culpable. Que le habían dicho que el forzamiento había sido obra de un oscuro grupo de gente que actuaba conjuntamente y del que Mitnick no

formaba parte. Pero si era Mitnick, dijo Markoff, no creía que fuera capaz de un comportamiento violento. Una historia narrada en *Cyberpunk* revelaba que cuando en una de sus primeras detenciones, a comienzos de 1980, un agente de paisano de Los Ángeles lo obligó a detenerse en la autopista, Mitnick se puso a llorar.

Una vez que todos nos declaramos satisfechos en ese aspecto, presioné a Walker en cuanto a los límites legales de la operación de seguimiento que planeábamos. Una de las principales cuestiones relativas a la intimidad en Internet tiene que ver con los derechos y

responsabilidades de los operadores de sistemas comerciales. A medida que los paquetes de datos fluyen a través de sus redes, los operadores de sistemas tienen la posibilidad de registrar o grabar cada pulsación de teclado y cada fragmento de información, ejecutando en los hechos un seguimiento de todas y cada una de las acciones y conversaciones. Los sniffer de paquetes como los que habíamos instalado en la Well pueden emplearse tanto de forma responsable como irresponsable. Al instalar nuestros filtros en la Well intentábamos capturar paquetes exclusivamente en las sesiones sobre las que establecíamos el

seguimiento. A menudo era difícil establecer claros límites. No había forma de saber si había uno o varios intrusos, y parecía que él o ellos utilizaban media docena o más de cuentas separadas. Existía una posibilidad cierta de que algunos datos inocentes cayesen en nuestras amplias redes. Hicimos un breve repaso de las disposiciones de la ley sobre Intimidad de las Comunicaciones Electrónicas, buscando pautas sobre lo que podíamos y no podíamos hacer en nuestra investigación. La ley permite el uso del seguimiento cuando se sospecha fraude o delito. Walker y los agentes del FBI

dijeron que lo que estábamos haciendo debía estar cubierto por esas leyes.

"Esta es una situación en la que usted no va a actuar como apoyo técnico nuestro", dijo Walker. "Nosotros vamos a servirle de respaldo legal y administrativo". Su actitud me impresionó. Hasta ese momento yo no había tenido realmente muchas esperanzas de que tuviésemos oportunidad de descubrir al atacante, pues había visto antes muchas de estas investigaciones echadas a perder por el FBI.

Les dije que necesitaría varios STU-III, unos teléfonos codificados

especiales del Gobierno para la seguridad de las comunicaciones. Kent dijo no saber nada de los STU-III, pero que él tenía acceso a montones de teléfonos Clipper, basados en el chip de codificación de datos con puerta trasera de escucha oculta que la Agencia Nacional de Seguridad había estado tratando que el Gobierno y el público adoptaran… sin demasiado éxito. Yo manifesté que prefería los STU-III.

Por último, Claudia y Méndez plantearon la preocupación de la Well sobre sus posibles responsabilidades en caso de mantener abierto el sistema mientras llevábamos a cabo el

seguimiento. Preguntaron si el Departamento de Justicia podía darles una carta respaldando la decisión de continuar operando como de costumbre, y Walker accedió a proporcionarles ese documento.

La reunión concluyó cerca de las cuatro, y Julia y yo nos quedamos en la sala de conferencias para que yo contestara a varias llamadas que había recibido en mi teléfono móvil mientras estaba reunido. Una era de Mark Seiden, un hacker de Unix y experto en seguridad informática que había aceptado ayudar a Internex con sus problemas de seguridad. Al llegar yo a

la Well esa mañana, Andrew me había dicho que la noche anterior el equipo de seguimiento había visto al intruso trasladar a Internex un archivo de 140 megabytes con el contenido de mi directorio en Ariel, y yo empezaba a experimentar la sensación de que estábamos tratando con una ardilla enterrando sus nueces, escabulléndose de aquí para allá y escondiéndolas en diversos agujeros por toda Internet. Cuando respondí a la llamada de Seiden le conté lo del archivo y le dije que lo quería eliminado. Pero como no queríamos advertir al intruso, acordamos que Seiden borraría el

archivo y a continuación le enviaría al usuario verdadero un mensaje que dijera algo así como: “Hemos borrado su archivo porque ha excedido usted el espacio asignado. Le hemos indicado una y otra vez que no dejase grandes archivos tirados por ahí”.

Cuando me hube ocupado de todas las llamadas, Julia y yo regresamos andando a la oficina de Pei en la Well. Claudia había estado dando vueltas por allí, aguardando para presentarme el mismo documento que había obligado a Andrew a que firmara, un compromiso de no divulgación para impedirme mencionarle a cualquiera ajeno a la

Well cualquier cosa de la que me enterase sobre la situación. El papel le había creado ya un grave problema a Andrew, que había intentado dar aviso a otras compañías de que sus respectivos sistemas habían sido forzados y les habían robado software.

Debido al compromiso, se había visto limitado a llamar a la gente y decirle: "No puedo decirle quién soy ni darle detalles de lo que ha ocurrido, pero quiero que sepa que tiene un problema de seguridad". Era una limitación con la que resultaba imposible trabajar, y yo le había sugerido ya que hiciera caso omiso de

esa parte de la restricción.

Claudia estaba tratando además de imponer su convicción de que todo el software robado encontrado oculto en la Well era propiedad de la misma. Eso estaba creando otro tremendo dolor de cabeza para Andrew en relación con su propósito de hablar con las víctimas del robo y conseguir su ayuda. Yo le expliqué a ella que la propiedad intelectual de otra empresa no se convertía automáticamente en propiedad de la Well sólo porque alguien la hubiese robado y ocultado allí. Su preocupación era que si se descubría que la Well era la zona de preparación

de forzamientos en Internet, la empresa sería responsable de cualquier perjuicio resultante. Yo le señalé que la Well podía verse ante problemas de responsabilidad igualmente graves si llegara a saberse que el servicio estaba al tanto de forzamientos en otros sitios y dejaba de notificar a las víctimas, tal y como ya había sucedido en algunos casos.

Finalmente, intenté sin éxito convencerla de que lo que más debía importarle a la Well, para que tuviésemos alguna posibilidad de resolver el problema, era allanar los obstáculos y permitirnos seguir adelante

a toda marcha.

“Tsutomu, tengo que pedirle que firme esto para proteger a la Well de posibles responsabilidades en la investigación”, repitió ella.

Yo me quedé mirándola como diciéndole, “No tengo la menor intención de firmar una cosa tan ridícula”, pero al final el tacto prevaleció en mi ánimo. “Creo que no puedo aceptar esto ahora mismo, pero lo revisaré y después hablaremos”. Lo que en realidad quería decir era, “¿Qué parte de ‘no’ es la que no entiendes?”. El hecho de que hubiera aceptado echar un vistazo al documento pareció aplacar

a Claudia, y mientras regresaba a mi trabajo no pude evitar pensar en lo que un amigo me había dicho una vez: la diplomacia es el arte de decir "lindo perrito" hasta que encuentras un garrote.

Tras haber pasado la mayor parte del día liado con los burócratas, pude por fin dedicar mi atención a tratar de entender la topología de la red de la Well. Andrew había conectado un RDI PowerLite a la red en el sitio adecuado para que todos los paquetes de la Well fluyesen por delante de su ordenador, pero estaban ocurriendo cosas raras. Pronto se hizo evidente que la distribución de comunicaciones de la

Well era una confusión total, de modo que más de la cuarta parte de los paquetes en la red interna se movían de forma en extremo ineficaz y poco directa. Uno de los ordenadores de distribución se estaba lavando las manos y remitiendo los paquetes a otro para que éste decidiese cómo enviar cada manojo de datos a su dirección correcta. Me sentí un poco como el fontanero que aparece en casa de un cliente y tiene que decirle al dueño que alguien ha hecho pasar la tubería del cuarto de baño a través del dormitorio.

El desarreglo de la distribución no era problema mío. Lo importante era que

empezáramos lo antes posible a registrar los paquetes pertinentes. Escribimos diversos filtros para capturar paquetes tanto de entrada como de salida de la Well. Elaborando una lista de todos los sitios comprometidos que conocíamos y registrando después otros lugares de donde sospechásemos que podrían provenir los datos tendríamos una buena posibilidad de contar con una completa relación de las actividades del intruso.

Lo que yo tenía pensado era empezar colocando en su sitio un vasto conjunto de filtros en dos ordenadores separados para estar seguros de disponer de redundancia[29]. Quería explorar durante

breves periodos una cantidad de sesiones para detectar la reveladora firma de nuestro intruso y después volver a estrechar el foco de vigilancia. De esa manera podríamos ver si estábamos pasando por alto alguna actividad encubierta. Pero cuando pusimos en marcha el sistema me di cuenta de que el de la Well era el más ocupado con el que había tratado nunca y de que había un exceso de datos para efectuar el seguimiento en ambos sentidos, de modo que lo reduje al de los datos entrantes. Hacia las diez de la noche creí haber comprendido lo que llevaría tener instalados los sistemas de

registro de paquetes y filtrado, así que Julia, Andrew y yo nos fuimos a cenar.

Fuimos los tres en el +4 Jeep de Intimidación a La Cantina, un restaurante mexicano en Mill Valley que Julia conocía. Según la leyenda de la casa, el padre de Carlos Santana solía tocar allí en un grupo de mariachis.

En el curso de la cena hablamos del problema en que se había metido Andrew por estar ayudándome en el norte de California. Mi acuerdo con Sid Karin había sido que el SDSC contribuiría pagando su salario durante unas semanas, pero por alguna razón los

de la administración no se habían enterado. Le dije a Andrew que yo le había puesto más temprano una llamada a Sid sobre ese tema y que al parecer se iba a arreglar. También dedicamos un rato a charlar sobre la carrera académica de Andrew y su búsqueda de un nuevo director de tesis. Yo le dije que estaría encantado de proporcionarle consejo y orientación, pero que él iba a tener que buscarse a algún otro que fuese oficialmente su director y manejase las cuestiones administrativas.

En algún momento después de las once preparamos una lista de las cosas que debíamos hacer para tener nuestros

sistemas de seguimiento completamente en su sitio, y regresamos a la Well. Pei se había ido a su casa a una hora razonable, pero varias personas continuaban aún realizando el seguimiento en el reducido cuarto trasero que era el centro operativo de la red de la Well. Estábamos capturando decenas de megabytes de datos cada hora, mucho más de lo que podían contener nuestros discos, incluso de una noche para otra, de modo que reforzamos nuestros filtros.

Después de medianoche empecé a revisar el archivo de registro de datos que habían recogido durante el día

anterior e inmediatamente encontré algo: las pulsaciones de teclado del intruso visibles en el directorio y el buzón de Markoff. Estudiando los datos comprendí fácilmente cómo había encontrado su camino a Internex: simplemente había mirado un archivo del directorio de Markoff en la Well que automáticamente dirigía su correo electrónico a Internex. Vi también que además de los de Markoff y Littman, estaba revisando otros buzones. Lo había hecho con el de Emmuel Goldstein, editor de la revista 2.600 para fanáticos del teléfono, llamado Eric Corley en la vida real; con el de Ron

Austin, programador de California del Sur que había tenido problemas por una cantidad de delitos informáticos; y con el de Chris Goggans, miembro reformado del mundo informático subterráneo que publicaba una revista alternativa sobre ordenadores online llamada *Phrack*.

Hacia las dos de la mañana habíamos hecho todo lo que razonablemente podíamos hacer. Julia y yo no queríamos pasar otra noche en el Holiday Inn, así que atravesando el Golden Gate entramos en la ciudad. Acabamos en el cuarto de huéspedes de la casa de Dan Farmer, próxima al

parque. Yo había llamado por la mañana a Dan para decirle que habíamos encontrado en la Well el código fuente de su programa SATAN y su correo electrónico. Tenía la esperanza de hablar con él sobre los forzamientos, pero cuando llegamos él ya se había ido.

Lo haríamos después. Por el momento, yo sabía que habíamos tendido nuestras redes abarcando lo más posible. Era cuestión de aguardar a ver qué podíamos atrapar. Ya habíamos captado un tráfico sospechoso proveniente de la Colorado SuperNet, la Intermetrics y la Netcom, y al parecer pronto tendríamos que adoptar una

decisión sobre qué camino tomar para dirigimos corriente arriba en la Internet. Alguien había establecido ya las reglas, y ahora que me incorporaba al juego yo había decidido zambullirme y no mirar atrás.

10. "¡Panda de ineptos!"

Regresamos a la Well a última hora de la mañana siguiente. Cualquier duda acerca de mi compromiso con la cacería se había disipado el día anterior. Siempre he estado convencido de que la forma en que se hace una cosa es tan importante como el hecho de hacerla, y si iba a dar caza a aquel ladrón, me parecía inaceptable enfocar el desafío

sin poner en ello toda la decisión y concentración de que fuera capaz.

Parecían irse acumulando bastantes datos que apuntaban a Kevin Mitnick como el que estaba sentado con un ordenador portátil, lanzando ataques sistemáticos a través de Internet, pero todavía no había una prueba terminante. ¿Era él directamente responsable del robo de mi software en diciembre? Las pruebas eran aún incompletas. Lo que sí sabía, por los datos recogidos antes por Andrew, era que incluso si Kevin en persona no era quien había atacado mi máquina, el intruso de la Well estaba en poder de una copia de mi software antes

de haberse cumplido doce horas del forzamiento original.

Ahora la persecución estaba en marcha, y el reto estaba en avanzar más rápido que cualquier filtración pudiese llegar al intruso. La seguridad se había convertido en una verdadera preocupación, porque me daba cuenta de que la gente hablaba de mí y de que mis días de cómodo anonimato estaban acabando. Esa mañana, mientras regresaba andando al atestado despacho de Pei, un miembro del personal de mantenimiento del sistema de la Well me detuvo y dijo: "¿No he visto su foto en el periódico?". La publicidad sobre

el ataque estaba evidentemente empezando a complicar nuestras actividades, y sería un desastre que alguien mencionase algo acerca de mi presencia en el sistema y eso llegase a oídos del intruso.

Pei abordó más tarde al empleado y le pidió discreción. Yo tenía la impresión de que Claudia y Pei creían que podían mantener las cosas en la sombra, pero me temía que ya se estaba viendo que eso era imposible.

De hecho, la situación empeoró casi inmediatamente al presentarse Kevin Kelly —director de *Wired* y uno de los fundadores de la Well— preguntando si

podía sacarme una foto para un artículo en su revista.

"Mejor mañana", farfullé, y procuré desaparecer.

Me metí urgentemente en el cuarto trasero y me puse a examinar los progresos que habíamos realizado en la instalación de nuestra estación de seguimiento. Una de las máquinas RDI estaba recogiendo datos junto con la SPARCstation de Pei, y al parecer lo habíamos hecho bastante bien la noche anterior ajustando los filtros, pues la acumulación de datos para nuestro posterior análisis se había vuelto algo menos abrumador. Pero nuestras

herramientas de software no leían los datos filtrados en la SPARCstation de Pei y ésta se estaba utilizando también para otras tareas, de modo que continuamos trabajando con el segundo RDI tratando de incorporar un disco que nos había dejado Pei.

La del martes había sido una noche bastante tranquila. Nuestro intruso había efectuado únicamente apariciones aisladas, dando tiempo a que Andrew contestase llamadas telefónicas. Se enteró de que los de seguridad en la Colorado SuperNet habían sido detectados por el intruso, que rápidamente borró todos los archivos

que había almacenado allí, dejándoles a continuación un mensaje insolente: "¡Panda de ineptos!"

Tomé nota de las horas en las que el intruso estaba en activo. Se había registrado en la Well a eso de las 8 de la mañana del miércoles. Si se atenía a los horarios normales de los hacker, trabajando hasta las primeras luces y durmiendo hasta tarde, resultaba obvio que no se encontraba en nuestra zona horaria: las más probables serían el Medio Oeste o la costa Este. Los datos parecían sugerir asimismo que nuestro atacante era un individuo solo y no un grupo, pues nunca había en un momento

dado más de una única sesión de registro de entrada que utilizase las cuentas robadas. Por lo demás, precisamente como lo describiera Andrew el domingo por la noche, su esquema de actuación parecía notablemente repetitivo. La Well era evidentemente terreno de preparación o base de lanzamiento desde la cual, una y otra vez, venía a buscar sus herramientas para llevarlas al emplazamiento de un nuevo ataque.

Mi creciente sospecha de que Kevin Mitnick era el intruso de la Well explicaba algunas cosas que antes me habían dejado perplejo. Mientras

examinaba el texto en el visor de la estación de trabajo y veía pasar las letras VMS tuve uno de esos extraños destellos de intuición que experimento ocasionalmente. VMS es el sistema operativo de la DEC, y me acordé de que varios años antes había leído en *Cyberpunk* que Neill Clift era el investigador informático británico especializado en localizar problemas de seguridad en la VMS. Quizá Neill Clift poseyese la inicial del medio que casara con la contraseña *fucknmc*. ¿Podría ser que Mitnick tuviese alguna cuenta pendiente con él?

Llamé a Markoff para pedirle que

comprobase la inicial del medio de Neill Clift y luego lo invité a venir a ver en acción nuestra operación de seguimiento. Llegó alrededor de una hora después y repasamos parte de la información sobre pulsaciones de tecleado que habíamos capturado y que mostraba en qué había andado el intruso de la Well.

También Claudia nos hizo una visita y me preguntó en qué estado se encontraba nuestra operación. La dirección de la Well se reunía al día siguiente, dijo, y tomaría una decisión sobre si desconectar o no los ordenadores.

“Nos sentimos muy expuestos”, anunció, “y pensamos que deberíamos tomar medidas para reasegurar el sistema, como quitar las puertas traseras que conocemos y pedir a los usuarios que cambien de contraseñas”.

Yo le expliqué que la noche anterior durante la cena había convencido a Katz de que adoptar esas medidas resultaría desastroso para nosotros y probablemente pondría fin a toda posibilidad de coger al intruso.

“Tsutomu”, replicó Claudia, “hace una semana que usted está aquí y no veo ningún progreso”.

“Perdóneme”, le espeté a mi vez.

“Métase esto en la cabeza: estoy aquí desde hace unas veinticuatro horas y es evidente que hasta que llegué yo ustedes no hacían nada útil. Estoy ocupado y ahora mismo no tengo tiempo para ocuparme de usted”, le dije, y me volví bruscamente para reanudar mi conversación con Andrew.

Por suerte Julia fue más diplomática y se llevó aparte a Claudia para explicarle el avance efectivo que habíamos realizado hasta el momento y nuestro plan de acción para los días inmediatos. Se enteró además de que Claudia estaba en parte preocupada porque Pei tenía a sus empleados

ocupados las veinticuatro horas en examinar los datos conseguidos y eso le estaba costando a la Well un montón de dinero.

Un rato más tarde Julia regresó y dijo que no parecía que Claudia fuera a recomendar a la dirección que nos echase de inmediato. La crisis había sido soslayada por el momento, pero cada vez era más evidente que íbamos a tener que avanzar con la mayor rapidez posible o se acabaría la investigación.

El miércoles pasamos la mayor parte del tiempo pendientes de la ejecución de un programa escrito por mí, llamado Crunch. Estaba diseñado para tomar los

datos acumulados de los paquetes de datos filtrados de la noche anterior, separarlos y organizarlos nítidamente en sesiones para poder reconstruir exactamente qué se proponía el atacante. Pero Crunch estaba operando lentamente, empleando en su tarea el doble del tiempo que nos había llevado recoger los datos. Habíamos conseguido acelerarlo un poco pero la red de filtrado era más grande que la que había tendido nunca, y se encontraba en el ordenador más ocupado con el que hubiese tratado hasta entonces.

Mientras esperaba, me senté ante la consola del ordenador de Pei e inicié mi

propia cacería con los datos que habíamos reunido. Entre los cientos de archivos robados ocultos en las cuentas hurtadas que habíamos encontrado hasta el momento estaba el archivo de la base de datos de las tarjetas de crédito de Netcom. Había nombres de algunos conocidos míos, como un amigo que era compañero de piso de Castor Fu. Éste estaba ausente cuando lo llamé, pero le dejé un mensaje pidiéndole que le leyese el número de su tarjeta de crédito a mi amigo. Probablemente, lo dejé con una sensación extraña.

A continuación llamé a Mark Lottor y juntos tratamos de imaginar de dónde

había venido el código que le habían robado y encontramos en la Well. Cuando le describí el archivo se dio cuenta de que era una versión muy vieja de su código Oki, lo cual significaba que probablemente había venido de mi ordenador, ya que Mark tenía las ultimas copias. Volví a revolver en el software robado cuando Andrew se acercó y vio lo que estaba haciendo.

Al proseguir con la revisión de los datos anteriores noté que esa mañana habíamos capturado datos de paquetes que mostraban que un forzamiento desde la Well a Internex se había interrumpido en medio de una palabra. En una sesión

de la Netcom que empezó a las 7:29 a.m., al parecer el intruso había empezado a teclear el mandato *uudecode* pero la conexión se interrumpió a las 7:31 tras haber él tecleado únicamente *uudeco*, las primeras seis letras. Minutos después volvió y reanudó exactamente donde había quedado, usando el comando para decodificar y ejecutando luego un programa llamado *1.Z* que lo hacía raíz en Internex. Pero la sesión interrumpida sugería que el FBI tal vez tuviese razón en creer que el intruso operaba con una conexión telefónica móvil poco fiable. En uno u otro caso, teníamos un valioso

indicio, un indicador que aparecería simultáneamente en cada uno de los registros de conexión de los operadores de redes informáticas y los registros de llamadas de las compañías telefónicas permanentemente atentas a la efectiva localización física del intruso.

Había pensado que podría salir con Julia a patinar un rato durante la tarde, pero ya empezaba a oscurecer cuando partimos hacia el norte por el carril de bicicletas por Bridgeway, una carretera que va de Sausalito a Mill Valley. Era agradable andar en patines, pero al principio el cambio —me había acostumbrado a las tablas de fondo—

me hizo sentir incómodo. No tardé mucho, no obstante, en encontrar mi ritmo, y en un largo trayecto colina abajo estuve haciendo círculos para esperar a Julia, a quien no le gusta demasiado ir rápido cuando baja una cuesta. Estábamos abajo cuando zumbó el busca, y aunque no reconocí el número, igual lo marqué en mi teléfono móvil para devolver la llamada. Era David Bank, el periodista del *San José Mercury*. Le dije que estaba ocupado y que no podía hablar con él. Colgué y pensé para mí: "Ahora que conozco su número, sé cómo ignorar sus llamadas".

Estuvimos patinando una media hora

y luego dimos la vuelta. Ya estaba oscuro, así que paramos a telefonear a Andrew para pedirle que viniese a recogernos. Patinamos en círculos hasta que él llegó y nos llevó al Samurai, un restaurante japonés en Sausalito. Durante la cena hablamos los tres sobre nuestros próximos pasos. Era evidente que teníamos que mudar nuestra base de operaciones, pero yo todavía dudaba de la conveniencia de ir a la Netcom o a la Intermetrics, y se me ocurrió que si el FBI creía que nuestro intruso estaba efectivamente en Colorado tal vez deberíamos dirigimos allí.

Pero Julia estuvo en contra, porque

no estaba convencida de que el FBI tuviera pruebas que sustentasen su creencia. Yo hice notar que puesto que habíamos comprobado que la mayor parte de la actividad tenía origen allí, valía la pena una visita; si él no estaba, podíamos comprobarlo rápidamente e irnos. Andrew se mostró preocupado porque los administradores de sistemas de la Colorado SuperNet (CSN) parecían un poco lerdos y nos recordó el incidente del que nos habíamos enterado esa mañana, en el que el personal de la CSN se las había ingeniado para ser detectado a su vez por la presa. Decidí que los llamaría para ver si estaban

dispuestos a cooperar con nosotros. Abandonamos el restaurante conscientes de que todavía quedaba un montón de trabajo por hacer, incluida la instalación de una segunda estación de seguimiento en la Well para servirnos de respaldo.

Cuando llegamos a la Well, Andrew llamó a la CSN. Habló un momento con alguien que estaba trabajando con el FBI y luego me pasó el teléfono. Me interesaba saber si el intruso estaba utilizando las líneas telefónicas de acceso local de Colorado o entraba por Internet.

"Hemos estado observando ataques en la Well provenientes de vuestros

ordenadores y pensé que podríamos encontrar alguna forma de compartir información", le expliqué al responsable de sistemas.

"Estamos trabajando en estrecho contacto con el FBI", replicó él. "Le agradezco su oferta, pero tenemos esto bajo control. Me han dado instrucciones de no darle ninguna información y de pedirle en cambio que se comunique con la oficina del FBI en Los Ángeles para que ellos le pasen oportunamente la que haya".

"¿Oportunamente?". No podía creer lo que estaba oyendo. "¡Pero si a ustedes los contra-detectaron esta

mañana!”.

“Sé que cometimos un error”, replicó él bruscamente, “y nos aseguraremos de que no vuelva a ocurrir”.

Le pregunté si ahora la CSN tenía instalado un dispositivo de captación y rastreo de llamadas y si estaban en contacto con la compañía de teléfonos móviles de allí. Me dijo que sí, que eso estaba cubierto.

No me pareció muy sincero, de modo que para ponerlo a prueba le pregunté: “¿Le han pedido a la compañía que vigile todas las llamadas de datos para ver si él se encuentra en la zona?”.

Eso era completamente imposible, porque no hay forma de que una empresa de telefonía móvil pueda llevar a cabo un seguimiento de todas sus llamadas. "Oh, sí", dijo el hombre sin inmutarse. Era evidente que hablar con esa gente era una absoluta pérdida de tiempo, así que colgué. Si íbamos a Colorado, tendríamos que empezar desde cero. No parecía una opción viable.

A continuación pasé a ocuparme de averiguar por qué no lográbamos poner en marcha el nuevo disco para la segunda estación de seguimiento que estábamos tratando de establecer. La mayoría de las estaciones de trabajo y

un creciente número de ordenadores personales utilizan una conexión estándar de hardware conocida por Small Computer Standard Interface[30] (SCSI) para conectar elementos tales como un disco duro o una disquetera para CD-ROM. Nuestro segundo RDI se negaba a reconocer el disco que Pei nos había prestado, y aunque Andrew había probado con otro cable, seguíamos sin tener suerte. Me dispuse a atacar el problema. Normalmente un bus de control[31] SCSI necesita ser adecuadamente terminado —una función reductora para asegurar que las señales en el cable no se reflejan o interfieren

entre sí—, pero tras probar con diferentes cosas nos dimos cuenta de que cuando yo dejaba la terminación externa separada del manipulador empezaba de pronto a funcionar. Curioso, pero con el hardware suceden estas cosas.

Con todas nuestras estaciones de seguimiento en marcha, volví a los datos del filtro. Esa noche alrededor de las ocho nuestro intruso había estado merodeando en la Well, siguiendo su acostumbrada rutina de hacerse raíz y luego ocultar su presencia con un programa encubridor. Comprobó brevemente si Jon Littman había

recibido correo nuevo, no encontró nada y dirigió su atención a Markoff. Al abrir el archivo de correo utilizó una orden estándar de búsqueda de texto de Unix:

```
# grep -i itni mbox
```

"Un momento", me dije, "esto es algo que no hemos visto antes". El intruso estaba buscando en el archivo de correo electrónico de Markoff la hilera de cuatro letras "itni". Él procuraba ser discreto, pero para mí aquello era una revelación total: daba la impresión de que Kevin Mitnick estaba en retirada; al parecer, tenía sumo interés en saber quiénes podían estar hablándole a

Markoff de él. En ese caso no tuvo suerte, pues no encontró material alguno.

Andrew y yo, que habíamos estado durante la semana rastreando metódicamente a nuestro intruso a través de la Red, ahora recibíamos indicaciones de Mark Seiden en Internex de que un parecido esquema de forzamiento estaba empezando a emerger también allí

Yo conocía un poco a Seiden porque a lo largo de los años habíamos pasado cierto tiempo juntos en las conferencias anuales de hackers en el lago Tahoe y otras conferencias informáticas. Era

también amigo de Markoff y de Lottor. Con su negro cabello rizado, la barba grisácea y sus gafas de aros metálicos, Seiden suele adoptar lo que alguna gente ve como la misma afirmación antimoda que nos caracteriza a Andrew y a mí. Uno lo encuentra generalmente vestido con una camiseta adornada con algún tema tecnológico, pantalón corto, riñonera y sandalias, y rara vez sin el mensáfono, el teléfono móvil y el terminal RadioMail. Graduado de la Bronx Science High School —donde fue compañero de clase de Bruce Koball— y ex investigador en el Centro de Investigación Thomas Watson de IBM

en Yorktown Heights, Nueva York, es otro miembro de la primera generación crecida entre ordenadores. Competente hacker de Unix, Seiden ha tenido una serie de trabajos como consultor de algunas de las empresas online más importantes de la nación. Ha hecho asimismo buenos negocios instalando firewalls para todo tipo de empresas, desde proveedores de Internet y software hasta prestigiosas firmas de abogados de Nueva York.

A Seiden le interesaba especialmente el forzamiento en Internex porque su grupo consultor, MSB Associates, tenía su sede en el mismo

edificio céntrico que Internex en Menlo Park, y su conexión a Internet era suministrada por Internex. En nuestra primera conversación telefónica cuando le devolví la llamada el martes le bosquejé someramente la situación diciéndole que habíamos visto transferir un gran archivo a *gaia.internex.net* y le pedí ayuda. También le expliqué que estábamos haciendo todo lo posible por evitar alertar al intruso, que teníamos crecientes pruebas de que nuestro entrometido era Kevin Mitnick y que quería que mi archivo de información privada fuera rápidamente quitado de Internex, porque no deseaba que el

contenido se propagase por toda Internet. Mark convino en realizar su propia vigilancia y después habló con Andrew para coordinar los detalles. Cuando éste le describió el acuerdo que había hecho con la Well de no copiar material, Mark decidió que no quería limitar su propia libertad aceptando esos términos y dijo que prefería continuar trabajando independientemente de nosotros.

Una vez que hubo empezado a examinar el sistema Internex, pronto encontró que una cuenta de nombre brian había sido expropiada de los ordenadores de la compañía situados en

la segunda planta de un céntrico edificio de oficinas, encima de una peluquería. La cuenta pertenecía efectivamente a Brian Behlendorf, un ex consultor de Internex que actualmente trabajaba en *Wired*. Cuando Mark escudriñó para ver lo que había almacenado en el directorio de brian, encontró una copia de *tzu.tgz*, el mismo archivo empaquetado y comprimido de mi directorio que nosotros habíamos descubierto en la Well. Trabajando desde su ordenador en el vestíbulo, que estaba conectado a la red mayor de Internex por una red local Ethernet, Mark estableció sus propios programas de husmeo para el

seguimiento de todas las conexiones externas con Internex. Como obviamente su ordenador no formaba parte de la red Internex y estaba siendo estrechamente vigilado, me había dicho que estaba bastante seguro de que el intruso no había forzado la entrada en su máquina. Confiaba en que podía utilizarla como puesto de información desde el que no era probable que el invasor pudiera saber que alguien seguía cada uno de sus pasos.

Al ponerse a explorar los ordenadores de Internex en busca de programas Caballo de Troya y clandestinos dejados por el intruso, le

llevó apenas unos minutos localizar en Gaia, el ordenador que manejaba su correo, un programa de apariencia inocente llamado *in.pmd*. Pmd es normalmente el nombre de un programa conocido como Port-master daemon, un pequeño elemento de software que se comunica con los dispositivos del hardware que normalmente conectarían con el ordenador a los usuarios que entraran desde el mundo exterior. Pero en este caso resultó inmediatamente visible, porque Internex no procesaba ningún Portmaster. El intruso no se había tomado la molestia de comprobar si su ardid tenía algún sentido en el contexto,

o tal vez no le importaba.

Mark desarmó el diminuto programa y descubrió que estaba mínimamente camuflado. Su operación era sencilla: si alguien conectaba con el puerto 5553 en el ordenador de Internex y tecleaba "wank", automáticamente se convertía en raíz, con todo el poder que eso conlleva. Lo interesante era que *in.pmd* existía únicamente en la memoria del ordenador; no había una versión correspondiente del programa en el disco duro. Esto significaba que el pirata lo había copiado al disco duro de Gaia, lo había empezado a procesar en la memoria del ordenador y luego lo

había borrado del disco, lo cual hacía más difícil detectar su presencia. Dando por sentado que nadie lo notaría, el programa había quedado operativo para uso del intruso cada vez que lo necesitase.

Andrew había advertido a Mark acerca de algunos trucos del pirata, y al continuar investigando éste descubrió que alguien se había metido con un programa estándar, aunque actualmente casi en desuso, del sistema Unix, llamado *newgrp*, un programa de utilidad que adscribe al usuario a un grupo particular con fines organizativos o de acceso. El intruso había

reemplazado el *newgrp* original con otro programa que tiene el mismo nombre, pero que secretamente tenía asimismo otras funciones. Nosotros estábamos familiarizados con él, ya que es una programa troyano bastante corriente que circula en el submundo informático. La versión troyana de *newgrp* permitía al intruso hacerse raíz o pasar por cualquier otro usuario del sistema. Cuanto más investigaba, más comprendía que Internex había sido completamente penetrada. Descubrió un puñado de otros programas troyanados y cuentas inocuas con nombres como "sue", establecidas y dejadas sin usar,

aparentemente como respaldo en caso de que el intruso se encontrase excluido.

Poco antes de la medianoche del martes Mark arrancó de nuevo el ordenador de Internex para expulsar cualquier puerta clandestina oculta o demonio secreto que no hubiera podido encontrar y borró también la versión troyanada de *newgrp*.

El miércoles, apenas dadas las 7 de la mañana, el intruso estaba de regreso, esta vez conectando desde *escape.com*, intentando utilizar la puerta clandestina que ya no estaba. Al no poder entrar, registró su entrada segundos después en la cuenta brian. Había cambiado su

contraseña a fucknmc, que evidentemente se había convertido en un mantra para él. Una vez dentro comprobó quién estaba normalmente registrado y quién había estado en el sistema recientemente. A continuación trajo una copia del programa demonio que Mark había borrado el día anterior y lo instaló en la memoria del ordenador de Internex, borrándolo otra vez del disco cuando terminó.

Treinta minutos más tarde estaba de vuelta de la Well, reinstalando y ocultando trabajosamente su programa troyano *newgrp* borrado por Mark la noche anterior. Mark, que lo seguía

desde su ordenador, observó al intruso comprobar todos los alias de "mark", presumiblemente para descubrir adonde estaba yendo el correo de Markoff.

No sólo apareció Markoff, sino que también lo hizo el nombre Mark Seiden, pero el intruso no pareció interesado. Poco después el invasor comprobó si la dirección en Internet de Markoff en el *New York Times* estaba conectada a la Red. Puede que le interesase forzar ese ordenador pero éste no contestó, por lo cual procedió en cambio a alterar el alias postal de Markoff con el fin de que una copia de todo el correo electrónico recibido fuera enviado automáticamente

a una misteriosa cuenta en la Universidad de Denver. El intento falló, no obstante, porque no se hizo correctamente. Casi doce horas más tarde el pirata estaba de vuelta, se hacía raíz y repasaba todos los encabezamientos en el buzón de Markoff. Aunque había un montón de correspondencia-basura, uno de los temas rotulados era "Intel stuff", pero el intruso no pareció interesado en él.

Puesto que los programas ilícitos habían sido inmediatamente reinstalados, esa noche Mark decidió no borrarlos de nuevo, sino escribir su propio pequeño programa que no sólo le

enviaría una llamada de alerta cada vez que alguien conectara a través de la puerta clandestina encubierta, sino que incluía además una contramedida de vigilancia. Como recibía información sobre de dónde venía el intruso cada vez, escribió el programa de tal manera que pudiera comprobar quién estaba normalmente registrado en el sitio de la transgresión. Observando durante los días sucesivos las idas y venidas del intruso vería que si bien en algunos casos se conectaba a Internex desde la Well, casi siempre entraba vía *escape.com*, que según comprobó correspondía a una empresa de Nueva

York proveedora de servicios de Internet, dirigida por un emprendedor estudiante de secundaria. Los listados de usuarios actuales que retomaban con frecuencia incluían nombres conectados al sistema, como Phiber Optic y Emmanuel Goldstein. Yo no lo llamaría arrabal, pero el sitio era probablemente uno de los vecindarios más míseros de Internet.

Allí donde mirásemos aparecían más señales apuntando a Kevin Mitnick, pero mi desafío inmediato era asegurarme de que los filtros proporcionasen indicios sobre su ubicación, y pasada la

medianoche del miércoles, mientras repasaba mentalmente los elementos de nuestra instalación de seguimiento en la Well, se me ocurrió preguntarle a Andrew si tenía en funcionamiento la sincronización temporal. La sincronización del tiempo es una prestación de redes de ordenadores que asegura que el reloj de cada ordenador marca la misma hora que los demás. Se trata de una herramienta útil para toda clase de actividades relacionadas con ordenadores y es esencial para el trabajo de seguridad informática. En las grandes redes de ordenadores puede haber cientos de personas registrándose

de entrada y de salida en cada minuto y miles de actividades en marcha. La única forma de asegurar una precisa reconstrucción de esa actividad es estar absolutamente seguro de que la hora coincida en los relojes de toda la red.

"Supongo que sí", fue la respuesta de Andrew.

¿Supongo? Lo comprobamos, y por supuesto la Well no tenía sincronización y nosotros tampoco.

Lo que ese desliz significaba era que todos los datos que habíamos recolectado desde la noche anterior serían difíciles de usar, al menos para el análisis del tráfico. Si los relojes no

estaban sincronizados sería mucho más difícil comparar los sucesos que tenían lugar en diferentes máquinas, paso necesario para rastrear a alguien que está conectado a Internet a través de una cadena de ordenadores.

"No quiero volver a oír la palabra *supongo*", le dije a Andrew.

Pareció herido. La suya había sido una larga y dura semana de jornadas de veinticuatro horas y estaba soportando el embate de todo lo que salía mal. Pero era un error *suponer* que porque en el SDSC nosotros funcionásemos con el tiempo sincronizado, todos los demás hicieran lo mismo. Desde mi punto de

vista la sincronía es un requisito imprescindible y no negociable, pues el tiempo es esencial para todo lo que hago.

Esa noche pasé un rato más intentando mejorar herramientas que pudiera utilizar para examinar los datos que íbamos recogiendo. Antes había llamado a mi teléfono móvil John Gilmore preguntando por Julia y ella se trasladó a otra habitación para hablar con él estando varias horas ausente. Julia había estado trabajando en el perfeccionamiento de una herramienta que necesitábamos con urgencia para nuestra búsqueda, y cuando vi que no

estaba lista me puse a terminarla. Al volver la encontré desasosegada, y los dos salimos fuera y estuvimos caminando por el muelle de Sausalito.

"John quiere que vaya a Wylbur Hot Springs este fin de semana", dijo ella. Iba a ser el fin de semana que Julia y yo habíamos programado pasar juntos antes de que ella viniera a la conferencia Vanguard en Palm Springs. Wylbur Hot Springs es un retiro rústico, al estilo de los años sesenta, al norte de San Francisco. Estuvimos hablando del asunto mientras caminábamos por el muelle, cerca de las viviendas flotantes. Sospechaba que en aquel fin de semana

había mucho más de lo que aparecía a primera vista.

"Es un lugar al que solíamos ir cuando las cosas iban mejor entre nosotros", dijo Julia mientras avanzábamos otro poco.

Aun cuando la idea era supuestamente decirse adiós, los dos nos dábamos cuenta de que John tenía en mente otra cosa, y eso a Julia le resultaba inquietante.

Continuamos paseando en silencio. Yo no tenía respuesta.

"Tenemos que regresar al trabajo y terminarlo", dije por fin.

Eran más de las tres de la mañana

cuando volvimos a casa de Dan Farmer. Yo experimentaba una creciente urgencia por hacer algo para dar rápidamente con el intruso, pero todavía no estaba seguro sobre que dirección tomar. Pero una cosa veía con claridad, y era que no ganaríamos nada permaneciendo en la Well.

Nuestra habitación al fondo de la casa de Dan contenía una cama, una estación de trabajo Sun y numerosos estantes llenos de libros de ciencia ficción. Contaba también con una fuente de agua con un tazón de piedra artificial, sucesivas planchas inclinadas verticales de un material oscuro semejante a la

piedra y guijarros esparcidos. Yo estaba exhausto y apenas oí, antes de caer profundamente dormido, el agua que caía en cascada a los costados produciendo un leve sonido burbujeante, neutro, que enmascaraba el ronroneo de la estación de trabajo situada en el rincón opuesto de la habitación.

11. Netcom

Me despertó el jueves el sonido de agua cayendo y aunque el dormitorio estaba todavía oscuro comprendí que la mañana estaba avanzada. Varios de los gatos de la casa andaban rondando por allí y en la penumbra distinguí la colección de botellas individuales de escocés del compañero de piso de Dan esparcidas por el suelo. Pensé que había llegado el momento de decidir la dirección de nuestro próximo

movimiento.

Andrew llevaba una semana en la Well y ahora poseíamos algunos datos reales y algunas pistas potencialmente sólidas. Pero nuestro intruso seguía suelto y sin control, y necesitábamos ponemos en movimiento. Con la opción de la Colorado SuperNet cada vez menos viable, tenía que afrontar la idea de efectuar nuestra observación desde la Netcom. Uno de los mayores proveedores de servicio InterNet del país, la Netcom haría que nuestra investigación fuese como buscar a alguien en la estación Grand Central Terminal. Me sentía frustrado por el

bloqueo en la CSN, y dediqué infructuosamente varias horas de principios de la tarde a ver si había alguna forma de evadir el impedimento del FBI de Los Ángeles en Colorado.

Después, como Julia estaba nerviosa, hablamos un rato. Los dos teníamos claro que John contaba con los recuerdos agradables de Wylbur Hot Springs para debilitar la decisión de ella de abandonarlo.

"Temo no poder conservar mi sentido de la perspectiva cuando esté con él", dijo. No estaba segura de su capacidad para independizarse de John y la preocupaba verse absorbida

nuevamente por la relación entre ellos. “Esto va a ser difícil”, añadió. “Quiero asegurarme de descansar lo suficiente esta noche”.

Estábamos a media tarde y yo decidí que no quería volver a la Well. Por un lado, el fotógrafo de *Wired* que yo trataba de evitar seguía allí clavado esperando. Andrew me había llamado ya varias veces y yo seguía diciéndole “ahora voy”, pero estaba claro que debíamos aceptar la oferta de apoyo de la Netcom. Hacía mucho que veíamos tráfico desde allí y un observatorio en su cuartel general nos proporcionaría un puesto de escucha de alcance nacional

en su extensa red y posiblemente una ubicación que nos situaría más cerca de nuestro atacante. Además, teníamos varios sucesos reveladores —las sesiones abruptamente interrumpidas— que tal vez pudiésemos utilizar para determinar la identidad del intruso en el sistema Netcom.

Me puse al habla con Rick Francis, el vicepresidente de la Netcom para el desarrollo de software, que había participado en la conferencia telefónica en la Well el martes, le conté mi plan y le pregunté si su oferta seguía en pie. Me excusé por llamarlo al final de un día de trabajo, pero a él no parecía importarle

y me dijo que su personal se quedaría aún un rato más para hablar con nosotros.

Antes de irme llamé a Andrew e hice que me leyera la hora exacta de varios sucesos corregida según su mejor cálculo de nuestro error de sincronía, de forma que tuviésemos algo que comparar con los registros de la Netcom. Eran casi las cuatro cuando Julia y yo compramos unos burritos en Zona Rosa, en Haight Street, y cogimos la I-280 hacia San José en su Mazda. Pensé que de una forma u otra más adelante podría traer mi ordenador de la Well.

La 280, que recorre una extensión de la falla de San Antonio, es considerada por muchos la autopista más hermosa del mundo. La descripción es simpática, aunque siempre me ha parecido una figura retórica. Arrimada a la falda de las montañas de Santa Cruz, la 280 corre por el centro de la península y es en realidad la Mulholland Drive de Silicon Valley. Camino del sur la carretera serpentea a través de Woodside, Portola Valley y las colinas de Los Altos, donde se mezclan la riqueza nueva y la vieja. Conduciendo por los miles de acres que una vez fueron propiedad rural de Leland Stanford, se pueden ver aún las

vacas pastando no muy lejos del 3000 de Sand Hill Road, centro cerebral de la comunidad de los capitalistas de riesgo, principal beneficiaria de lo que se ha descrito como la mayor acumulación legal de riqueza de la historia.

Por el camino me comí mi burrito y telefoneé a Kent Walker para comunicarle nuestro próximo paso. Le hablé de los obstáculos en Colorado y le pregunté sobre los alcances de la ley de Intimidad de Comunicaciones Electrónicas, que hace ilegal interceptar llamadas de teléfonos móviles. Aunque sea ilegal escuchar llamadas orales, ¿sería una violación de la ley verificar

simplemente la presencia o ausencia de un portador de datos enviado por modem en una llamada de teléfono móvil? Me respondió que mientras no descifrásemos el contenido de la información, la intercepción probablemente sería legal. A esas alturas mi pregunta era solamente hipotética, pero en cierto momento se me había ocurrido que tal procedimiento pudiera ser nuestra única opción.

Veinticinco kilómetros más al sur, en Cupertino, la I-280 pasa junto a las nuevas instalaciones de investigación y desarrollo de Apple Computer. Aquí, en 1993, el ex presidente de Apple, John

Sculley, planeó establecerse como principal funcionario técnico de la compañía, sólo para ser depuesto por un golpe de mano en el directorio muy semejante a aquel por el cual él mismo desplazó ocho años antes al visionario original de Apple, Steve Jobs. Desde Cupertino la carretera describe un arco a través del corazón de Silicon Valley, brindando interminables imágenes de la fabricación de semiconductores, diseño de ordenadores y plantas de montaje.

La Netcom está alojada en una torre de acero y cristal de doce plantas frente a la Winchester Mystery House muy próxima a la 280 en San José. Aunque

actualmente sea una atracción turística, el hogar de los Winchester fue proyectado por la paranoica viuda del inventor del rifle de repetición que lleva su nombre y está llena de habitaciones ocultas y pasajes secretos que no conducen a ninguna parte. El nombre Winchester fue más tarde tomado en préstamo por la división de fabricación de unidades de disco de IBM, situada en el mismo extremo sur del valle, para el primer disco duro moderno.

Una vez que traspusimos las puertas de acceso e iniciamos la búsqueda de las oficinas de la Netcom, tuvimos la impresión de haber errado y hallarnos al

otro lado de la calle, en la Mystery House. Acabamos bajando unas escaleras, cambiando de dirección después de asomarnos a un vestíbulo y subiendo otras varias antes de dar finalmente con el despacho de Rick Francis.

Sociológicamente hablando, Silicon Valley se divide en *techies* y *suits*. La diferencia entre ambos suele ser que los *suits* saben cómo vestirse y han conseguido abrirse paso desde las filas de los ingenieros a la órbita de los directivos. Francis era visiblemente uno de estos últimos, con su camisa abotonada, sus mocasines con borlas y

el suéter con dibujos, el uniforme típico de los gerentes de mercadotecnia y los vicepresidentes ejecutivos a lo largo del Valley. Era evidente que lo de tratar con alguien de fuera sobre un asunto de seguridad informática era territorio virgen para él, y aunque quería colaborar, no estaba completamente seguro de lo que podía esperar de mí y en consecuencia estaba levemente en guardia.

Después de haberle puesto rápidamente en conocimiento de lo que sabíamos tras nuestra estancia en la Well, subimos con Francis a reunimos con dos miembros de su equipo técnico.

Uno de ellos John Hoffman, administrador de sistemas, era del tipo del ingeniero ensimismado y estaba encargado de la configuración y el mantenimiento de los sistemas informáticos de la Netcom. El otro, Robert Hood, era administrador de red: tenía el aspecto del auténtico hacker que realmente conoce su oficio. Era tranquilo, competente y nada arrogante acerca de sus capacidades. Era asimismo el contrapunto de Francis en materia de apariencia. Rollizo y bien afeitado, Hood poseía una abundante cabellera negra rizada que le caía veinte centímetros más allá de los hombros.

Vestía una desteñida camiseta negra adornada por una calavera sonriente, pantalón tejano, zapatillas deportivas, y llevaba colgado del cinturón un busca alfanumérico. Me resultó simpático de entrada. Robert era el clásico hacker de Silicon Valley que disfruta efectivamente con su trabajo. Había crecido con la Netcom desde los primeros días de la empresa como proveedora local de Internet.

Una vez que Francis les dijo a Hood y a Hoffman que nos dedicaran todo el tiempo y el equipo que necesitásemos, buscamos una sala de conferencias y nos pusimos a trabajar. Yo dejé claro que

nuestro objetivo era localizar a nuestra presa lo más pronto posible y avanzar a contracorriente hasta dar con él. Una vez más repasé los datos provenientes de la Well y señalé que las conexiones en las que estábamos interesados venían reiteradamente de la Netcom y la CSN. Les expliqué asimismo que teníamos la creciente sospecha de que nos las estábamos viendo con Kevin Mitnick. Los de la Netcom ya sabían quién era; al parecer les había causado muchos problemas en el pasado.

Le mostré a Robert la lista de ocurrencias que Andrew me había leído y le pregunté si la información servía

para averiguar qué cuenta podría estar utilizando el intruso en la Netcom.

"No hay problema", respondió.

Durante la reunión, Robert y yo monopolizamos prácticamente la palabra sopesando los obstáculos para realizar el filtrado de paquetes en la Netcom. Yo hice preguntas sobre su red interna, sobre detalles de incidentes de forzamiento recientes y sobre la clase de precauciones que estaban adoptando. Pregunté también sobre los números de tarjetas de crédito robados que habíamos encontrado en la cuenta dono en la Well, y resultó que habían sido robadas casi un año antes flotando

durante un tiempo en el submundo informático; su existencia había sido mencionada el año anterior en la revista *2600*. Francis dijo que inicialmente la Netcom no tenía ningún firewall protector y que los datos de los clientes se habían conservado en ordenadores relativamente desprotegidos. El descuido había sido un costoso error, y lo sabían. Quiso saber si teníamos una copia sacada el presente año después de mediados de enero. Si los datos de las tarjetas de crédito habían sido robados de nuevo, estaban ante un problema gordo.

Al final fue una reunión breve, lo

cual me sorprendió, pues habíamos conseguido obviar la mayor parte de las concesiones a la sociabilidad e ir directamente al grano. A continuación Francis dijo que quería que escuchase una cinta y nos llevó a una habitación próxima a su despacho, donde nos pasó la grabación del diálogo mantenido entre uno de los piratas que habían estado importunando en la Netcom y un técnico auxiliar. Francis tenía una obvia curiosidad por saber si la voz era semejante a la de los mensajes en mi sistema de correo vocal en San Diego. En la llamada grabada el técnico hablaba con el pirata acerca de la

motivación de este ultimo para forzar los ordenadores de la Netcom y lo interrogaba sobre algunos de sus métodos; pero Julia y yo estuvimos de acuerdo en que la voz al otro extremo de la línea no tenía nada que ver con la de mi buzón.

Eran casi las 6:30 y Francis se disculpó por tener que irse temprano. Le habría encantado quedarse a observar, explicó, pero tenía un importante viaje de negocios a la mañana siguiente. Pero antes de irse dio su autorización final para nuestra búsqueda.

“Recuerde, cualquier cosa que le haga falta, pagamos nosotros”, dijo. “Y

si tiene que viajar a alguna parte para rastrear a ese tipo, la Netcom corre con los gastos".

Después de los choques con Claudia y de ser menospreciado por todo el mundo en la Well, el apoyo incondicional por parte de la Netcom fue un bienvenido alivio. Por primera vez empecé a sentir que teníamos una razonable probabilidad de pescar al ladrón de nuestros datos.

Julia, los dos tíos de sistemas de Netcom y yo subimos y nos apretamos en el pequeño despacho de Robert, que apenas tenía espacio para una estación de trabajo Sun y estaba atestado de

manuales técnicos.

La lista que yo le había tomado por teléfono a Andrew nos daba la hora precisa de inicio y finalización de las sesiones provenientes de la Netcom con destino a las cuentas ilícitas en la Well, de modo que nuestro reto era descubrir si había un usuario único cuya entrada en la Netcom hubiera sido registrada en todas las horas de mi lista. Teníamos un indicio determinante: la hora de la conexión interrumpida en la Well debía corresponder a un similar registro de salida en la Netcom, algo que debía resaltar en las montañas de datos registrados. Además, si descubriésemos

que nuestro atacante era una persona sola en vez de varias o de una pandilla que compartiese la cuenta, simplificaría grandemente nuestra tarea: Limitaría la caza a una única localización. Yo confiaba en la Navaja de Occam[32], el principio científico según el cual cuando coexisten teorías para explicar un fenómeno desconocido, ha de preferirse la más sencilla.

Robert se sentó ante su estación de trabajo y los tres nos amontonamos en torno suyo a observar mientras él buscaba en sus archivos registros de entrada y de salida ocurridos en determinadas horas. Me di cuenta

inmediatamente de que era un auténtico *gurú* del Unix. Jamás vacilaba con el teclado, y los comandos fluían sencillamente de sus dedos. Cuando yo formulaba una pregunta, no se detenía a recordar cómo buscar una información determinada, sino que el resultado aparecía casi instantáneamente. Robert se sentía además comprometido en la captura de nuestro intruso. "Ese tipo nos ha estado molestando de veras", dijo. "He empezado a tomarme esto como algo personal. Si das con él, allí estaré yo contigo. Y también Rick Francis y Bob Rieger, nuestro presidente. Están realmente furiosos con esto".

Parecía entusiasmado por nuestra llegada. Con la permanente expansión de la Netcom en diferentes ciudades había tenido ya abundante trabajo. Ahora sentía una gran expectación por una aventura en la que no tendría que considerar la importancia de su trabajo oficial de administración de sistemas sino la cacería de un intruso.

Para encontrar una coincidencia entre los datos de la Netcom y la Well tenía que buscar información entre las 23 Sun SPARCstations que constituían el servicio online de la Netcom. Robert tenía un guión de búsqueda por los registros de estadísticas de uso del

sistema de todas las máquinas a partir del 1 de enero, pero llevaría su tiempo.

Mientras el guión operaba, Robert empezó a hablarme de la red interna de la Netcom. Me explicó que las 23 SPARCstations estaban conectadas a un anillo de red local FDDI (Fiber Distributed Data Interface). Conectados también a este anillo estaban los ordenadores de distribución que proporcionaban conexión con Internet, así como su propia red transcontinental T-3, capaz de mover casi 45 millones de bytes de información por segundo. Este sostén, a su vez, estaba conectado a un entramado de líneas de datos T-1 que

vinculaba a sus clientes de datos de alta velocidad y a sus Puntos de Presencia o POP con su concentrador de red en San José.

En lugar de tener un único número telefónico 800 o de larga distancia, la mayoría de los proveedores nacionales de servicio de Internet colocan POPs con pequeños grupos de modems de conexión en docenas e incluso cientos de ciudades por todo el país. Fue esa capacidad para establecer una red privada de datos —que fuera más allá de la red estándar telefónica pública— lo que creó las economías de escala que hicieron posible que la Netcom

prosperase como proveedor de servicio de Internet a escala nacional con teléfonos de llamada incluso en ciudades bastante pequeñas por todo el país.

Quizá el esfuerzo de la Netcom por hacer fácilmente accesible su red obrara a nuestro favor. Si bien nunca habíamos visto al intruso utilizar las líneas telefónicas de llamada de la Well para acceder directamente al sistema Online de Sausalito —Netcom tenía líneas de llamada en 51 ciudades por todo el país —, si él era descuidado era posible que revelase por su propia mano su ubicación llamando a un número local

de Netcom. El dispositivo de rastreo de la compañía telefónica podría entonces permitimos localizarlo, incluso si estuviese empleando un teléfono móvil.

Hablamos de lo que supondría establecer un seguimiento en una red de ordenadores que era más grande que cualquiera de las que yo hubiera tenido por delante alguna vez. Lo que necesitaba era un único punto desde el cual pudiéramos acceder a todos los paquetes que pasaban por la red. Con la Well la cosa había sido como instalarse en una esquina de la calle principal de una pequeña ciudad del Medio Oeste, interceptar todos los Ford rojos o todos

los coches con matrícula de California que pasaran y hacerle una foto al conductor de cada uno. Con la Netcom, en cambio, sería como venir a Los Ángeles y hacer lo mismo en la autopista de Santa Mónica.

Resultó que había un solo punto de atasco en esta red. Esa fue la buena noticia. La mala era que ese punto se hallaba en el principal anillo FDDI. El FDDI es un elemento de red de ordenadores de muy alta velocidad que transmite datos a 100 millones de bytes por segundo, diez veces más rápido que la red Ethernet con la que operábamos en la Well. El seguimiento en esta red

requería hardware adicional y un software específico, pues las herramientas de seguimiento de Ethernet empleadas en la Well eran aquí inútiles.

Para entonces disponíamos de los datos sobre registros de entrada de usuarios y Robert empezó a hurgar en ellos buscando una coincidencia. Al cabo de un rato resultó cada vez más evidente que había una única cuenta que coincidía en cada caso con los registros de entrada del transgresor en la Well.

Nuestro culpable parecía ser el usuario de una cuenta llamada gkremen. Había varios registros de entrada locales desde San Francisco este mes,

pero cada una de los accesos a gkremen por teléfonos de llamada remotos venía exclusivamente a través de su remoto POP en Raleigh-Durham, Carolina del Norte.

"Estoy seguro de que es él", dijo Robert, pero yo no quería llegar a conclusiones prematuramente, en especial porque sólo contábamos con cuatro puntos de datos, tres registros de entrada a la Well y una sesión ftp a partir de lo cual trabajar. Prestamos más atención a gkremen. ¿Quién era aquel tío? Encontramos información sobre cuentas de Netcom que indicaba que gkremen era un usuario legítimo, no una

cuenta inventada como muchas de las que habíamos encontrado en la Well y en Internex. Gkremen arrendaba una conexión de red de alta velocidad de Netcom directamente desde el emplazamiento de su ordenador, pero tenía además en los sistemas de Netcom una cuenta secundaria, conocida como cuenta "shell" o de cobertura. Daba la impresión de que el verdadero gkremen utilizaba la cuenta en raras ocasiones, y el examen de los registros de conexión fue haciendo cada vez más evidente que su cuenta había sido "expropiada".

Robert recorrió el directorio de gkremen, que resultó bastante anodino

excepto por algo que le llamó la atención: un pequeño programa llamado test 1. Nos explicó que se trataba de una versión del programa telnet que no registraba su utilización. Normalmente, cuando alguien utiliza el programa telnet estándar de Netcom para conectar con otro ordenador, quedan registrados el nombre del usuario y el del ordenador remoto. Robert había empezado ya a trabajar en una modificación para el sistema operativo de la Netcom para que no se pudiera eludir la función de registro. Era obvio que alguien había secuestrado la cuenta de *gkremen* y la estaba usando clandestinamente. Cada

vez daba más la impresión de que habíamos dado en el clavo. Explorando los registros de entrada de gkremen descubrimos incluso conexiones provenientes de emplazamientos conocidos, como *escape.com* y *csn.org*. No obstante, su favorita parecía ser Raleigh; en los pasados cinco días había accedido 26 veces desde allí. Había estado operando casi diariamente, incluyendo algunas sesiones esa misma mañana.

Creía recordar que algunos de mis amigos que viven en Raleigh se quejaban de la calidad de su servicio telefónico.

“Robert, ¿sabes qué compañía telefónica está cerca de Raleigh?”, le pregunté.

“Claro”, replicó él, “la GTE”.

“Oh, no”, dije con un gemido. “Me lo temía”.

La GTE era conocida por la lasitud de su seguridad. Era notorio que los conmutadores de su oficina central solían caer en manos de chiflados del teléfono que clandestinamente los reprogramaban para conseguir llamadas gratis y a menudo realizar esotéricos y desagradables trucos. Nuestra tarea se dificultaría mucho más si nuestro intruso había logrado también manipular el

equipo de la compañía telefónica, pero ese era un obstáculo que no tendríamos que afrontar por el momento.

Potencialmente, el descubrimiento de Raleigh era un avance significativo. Nuestras operaciones de seguimiento resultarían sumamente simplificadas si el intruso estuviera sencillamente conectando con la Netcom desde el POP de Raleigh. La Netcom utilizaba una red Ethernet en cada uno de sus POP para conectar desde Portmasters hasta routers. Si pudiéramos encontrar un único emplazamiento local en la periferia de la red nacional de datos de Netcom evitaríamos tener que armar un

sistema de seguimiento FCCI y seleccionar entre la enorme cantidad de datos que discurren por el meollo de la red FDDI aquí en San José. Empezamos a examinar los horarios de vuelos para ver con qué rapidez podíamos poner a alguien en Raleigh y al mismo tiempo llamé a Kent para pedirle que consiguiera una orden de intervención telefónica para el POP de Raleigh.

"Esta noche no puedo porque ya es tarde", contestó. "Pero la tendré a primera hora de la mañana. ¿Cuál es la compañía telefónica?". Se lo dije, pero él no pareció experimentar ante la GTE la misma reacción que yo.

Mientras yo hablaba con Kent, Robert escribió un sencillo guión para que cada vez que se usara la cuenta gkremen llegase a su busca un alerta informándole de qué POP de Netcom venía la llamada.

Eran casi las 8:30 de la noche, y el busca de Robert sonó casi enseguida de haber él terminado de instalar la alerta, pero esta vez con una mala noticia. Gkremen había registrado una entrada, pero no provenía del sistema de la Netcom a través de su POP de Raleigh: esta vez venía ¡de Denver!

"Maldición, pensé, ha actuado de forma increíblemente constante durante

los últimos cinco días y ahora que aparecemos cambia de emplazamiento". Quería decir que no podíamos estar seguros de que pasaría por Raleigh y que, por tanto, para rastrearlo tendríamos que examinar los datos de todo el país en la red Netcom. Me pregunté por un momento si lo habíamos asustado o estaba realmente en otra parte. Aunque era posible que estuviese conectando a diferentes POPs en un intento por encubrir y ocultar su ubicación real, Robert mencionó que ellos estaban teniendo problemas técnicos en Raleigh y era también posible que el intruso estuviese

telefoneando a un POP distinto para conseguir una línea de modem que funcionase.

Mientras vigilábamos, Robert utilizó un programa de diagnóstico en el POP para espiar una sesión de tecleo de gkremen. Aunque el software no estaba pensado para el seguimiento de una sesión en vivo, funcionaba con ese objeto, más o menos. Cuando la persona que estaba usando la cuenta de gkremen tecleaba, Robert pulsaba el ratón, y el contenido de un pequeño buffer[33] de memoria de un Portmaster en el emplazamiento de Denver aparecía en su pantalla mostrándonos lo que el intruso

tecleaba. Desgraciadamente, el buffer sólo podía mostrar sesenta fragmentos de caracteres de la actividad que iba en cada dirección, por lo que veíamos casi todo lo que el intruso escribía en su teclado, pero sólo teníamos un atisbo ocasional de lo que él estaba efectivamente viendo en su pantalla. Nos encontramos además con otro problema que dificultaba aún más el ver claramente lo que ocurría. En aquel tiempo la Netcom estaba luchando con un defecto de software en el mayor de sus routers Cisco. Se trata de los ordenadores encargados de encaminar los billones de paquetes de datos diarios

que circulan por el anillo de red FDDI y enviarlos a sus destinatarios respectivos en Internet. Cada treinta segundos o así la red entera sufría un miniacceso, lo que significaba que perdíamos más pulsaciones de teclado.

No obstante los paquetes perdidos, igual podíamos hacernos una idea aproximada de lo que él hacía. Lo observamos mientras intentaba forzar la entrada en un ordenador en la CSN, al parecer sin éxito, y luego se volvía hacia otro ordenador de la instalación de Colorado y trataba de editar uno de sus archivos de configuración del sistema, pero se encontraba con que era

un archivo sólo de lectura y, por tanto, no podía ser manipulado.

Observamos que a continuación el transgresor utilizaba el comando de transferencia de archivos para conectar con el ordenador de archivo público del CERT, el centro gubernamental de información sobre seguridad.

Me puse a reír. "Parece que tenía razón, los críos están leyendo manuales técnicos", dije.

Estaba buscando en los archivos del CERT la palabra "monitor", y sus intenciones eran obvias: intentaba saber cómo reinsertar un pequeño programa de seguimiento de red dentro del sistema

operativo de uno de los ordenadores de la CSN. El programa, conocido por NIT (Network Interface Tap), es una parte estándar del software operativo básico del ordenador, pero generalmente se quita por motivos de seguridad. Si él conseguía reinstalarlo en el sistema operativo podría capturar secretamente contraseñas y otros datos útiles. Encontró lo que buscaba en un archivo llamado *94:01.ongoing.network.monitoring.atta* El archivo proporcionaba instrucciones para desactivar el software de seguimiento, y ahora él procuraba averiguar cómo activarlo de nuevo. Lo

irónico del asunto era que el archivo de CERT no era siquiera un aviso reciente, sino en realidad de hacía más de un año. No obstante, él lo seguía con la misma atención de quien sigue una receta en un libro de cocina, trabajando en las mismas narices de los administradores de sistema de la CSN.

Al ver que nuestro intruso venía ahora de Denver, le puse otra llamada a Kent para decirle que necesitábamos un rastreo y localización de llamadas telefónicas allí, además de en Raleigh. Mientras Robert y Julia permanecían absortos en los fragmentos de las sesiones del intruso, yo empecé a pensar

en cómo íbamos a montar una operación de seguimiento que nos permitiese efectivamente rastrearlo. Cada POP de la Netcom tenía bancos de modems conectados a un dispositivo llamado servidor de comunicaciones Portmaster, fabricado por Livingston Enterprises, una compañía de Pleasanton, California. El Portmaster permite al usuario acceder a los ordenadores de la Netcom de su propia red. Nuestro problema era que los Portmaster, a diferencia de otros modelos, mezclaba las sesiones independientes de cada ordenador en una sola corriente de datos, lo que nos imposibilitaba desmenuzar

individualmente cada sesión. Robert conocía al fundador de la Livingston y dijo que haría una llamada de emergencia para preguntarle si podía ayudamos.

Nuestro siguiente problema era encontrar la forma de realizar el seguimiento del anillo de FDDI. La tarea requería un ordenador rápido, una tarjeta interfaz y un concentrador para enganchar la máquina al anillo de la Netcom. Desgraciadamente la Netcom no disponía de recambios de ese hardware. Suponiendo que pudiésemos conseguir el hardware, aún nos haría falta un código fuente del controlador de

software para la tarjeta y poder modificarlo de forma que nos permitiese el seguimiento del anillo. Yo recordé que tenía software FDDI copiado en una cinta en mi casa de San Diego, pero como nadie tenía allí una llave de reserva, no iba a servirnos de mucho.

Estuve paseándome por el atestado despacho de Robert intentando pensar dónde podíamos conseguir un concentrador FDDI para enganchar un ordenador de seguimiento al anillo de Netcom.

Me devané los sesos pensando dónde podría encontrar semejante equipo en Silicon Valley a esa hora de

la noche. No podía simplemente entrar en cualquier parte y servirme, y era improbable que lo que necesitábamos lo tuviesen en Fry's, la tienda de suministros famosa en el valle por vender desde ordenadores hasta patatas chip, pues los concentradores FDDI cuestan normalmente muchos miles de dólares.

De pronto me di cuenta que conocía a la persona justa.

Llamé a mi amigo Soeren Christensen, el *gurú* en redes ATM de la Sun, con quien yo había trabajado. Estaba aún en la oficina cuando telefoneé y, después de explicarle

nuestros apuros, le dije que era vital que para las 7 de la mañana siguiente —hora a la que el intruso solía reaparecer cada día— dispusiéramos de una estación de rastreo instalada y en funcionamiento

"Soeren, ¿te acuerdas de aquel concentrador FDDI que estaba en el techo de vuestro laboratorio en Mountain View antes de que os mudaseis a Menlo Park?", le pregunté. "No lo habréis conservado y lo tendréis abandonado por ahí, ¿verdad?".

"Creo que puedo dar con lo que necesitas, Tsutomu. Me parece que recuerdo por dónde está", respondió. "Es probable que encuentre también

algún hardware extra. Voy a echar una ojeada".

"Estupendo", dije. "¿Dónde podemos vernos?".

Resultó que Soeren planeaba cenar con su mujer en una pequeña cervecería de Sunnyvale llamada la Fault Line, no lejos de las oficinas de la Netcom. "Ordenaremos un poco aquí y nos reuniremos contigo allí dentro de un ratito", le dije.

Cuando colgué el auricular, Robert y Julia seguían observando las payasadas del intruso, y me llevó cierto tiempo arrancarlos de allí para estar seguro de llegar a tiempo al restaurante. Eran casi

las diez menos veinte de la noche y la cervecería cerraba dentro de veinte minutos. Resolvimos ir todos en el mismo coche, puesto que planeábamos volver a pasar el resto de la noche preparando las operaciones de seguimiento. El Mazda de Julia estaba casi enteramente ocupado por mi equipo de esquí, así que nos apilamos en el brillante Mustang verde azulado de John Hoffman. Tanto Robert como Hoffman tenían lo que parecían potentes coches americanos recién salidos de fábrica. Mientras que el modelo estándar de coche del ingeniero de Silicon Valley es normalmente un BMW o un Saab, los

dos técnicos de la Netcom debían estar algo impregnados de la cultura nativa de San José. Era un poco como en *American graffiti*, el filme de 1973 en el que George Lucas describe los primeros años sesenta en una ciudad del Central Valley de California donde la vida gira aún en torno a los coches y no los ordenadores.

La Fault Line es una de las docenas de cervecerías que han surgido en la zona de la bahía durante la última década. Sustituto mejorado de las tabernas de cerveza y hamburguesa de una era anterior, estas minicervecerías poseen una cocina californiana más

sofisticada, así como una selección de cervezas exóticas, elaboradas en grandes cubas generalmente a la vista detrás de mamparas de cristal al fondo del edificio.

Julia y yo quedamos perplejos ante la lista de cervezas, pero admitimos que después de un par de vasos no habría forma de permanecer activo toda la noche, que era lo que al parecer nos esperaba.

Soeren y su esposa, Mette, ya habían llegado cuando aparecimos los cuatro. Vi que la camarera le traía a Mette puré de rábano picante. "Sólo en California", pensé. Mientras le contaba a Soeren lo

que nos proponíamos, todos intentábamos relajamos, porque sabíamos que aquel podía ser el último paréntesis de descanso que tendríamos en bastante tiempo. Durante la cena hablamos del sistema de seguimiento que necesitábamos instalar y del problema de conseguir un ordenador lo bastante rápido para adaptarse al anillo FDDI de la Netcom. Soeren, uno de los mejores diseñadores de equipamiento de redes de la Sun, dijo que había encontrado las suficientes partes sueltas de hardware como para que armásemos un ordenador a la medida. Creía también tener el controlador del código fuente

del FDDI en una copia en cinta que guardaba en su apartamento, cercano al restaurante, de modo que convinimos en que Julia volviera más tarde con él a recogerla.

Después de la cena nos detuvimos en el aparcamiento mientras Hoffman maniobraba marcha atrás hasta situar su coche junto al maletero del de Soeren.

"Esto parece un negocio con drogas en Silicon Valley", dijo Julia. Todos reímos nerviosamente.

Desde luego que en realidad era sumamente improbable que alguien nos dedicase siquiera una segunda mirada. Probablemente, la mitad de las empresas

del valle empezaron con los vendedores trabajando con la mercancía en el maletero de su coche. Soeren me alcanzó dos bolsas llenas de elementos diversos, incluyendo conectores, memoria, un módulo procesador y varias tarjetas interfaz. Mirando el material, dije: “Vaya, no deberías haberte tomado el trabajo de desarmarlo, podrías haber traído el ordenador entero”.

En cuanto llegamos a la Netcom, Hoffman se puso a armar el nuevo ordenador de seguimiento, poniendo pequeñas pegatinas verdes en todas las piezas de equipo de Sun para que pudiésemos identificarlas fácilmente.

Eran más de las once cuando llamé por el busca a Andrew, que estaba en Berkeley cenando con Mark Seiden en el Siam Cuisine, el primero, y algunos dicen que todavía el mejor, de los restaurantes de la East Bay. Habíamos convenido en cederle a Mark parte de nuestra estrategia de seguimiento para facilitarle el rastreo del intruso en Internex.

"Andrew, necesito que vuelvas a la Well a recoger mi RDI y a traer todas nuestras herramientas de software aquí a la Netcom", le dije. "Va a ser una larga noche, porque hemos de tener el seguimiento listo para cuando él entre en

actividad de nuevo mañana por la mañana".

Nuestro transgresor iniciaba su tarea generalmente alrededor de las 7, hora del Pacífico, y luego continuaba accediendo de forma intermitente a lo largo del día. Solía desaparecer por unas horas a eso de las tres de la tarde y luego retornaba a pleno rendimiento y con frecuencia permanecía activo hasta bien pasada medianoche. Era cada vez más claro que quien fuera que estuviese al otro lado de la pantalla de nuestros ordenadores no era un travieso casual, sino un adversario profundamente obsesionado con lo que fuera que

estuviese haciendo.

Julia volvió alrededor de medianoche con la cinta FDDI de Soeren y nos llevó un buen rato dar con el controlador de cinta adecuado para leerla. Cuando finalmente miré el software de Soeren mi corazón dio un vuelco. Era ciertamente el código fuente del software del controlador, pero estaba escrito para el sistema operativo Solaris 2 de Sun. La Netcom operaba con Solaris 1. Era inútil.

Yo había esperado insertar fácilmente el software de Soeren en nuestro ordenador de seguimiento. Si efectivamente hubiésemos tenido el

código fuente habría sido bastante sencillo. Habría querido usar mi software modificado de filtro de paquetes Berkeley (BFP) porque estaba escrito como para adecuarse al torrente de paquetes de datos que discurría por el anillo de fibra óptica de la Netcom. Ahora íbamos a tener que emplear otra estrategia.

A las 12:40, mientras desempeñábamos nuestras diversas tareas, el intruso reapareció. Seguía entrando desde Denver y continuaba interfiriendo los ordenadores de la CSN. Poco rato después Robert le vio forzar la entrada en *fish.com*, el ordenador de

Dan Farmer. Observó al intruso examinando en el correo de Dan la aparición de sus diferentes hileras de texto, itni y tsu. La primera significaba que ciertamente seguía buscando la palabra Mitnick, y la segunda era probablemente por mí. Si mi oponente era realmente Mitnick, ahora había cobrado un acuciante interés en mí. Al cabo de un rato estaba de nuevo en los ordenadores de la Netcom, esta vez tratando de descubrir adonde era encaminado el correo de Rick Francis.

Como a las dos de la mañana apareció Andrew con nuestro hardware y software y se puso inmediatamente a

trabajar con la intención de encontrar la forma de instalar el software de paquetes Berkeley en el software del controlador FDDI partiendo de cero. Yo estaba completamente seguro de que sin el código fuente no iba a funcionar, pero Andrew era optimista y se puso a la tarea.

La mayor parte del personal de la Netcom se había ido horas antes, dejándonos solos entre aquellos cubículos individuales separados por mamparas en los salones sin ventanas. Las únicas otras personas que quedaban eran unos instaladores al otro extremo del piso que ponían un nuevo PBX en el

cuarto de las máquinas de la Metcom. La compañía tenía el aspecto de un típico negocio de Silicon Valley en pleno hipercrecimiento. Tan pronto como se trasladan a una nueva sede, estas organizaciones tienden a crecer exageradamente. Todo parece estar cambiando de continuo. Desgraciadamente, otra característica del valle es que las cosas tienden a derrumbarse a la misma velocidad con que se expanden.

Hacia las tres de la mañana todos notábamos la falta de sueño, y Robert, Hoffman y Julia iban a cada momento hasta la máquina expendedora de

refrescos que estaba en un espacio abierto al otro lado de la oficina del primero. A mí la cafeína nunca me ha hecho efecto. Al cabo de un rato se empezaron a agotar las existencias.

"Pronto nos quedaremos sin nada que tenga cafeína", dijo Andrew.

Yo me paseaba nerviosamente entre Andrew, que luchaba con el software FDDI; Robert, que controlaba las operaciones de la red; y John Hoffman, que seguía trabajando en el cuarto de máquinas de la Netcom para establecer nuestra nueva estación de seguimiento.

No obstante mis quejas sobre la Netcom, en realidad estaba sumamente

impresionado por su organización. Entré en el cuarto de máquinas y vi filas y más filas de ordenadores de servicio SPARCstation. Todo estaba dispuesto de manera impecable y profesional. El diseño y la construcción del sistema parecían inobjetables.

Eran casi las tres y media de la mañana cuando finalmente encendimos el nuevo ordenador que había sido instalado detrás de la puerta cerrada con llave del cuarto de las máquinas de la Netcom. Hoffman le puso de nombre "looper"[34], en referencia a la red FDDI instalada a modo de anillo en torno al cual fluían los paquetes.

Andrew no había conseguido insertar el BFP sin el código fuente, y el tiempo para más experimentos se nos agotaba con rapidez.

Pensé en nuestras demás opciones. Teníamos dos tarjetas FDDI diferentes de Soeren: una hecha por la Sun y otras por una compañía llamada Crescendo. Estaba bastante seguro de que la de Sun, con su software estándar de controlador no nos permitiría, incluso operando en una SPARCstation veloz, filtrar paquetes con suficiente rapidez para seguir el ritmo del anillo FDDI de Netcom a plena carga. La tarjeta y controlador de la Crescendo

supuestamente tenían un mejor rendimiento, pero yo no sabía hasta qué punto.

Probé primero la tarjeta Crescendo. Tenía la esperanza de que funcionara lo bastante bien como para que, incluso si no podíamos emplear el software BFP, la NIT hiciera el trabajo. La NIT es lenta, pero tal vez la velocidad de la tarjeta y la SPARCstation 10 pudieran compensar esa ineficacia. Si eso no solucionaba el problema, la única opción restante era pensar en alguna otra salida inteligente, que todavía no se me había ocurrido.

Una vez colocada la tarjeta, sólo

fueron necesarios un par de minutos para damos cuenta de que no era ni de cerca lo bastante rápida y de que cuando la costa Este se pusiera en actividad estaríamos peleando una batalla perdida.

Todas las mañanas, alrededor de las cinco o las seis, el número de paquetes que circulaba por su red FDDI empezaba a aumentar, a medida que la gente de la costa Este registraba su entrada para revisar su correo y poner su red en funcionamiento. Robert se fijó en el visualizador que controlaba en su ordenador el número de paquetes en curso por el núcleo de la red FDDI.

Unos 4.000 paquetes por segundo.

"Eso es habitualmente el nivel mínimo", dijo.

Andrew, entretanto, vigilaba el funcionamiento del looper.

"Esto no va bien, Tsutomu", dijo. La red Netcom apenas se percibía y ya estábamos perdiendo el uno por ciento de los paquetes que pasaban ante nuestra estación de seguimiento.

"Esto no sirve", me quejé, sin dirigirme a nadie en particular.

Resolvimos probar la tarjeta FDDI de Sun, pero resultó ser todavía más lenta que la de la Crescendo, y menos fiable. Reinstalamos la primera y

reanudamos nuestro intento de seguimiento de la red.

No servía. Al mirar la pantalla de la SPARCstation vimos que estaba funcionando a un 70 por ciento de su capacidad. No tardó en ponerse peor. Mientras estábamos sentados observando, el número de paquetes que perdíamos empezó a aumentar vertiginosamente según crecía la carga en la red. En mi mente se formó la imagen de una multitud de personas a lo largo de la costa Este, todavía en bata de dormir y cada una con el jarro de café en la mano, yendo a su estudio a conectarse a la Netcom. Me pregunté:

“¿Disfrutarán esos la vida más que nosotros? Bueno, al menos ellos han dormido bien”.

“Tsutomu, dentro de poco vamos a estar en veinte mil paquetes por segundo”, dijo Robert.

Parecía evidente que teníamos que hacer algo que llevase sólo un par de minutos y funcionase, aunque fuera un kludge (en la jerga informática, un artefacto semejante a los inventados por Rube Golberg).[35]

“Podría funcionar si colocásemos algo delante de la NIT”, le dije a Andrew. “Podría intentar una chapuza escribiendo un prefiltro que clasifique

los paquetes antes incluso de entrar a la NIT".

Andrew asintió con la cabeza, aunque a esas alturas no estoy seguro de que en realidad le importase. Estaba tendido en un sillón de oficina frente a mí y parecía estar ya medio dormido.

Estuve pensando otro poco en el problema y repasé los archivos de fuente de los sistemas operativos que tenía en orden para tratar de entender algo mejor lo que estaba ocurriendo entre el software del sistema y la NIT. Probablemente, un filtro muy pequeño fuese bastante rápido; no descomunalmente rápido, claro, pero

quizá lo suficiente para poder hacer frente a la cantidad de paquetes que pasaran por delante de nuestra máquina de seguimiento incluso en los momentos de máxima carga. Mi programa era lo menos parecido a una solución perfecta, un pedacito de software de muy bajo nivel que colocado delante de la NIT descartaría la mayor parte de los paquetes antes siquiera de que llegasen al ineficaz y engorroso programa. Le puse *snit___foo* y lo escribí sin tomarme siquiera la molestia de usar un editor. Simplemente fui copiando cada línea que escribía en un archivo y luego la convertí para que pudiera ser leída por

el ordenador.

Me senté ante el RDI y escribí lo más rápido que pude mientras Andrew miraba por encima de mi hombro. Cuando terminé, me volví hacia él y dije: "¿Has notado que hiciera alguna cosa mal?".

Él echó una rápida ojeada a mi código para ver si en alguna parte corría el riesgo de desbaratarse. Mi programa estaba diseñado para filtrar hasta ocho direcciones de red diferentes y rechazar todos los demás paquetes. Si funcionaba correctamente, la NIT tendría que operar únicamente con un pequeño porcentaje de los paquetes que circulasen por el

anillo FDDI.

Después que Andrew inspeccionó el código yo lo compilé en el RDI y pareció funcionar. Copiamos el programa en un disco flexible y lo llevamos al cuarto de las máquinas, donde lo pusimos en el looper. Era un *kludge* horrible, pero a esa altura no había nada que perder.

Yo estaba exhausto, pero la presión de saber que podríamos ver a nuestro oponente a las siete de la mañana me mantenía en actividad. Estuve un rato tratando de insertar correctamente mi programa en el núcleo del sistema operativo. Después de varios intentos

comprendí qué era lo que estaba haciendo mal. Eran casi las seis cuando empezó el goteo de paquetes a archivos que reconstruiríamos más tarde ese día. La red de Netcom comenzaba a mostrar actividad. Hice algunas pruebas y todo parecía funcionar adecuadamente, y la carga en la máquina era manejable. Entonces Andrew y yo dedicamos algún tiempo a configurar el filtro. Con todo bajo control por el momento, abandoné el cuarto de las máquinas y fui a ver qué había sido de Julia. Ella mantenía el plan de irse el fin de semana con John y alrededor de una hora antes había desertado y se había acurrucado debajo

de uno de los escritorios de la oficina, fuera del despacho de Robert. Seguía aún agotada en el rincón, con mi parka de almohada.

A Robert lo preocupaba el que los empleados de la Netcom que entrasen por la mañana fueran a llevarse una sorpresa al encontrar a una desconocida durmiendo debajo de un escritorio. Pero Andrew se había ocupado de ese problema colgando por encima de la cabeza de ella un trozo de papel que ponía: “¡No molestar!”.

12. La prueba

Las primeras luces del alba nos encontraron a Julia y a mí de pie en un balcón del edificio de la Netcom frente a la oficina de Robert. A través de la fría bruma matinal vi que el tráfico de primera hora de los abonados al transporte público fluía ya por el bulevar Winchester. Me puse la parka, pero la neblina de la mañana seguía dándome escalofríos.

"Tsutomu, aquí todo el mundo tiene

algo que hacer, excepto yo", dijo ella. "Me siento como una quinta rueda. No debería estar".

Era verdad. Durante casi toda la larga noche Robert se había encargado de la red, Andrew y yo habíamos lidiado juntos con el código de filtrado, y John Hoffman había establecido la estación de seguimiento. Después de volver de la casa de Soeren con la cinta de control, Julia había quedado en un segundo plano mientras los demás nos enfrascábamos en aquella tarea. Estaba disgustada por ser la recadera del equipo.

Le hice notar que en la Well había

sido nuestra diplomática, actuando de puente con Claudia, a quien en rigor yo no había prestado atención. Pensé en el fin de semana anterior, cuando Julia decidió acompañarme en el viaje a la Well.

"Cuando empezamos esto me dijiste que querías participar porque sería una oportunidad para observar y aprender", le recordé. Me daba cuenta de que estaba exhausta, que se sentía mal consigo misma y de que había otra cosa que la preocupaba. Pero yo no quería mantener esa conversación en aquel momento. Los dos habíamos estado despiertos durante casi veinte horas y

nos aproximábamos a la hora en que generalmente el intruso entraba en actividad. Era necesario que volviésemos adentro; porque nuestro equipo de seguimiento requería una cuidadosa atención, pues en las pasadas doce horas el intruso había cambiado sus pautas y ya no venía exclusivamente por el POP de Raleigh. Lo habíamos rastreado hasta este momento y ahora era preciso que calculásemos rápidamente cuál sería el próximo paso. Mi sensación de urgencia aumentaba y no quería que esta oportunidad se nos escapase. Cuanto más esperásemos, mayor era la posibilidad de que algo

marchase mal. Yo había contado con que fuera una criatura de hábitos, y ahora me preocupaba perder algo de nuestra ventaja.

Permanecimos allí un rato más contemplando hacia el este las colinas, apenas visibles a través de la bruma. Hacía frío y yo experimentaba ese estado nauseabundo de cuando se ha pasado demasiado tiempo sin dormir.

Finalmente, para romper el silencio, dije: "Él se pone en acción a partir de las siete, tengo que volver adentro. Es preciso que vea si estamos preparados".

Entré en la oficina de Robert y me quedé sentado un rato. Tras haber

pasado la noche con nosotros, él estaba ahora de nuevo trabajando en sus tareas cotidianas. Observamos cómo el software de seguimiento operando en su estación de trabajo mostraba que la carga de la red FDDI empezaba a aumentar de una forma constante. Quedaba aún mucho trabajo que hacer, pues la información desde cada POP que veíamos era conservada como una masa indiferenciada de datos. Sin el software que Robert le había pedido a Livingston que nos suministrase no podríamos dividirla en sesiones de usuario individual. Era como si nos hubiesen entregado una caja conteniendo las

piezas de diferentes rompecabezas. Primero teníamos que separar unos de otros, que era precisamente lo que el software de Livingston nos ayudaría a hacer. Sólo entonces podríamos reconstruir lo que efectivamente ocurría en una sesión individual.

Al cabo de aproximadamente una hora Robert sugirió que bajásemos todos a desayunar en una pastelería situada en la planta principal del edificio de la Netcom. Andrew había gastado todo su dinero y pensaba tomar únicamente una taza de té, pero cuando abrí mi billetera y me encontré seis dólares, le di la mayor parte para que se comprase algo

de comer. Julia tomó café y yo un té en taza de plástico, y como Andrew y Robert se habían ya sumido en una discusión técnica, salimos fuera a sentamos en un patio del edificio. Mientras salíamos comentamos riendo la imposibilidad de hablar todo el tiempo en términos tecnológicos, como parecían hacerlo Robert y Andrew. Estuvimos de acuerdo en que en esta vida es necesario un cierto equilibrio.

Yo fingía beber de la taza vacía escuchando a Julia. Percibía la tensión en su voz. Era algo habitual, cada vez que tenía que volver a encontrarse con John se ponía tensa y nerviosa. Pero esta

vez no se daba cuenta.

"Tendré que descansar un poco si voy a encontrarme con John este fin de semana", dijo. "Si me presento allí totalmente agotada no será más que otro desastre".

Pasamos una hora y media intentando hablar de lo que la inquietaba, pero no estábamos llegando a ninguna parte y yo me sentía cada vez más frustrado. Regresamos arriba y seguí trabajando en mis herramientas de seguimiento. Había llegado el software para separar los datos venidos de los Portmaster, pero para poder usarlo tenía primero que trabajar bastante con mis

propias herramientas.

Nuestro filtro perdía paquetes, y estuve un buen rato con el programa de Livingston para estar seguro de que capturaría alguna de las sesiones de *gkremen* en los ordenadores de la Netcom.

El intruso había retornado poco después de las diez de la mañana y como una hora después Julia y Andrew entraron en la oficina de Robert para ver qué hacía. Robert nos dijo que hasta el momento lo había visto registrar su entrada a través de los POPs de Raleigh y Denver. Mientras ellos miraban por encima del hombro de Robert, yo

continuaba trabajando en el software y escuchando al mismo tiempo sus comentarios a través de la puerta de su oficina.

El pirata había conectado desde Netcom con *hacktic.nl*, el ordenador que en Holanda es un centro de reunión para el submundo informático. Utilizaba el nombre de cuenta martin. Más tarde podríamos extractar con precisión sus actividades en un vídeo, pero por el momento teníamos que depender de la tosca herramienta de Robert que capturaba caracteres en un pequeño buffer de memoria temporal y los desplegaba en la pantalla.

“El pulsador de mi ratón se está gastando”, dijo Robert. El último día, cada vez que había un forzamiento Robert le había seguido el rastro apretando repetidamente el botón del ratón para recoger los fragmentos de las pulsaciones del intruso en su teclado.

Estaban observando la pantalla cuando el intruso intentó establecer una sesión de conversación con alguien cuyo nombre de usuario era jsz. La base de datos de un centro de información de red reveló que estaba localizado en Israel. Indicó asimismo que tecleaba desde una estación de trabajo Silicon Graphics. La conexión israelí era interesante, pues se

rumoreaba que Kevin Mitnick había huido a Israel cuando era un fugitivo en California a mediados de los años ochenta. Era otra pista provocativa.

El intruso inició un programa llamado talk, que dividía su pantalla en dos permitiéndole ver en la parte superior lo que él tecleaba y en la inferior lo que respondía jsz.

```
[sin conexión aún]
[aguardando respuesta]
[llamando nuevamente]
[aguardando respuesta]
[conexión establecida]

martin: joder esto va lento
jsz:        eh. OK, un momento.
        Estoy también en otra
```

```
          ventana.
martin:   hola
jsz:      hola
martin:   sí, estoy retrasado con
          el hacktic.

jsz:      AHhh. OK. ¿qué pasa?
martin:       ¿puedes      enviarme
          material sol & mail?
```

Después de quejarse de la extrema lentitud de la comunicación, al parecer martin le pedía información a su contacto israelí. “Sol” se refería probablemente a Solaris, la versión de Unix distribuida por Sun Microsystems, y “mail” podía significar Sendmail. Los fallos de seguridad en los sistemas de correo han sido tradicionalmente una vía

para el forzamiento de ordenadores.

jsz: ok. ya te envié sol.
martin: necesito que lo envíes de nuevo estaba alterado. ¿puedes enviarme ahora lo del correo también?
jsz: ok. vale, te lo envío, pues.
martin: ok favor enviar ambos de nuevo tus anteriores pgp msg inservibles.
jsz: ok. te dejaré uno otra vez :0
martin: ok ¿quieres probar lo de correo conmigo ahora?

Aquí se produjo una larga pausa; estaba claro que martin era persistente.

jsz: ¿ahora? no; lo probaré yo mismo después, tal vez… ¿quieres probarlo @oki?

martin: ok puedes enviarlo ahora para que pueda probarlo yo :-)

jsz: OK. Te envié material sol. compruébalo ahora, ¿ok?

martin: vale

jsz: buscaré y envío 8.6.9. después.

martin: hmm… esperaba me enviaras lo de correo enseguida para poder hacer ciertas cosas.

Otra larga pausa. Estaban efectivamente hablando de Sendmail: la

versión actual era la 8.6.9.

```
jsz:     OK. sendmail enviado.
martin:  un momento
jsz:     comprueba tu correo
martin:  estoy también en lo del
         teléfono… ok ¿entonces
         enviaste sendmail & sol?
jsz:     sí
martin:   gracias ¿no quieres
         probar oki ahora?
jsz:     no
```

En este punto parecía que martin tratara sin éxito de persuadir a su colega de que utilizara sus herramientas especiales de forzamiento para atacar a un ordenador pasarela a Internet perteneciente a Oki Telecom, el

fabricante de teléfonos móviles.

martin: ok, ¿están los detalles completos en sendmail para que yo pueda hacerlo con o sin tu ayuda?

jsz: fíjate y lo verás por ti mismo, si sabes instalar identd, supongo.

martin: ok, eh ¿estás en labs?

jsz: no el CS.

martin: ohh ok bien ¿quieres reunirte online más tarde?

jsz: vale, pero no vayas a estropear este fallo :-)

martin: dame una oportunidad. CERT lo hará en pocos días :-(

jsz: Jejeje.

Jsz le estaba diciendo a martin que no compartiese la información que sobre una determinada vulnerabilidad de sistema acababa de darle. Ambos sabían que tan pronto como ellos sacaran partido de la misma la comunidad de seguridad informática entraría en alerta y la puerta clandestina desaparecería.

martin: gracias por la confianza, yo también la protegeré ¡tengo tantos deseos de utilizarla como tú!

jsz: sin problemas B-)

jsz: "Dadme un punto de apoyo", dijo Arquímedes, "y moveré el mundo" :—) (acabo de leerlo en el

correo de alguien mientras hablamos :—)

martin: :-)

Aquellos tipos usaban el correo electrónico de los demás como quien utiliza la biblioteca.

La sesión terminó, y Robert dijo a todos que salieran de su atestada oficina. A partir de los datos de la sesión yo revisé lo que sabía sobre la técnica del intruso. Era evidente que se creía inmune a la vigilancia. Como había ocurrido en muchos de los otros emplazamientos de ordenadores en los que había forzado su entrada, probablemente había intentado plantar

un sniffer en la Netcom y se había encontrado con que no podía controlar el FDDI de alta velocidad. Al fracasar, había supuesto que si él no podía instalar un husmeador, nadie más podía hacerlo. Habría concluido que poseía una gran ventaja de seguridad al efectuar el primer salto de sus incursiones de pillaje en Internet a través de la Netcom, donde no podía ser detectado. Se equivocaba, pues nosotros habíamos logrado algo que él probablemente consideraba técnicamente imposible. En esta partida que jugábamos él había hecho una suposición incorrecta y puede que tuviera que pagar por ello.

Me encontraba aún en el espacio abierto al que daba la oficina de Robert, fascinado por el anuncio luminoso en forma de caracol encima de la máquina expendedora de golosinas cuando, un momento después, Robert gritó: "Hay una sesión de gkremen procedente de Atlanta".

¡Atlanta! Nunca habíamos visto una sesión procedente de allí. ¿Intentaba el intruso enmascarar su ubicación entrando en la red de la Netcom desde todavía más sitios? Entré de nuevo en el looper y agregué la dirección de Atlanta a nuestro filtro, e inmediatamente la información que estábamos guardando

se convirtió en una cascada. Atlanta sola generaba más de nueve megabytes de datos por minuto.

Me asusté mucho.

Hasta la noche anterior a nuestra llegada a las oficinas de la Netcom, sus registros habían indicado que el intruso había estado conectando exclusivamente desde Raleigh, excepto cuando entraba en Netcom vía Internet desde *escape.com* o la CSN. Al llegar la noche del jueves había entrado varias veces desde Denver, y ahora desde Atlanta; por los registros vimos asimismo una breve conexión desde Chicago. Y lo peor de todo, la nueva pauta de

actividad había empezado casi inmediatamente después de que yo le pidiese a Kent, el fiscal ayudante, una orden de rastreo y localización. ¿Sabía el intruso lo del rastreo? ¿Era capaz de interceptar las comunicaciones de la compañía telefónica? ¿O de espiarnos a nosotros? Se sabía que nuestro adversario —si es que efectivamente era Kevin Mitnick— había interceptado ilícitamente las comunicaciones de representantes de la ley para mantenerse un paso por delante de ellos. Era posible que estuviese mofándose de nosotros. En tal caso, nuestra tarea iba a ser mucho más difícil. Me dije que

debía aguardar pacientemente y no ceder al pánico, esperando que la nueva pauta fuera sólo una anomalía.

Andrew y Julia volvieron para observar en el momento en que el intruso se conectaba de nuevo desde la Netcom con *hacktic.nl*, registrándose como martin, con la contraseña "oki, 900".

Primero revisó su correo, donde había tres mensajes de jsz El primero era la respuesta a una pregunta: "Eh, ¿donde estás, tío?"; contenía únicamente una línea: "okay, de vuelta".

El segundo y el tercer mensajes eran los archivos de texto provenientes de

jsz, codificados en PGP o Pretty Good Privacy, el programa de encriptación de datos gratuito, y guardados por martin con los nombres de archivo *solsni.asc* y *sendmail.asc*. Aunque los nombres eran intrigantes, su contenido estaba fuera de nuestro alcance. Con una clave de codificación suficientemente larga, los archivos PGP estaban fuera del alcance de las posibilidades decodificadoras de las agencias de inteligencia del mundo.

A continuación el intruso tecleó "w jsz", un comando que comprobaba si jsz seguía conectado al ordenador hacktic; pero jsz se había esfumado. Entonces martin retrocedió, se desconectó de

hacktic y retornó a la Netcom. Tecleó "ftp hacktic.nl" y luego volvió a entrar en el sistema holandés como martin. Esta vez transfirió a la cuenta gkremen los dos archivos que jsz le había dejado del ordenador holandés. Finalmente, completó el proceso descargando los archivos de la cuenta gkremen del ordenador de la Netcom en San José hacia su propio ordenador personal, donde quiera que éste estuviese oculto. Finalizada la transferencia borró inmediatamente de su cuenta los dos archivos.

Hubo una larga pausa. ¿Estaba pensando? ¿Estaba decodificando y

leyendo sus archivos? De pronto conectó otra vez con *hacktic.nl* y puso en marcha un programa llamado Internet Relay Chat, o IRC, que permite a miles de personas en todo el mundo participar en centenares de "charlas" de teclado simultáneas. Cuando el ICR le requirió, "por favor, introduzca su contraseña", él tecleó "marty".

¡Marty! Andrew y yo habíamos visto antes a "marty": era el nombre de la cuenta en la Well donde habíamos encontrado un escondite de software robado de telefonía móvil. Con el IRC se incorporó a un canal público llamado #hack, un punto abierto de reunión para

ciertos tipo de gente del submundo informático mundial. Instantáneamente su pantalla se llenó de la cháchara procaz de decenas de pesados, en su mayor parte obscena.

Haciendo caso omiso de la cháchara, le envió un mensaje a jsz. "¿ola jsz…? y luego corrigió la ortografía, "¿hola jsz?"

Sin suerte. Llegó un mensaje de réplica, "jsz ausente, envíame email".

Mientras meditaba su siguiente movimiento fue interrumpido: jsz contestaba. Reconociéndose mutuamente los dos conspiradores volvieron a hacer contacto secreto usando el programa

ntalk.

[sin conexión aún]
[conexión establecida]

martin: hola leí ese material MUY interesante SABÍA que el mastodon sería ORO!
jsz: :—) yo también sabía.
martin: oye necesitamos instalar una bd para que yo pueda usarlo también, hasta ahora no he JODIDO un emplazamiento dado por ti así demuestra la historia. :-) te gusta la historia, ¿no?
jsz: es mi asignatura favorita :)

Al parecer hablaban de un ordenador llamado Mastodon en el que se supone habían encontrado información útil sobre una puerta cladestina ("bd", por "back door").

jsz: jejeje. o sea, ¿quieres estar en el alias también? :—) mezquino :0

martin: eh, eso es bastante evasivo así: cuando alguien conecta a 25 ¿lo conecta efectivamente de vuelta a inetd en el remoto?

jsz: de vuelta, sí, exactamente — así es como realmente funciona (ie identd…) podría ser una desagradable bd allí

.—)

martin: Jejeje. ¿Cómo no se me ocurrió? pregunta: parece que puedes meter lo que sea en la que, ¿puede ejecutar portd como raíz o sólo cosas de correo?

jsz: lo estoy pensando, no creo que puedas hacerle ejecutar nada como raíz, pero podrías trucarlo para ejecutar algo para ti, trabajaré en ello más tarde hoy.

martin: hmm.. como dedo :-)

Andrew, Julia y Robert observaron con alarma que el amigo israelí de Martin se había enterado de un nuevo

fallo de seguridad en Sendmail. “Eh, tienen un nuevo agujero en sendmail”, me dijo Andrew a través de la puerta. “Algo relacionado con identd”. “Voy a desviar el rasgo enseguida”, repliqué. Lo dejé todo y me conecté con mis ordenadores en San Diego, asegurándome de que si nuestro intruso probaba el nuevo truco con nuestras máquinas se daría contra la pared. Al mismo tiempo, Robert telefoneaba a John Hoffman, dándole instrucciones de hacer lo mismo con todos los ordenadores de la Netcom.

Julia y Andrew empezaron a leer en voz alta lo que iba apareciendo en la

pantalla de Robert, para que yo pudiera oírlo mientras me ocupaba en cerrar el agujero en sendmail.

```
jsz:     mi héroe es eric allman
         :)
martin: el mío es japboy!
jsz:       a markoff dedo en el
         culo :)
martin:  ves markoff no actúa
         correctamente,        un
         reportero no AYUDA a
         agarrar a alguien no es
         ético, él es el motivo
         por el que mi foto
         estaba en primera plana
         del new york times
```

¡Teníamos la prueba! Martin no podía ser otro que Kevin Mitnick, y me

llamaba “japboy”. Aquello se estaba volviendo una cuestión personal, pero yo la sentía como algo distante y un tanto surrealista. “No me gusta nada”, comenté.

jsz: sabes, creo que markoff es un negro de mierda, está cansado de su vida negra, y necesita un poco de aventura. Habría que matarle :—) Le enviaré un paquete de parte de Sadam Hussein, o del Coronell Gadaffi, ¿quién suena más asustante, hussein o gaddafi?

martin: nah alguien :) hay que acceder a nytimes.com y

crear una historia sobre japboy de que es un bujarrón de niños convicto y que se imprima firmado por markoff.

jsz: JAJAJA., eso sería fenomenal. :)

martin: puedes suponer las consecuencias.

jsz: ¡tsu se pondrá furioso!

martin: sí, o añadir a un reportaje verdadero de markoff que menciona tsutomu es amante gay de dan farmers y que se reúnen en secreto en queernet.org

jsz: para hacer sexored :—) JAJAJA. Eso sería todavía más divertido.

martin: ¡sería el golpe del siglo!

jsz: jajaja, de veras que sí :-) markoff también *morirá*, tsu hará cuestión de honor joderle :)

El comentario continuaba, con nosotros tres asombrados por lo pueril e inane de aquel intercambio. Más que a criminales, sonaban como un par de delincuentes juveniles.

martin: oye, ¿8.6.9 conecta por defecto de nuevo con el arco inetd dor identd?

jsz: sí, claro (por defecto…) lo mismo el sendmail que ejecuta casper dick :—)

dik, incluso.

martin: :—) hmmm… bien obviamente podemos hacerle enviar mierda (ejemplo en memo) pero la mejor técnica es ejecutar código. :)

jsz: conoces técnica sendmail :)

martin: mira ¡yo SÉ la técnica sendmail! el truco es hacerlo pronto de modo de alcanzar nuestros objetivos antes de que cert anuncie el fallo.

En ese momento recordé el primer mensaje que recibí, en el que mi interlocutor se jactaba de conocer la técnica de sendmail. Obviamente,

aquellos dos lo sabían todo acerca del forzamiento de mis máquinas.

jsz: OK, trabajaré en ello, creo que no sería difícil, creo que no hay muchos okidoki, y algunos otros parientes :—)

martin: buena palabra, oki, dsys.

Martin se refería a Motorola, Oki Telekom y a un sistema informático en Colorado, como posibles blancos para un ataque.

jsz: usa telnet con ellos y ves :—)

martin: aquí yo no tengo

```
ventanas como tú.
tendría que
desconectarme de talk
entonces tú quieres
aguantar, aguanta en brb
```

En este momento Martin salió del programa de conversación y realizó un breve chequeo para ver qué versión de Sendmail estaba empleando el ordenador puerta de Motorola.

```
Parado
xs1% telnet motgate.mot.com 25
Probando 129.188.136.100 …
Conectado con motgate.mot.com
Carácter de escape es '^]'.
220 motgate.mot.com. 5.67b/10a -
        1.4.4/mot-3.1.1
Sendmail está listo en Viern.10
```

Febr 1995 15:01:15 -0600

500 Comando no reconocido
fuera
221 motgate.mot.com cerrando conexión
Conexión cerrada por huésped ajeno.

xs1% fg
martin: no va 5.67b sendmail acabo de comprobar
jsz: un momento ahh… eso es IDA sendmail.
martin: Supongo que no hace el mismo truco identd.
jsz: no estoy seguro, ejecuto el mismo sendmail en netsys
martin: eh ¿es netsys.com un servicio que vende cuentas shell como

escape?

Netsys era un sistema de ordenadores perteneciente a un programador llamado Len Rose, que había estado un año en la cárcel por robar software mientras actuaba de consultor en AT&T.

jsz: no
martin: ¿cómo conectas?
jsz: no se puede conectar con netsys desde afuera siquiera :—) inténtalo. detestable firewall obra de moi :-)
martin: veamos: ¡podemos ejecutar tap en ramon NOT!

Reconocimos a “Tap”: era el programa que habían utilizado en el secuestro de mi conexión entre Osiris y Ariel.

jsz: ramon es SGI, no admite módulos cargables :) :) :)

martin: bromeaba si pudiera violaría nuestra confianza.

jsz: ¡lo sé! Huy, beavis & butthead en MTV (tenemos tv en los laboratorios en EE)

martin: eh acaban de dar sneakers por t.v. esta semana el viejo marty qué tío.

jsz: hmm, aquí tenemos

canales europeos, sólo CNN es desde US. [visne]akers hace poco

martin: eh ¿todavía no tenemos playnyboy.com?

jsz: no ha habido tiempo :) me ocuparé de ellos más tarde hoy, supongo, o mañana.

martin: ahh ¿tienes una bd en sunos.queer box husmearé un poco si quieres.

jsz: aún no. maddog.queemet.org es el sol, la última vez que comprobé : vaya nombre, eh ddog.

martin: normal bd como access1

Cuando Andrew mencionó "access1" yo agucé las orejas. Ese era

el nombre de un ordenador firewall utilizado por Sun para proteger su red interna de la ingobernable Internet. ¡De modo que también tenía una puerta secreta!

```
jsz:     ^F—tu apellido :-)
martin:        JAJAJAJAJAJAJAJAJAok
         ^fbishop
jsz:           ^F^B^I   :—)   rsh
         ard.fbi.gov —1 marty csh
         - fbi :-)
martin:  no debemos NUNCA dejar
         que se sepa esa bd, ¿así
         que lo tienes instalado
         en maddog?
jsz:      nah, como dije: no hubo
         tiempo ;—)
martin: ahhh pensaba que siempre
         harías   una   bd   para
```

ulterior acceso oh bueno…

jsz: sí lo haré en algún momento este fin de semana, de todas formas, vuelvo a codificación :—)

martin: eh tenemos que repasar de nuevo el procedimiento para que yo también pueda empezar a hacerlo. Tengo algunas nortas pero ha pasado tiempo, lástima que estés tan lejos.

jsz: ¿algunas nortas?

martin: notas - perdón.

jsz: una vez te mandé contraseña :-0

martin: ahh bueno comprobaré el otro disco codificado.

eh has sido EN VERDAD una gran ayuda con lo de unix. Voy a enviarte un agujero que funciona en TODAS las cajas VMS hasta 6.0 de mti amigo nmc.

jsz: uau. eso será muy impresionante, ojalá conociera mejor VMS :—)

martin: pero NADIE más lo tiene así que es como darte fr. POR FAVOR JAMÁS lo compartas, ok

jsz: nmc sí, ¿no? fr /:0 No tengo a nadie con quien compartirlo, y de verdad no tengo ningún deseo de echar a perder tu diversión VMS :-)

Nmc era obviamente Neill Clift: otra prueba de que efectivamente Martin era Kevin Mitnick.

martin: perfecto yo lo pgp más tarde está noche ahora estoy saliendo, funcionará en bgguvms :-)

jsz: Gracias… lo apreciaré… Ok, esta noche estaré codificando… te hablaré mañana o así.

martin: ni siquiera dejo que alguien más sepa que lo tengo pero tú confías en mí y yo en ti así que tal vez puedas usarlo tú también en tus exploraciones :-)

jsz: mándame email ¿vale? ¡gracias!

martin: ok no hay problema es efectivamente el MEJOR fallo en VMS que tengo en mi caja de herramientas.

jsz: gracias :—) ¿desde remoto? :)

martin: no, remoto no. No tengo un fallo remoto en VMS 5.0 y mayor. pero sí para vms 4.7 y menores.

jsz: estupendo… creo que bgvms es 6.0, (no estoy seguro, tendré que comprobar…todavía) Gracias de todos modos :-)

La conversación cesó de repente, al

parecer porque la conexión se había cortado, pero en el atestado cuartel general de Robert se creó un cierto alboroto. Ahora no cabían muchas dudas sobre quién era el intruso. Que yo supiera sólo había un delincuente informático cuya foto hubiera salido en la primera plana del *New York Times*.

El 4 de julio de 1994 Markoff había escrito un artículo en el que llamaba a Mitnick "el mayor fugitivo del cyberspacio". Había contado algunas de sus huidas haciendo notar que llevaba más de año y medio eludiendo al FBI y a otros cuerpos de seguridad. Creo que en aquel momento el artículo dejó al FBI en

ridículo.

Llamé a Markoff, le conté la conversación que Robert acababa de ver y le pregunté si en la primera página del *New York Times* había aparecido algún artículo suyo con la foto de algún otro.

"La única otra persona que se me ocurre es Robert Tappan Morris, y es obvio que esto no es cosa de él", me dijo.

Por fin teníamos un rostro y una serie de motivos que atribuir a las fantasmales huellas electrónicas que habíamos estado siguiendo durante más de un mes, pero todavía quedaba mucho por explicar.

¿Quién era jsz? Hice algunas llamadas, y las personas con las que hablé dijeron haber oído hablar de él. Una dijo que creía que jsz estaba trabajando como subcontratista para una compañía estadounidense de semiconductores que poseía un laboratorio en el Oriente Medio.

Estaba claro que Mitnick dependía de jsz como fuente de conocimiento experto en la violación de Unix, a cambio de su propia práctica con el sistema operativo VMS de la DEC. ¡Eso sí que es honor entre ladrones! Yo tenía también el presentimiento de que jsz estaba de alguna forma implicado en el

ataque contra Ariel en San Diego: probablemente había suministrado las herramientas, o quizá había sido él mismo el director de la operación.

Nos enteramos también de otro hecho importante, pues si bien habíamos visto que los archivos de Eric Allman habían sido robados y almacenados en la Well, ni Andrew ni yo los habíamos examinado para ver qué clase de información contenían. Allman era el autor y responsable del mantenimiento del programa de sendmail, y ahora sabíamos que era probable que jsz hubiera encontrado una descripción detallada de un nuevo fallo de seguridad

mientras leía el correo de Allman después de entrar en *mastodon.cs.berkeley.edu*, el ordenador en el que estaba almacenado.

Mitnick y jsz estaban rastreando sistemáticamente Internet, y parecían apuntar específicamente a los ordenadores de los expertos en seguridad para examinar su correo. Con las técnicas robadas, atacaban luego a los ordenadores de empresas como Apple, Motorola, Oki y Qualcomm.

A las 2:11 p.m., Mitnick conectó desde Denver con *escape.com* a través de Netcom. Desde mi puesto al lado de la máquina de refrescos oí reír a los

otros miembros de nuestro equipo viéndolo copiar un archivo llamado girls.gif a un directorio perteneciente a jsz en escape. A continuación examinó el archivo del correo de Markoff y pasó revista a los encabezamientos por materia, deteniéndose sólo para leer una nota personal que aquél había recibido de un amigo.

Unos minutos más tarde buscó de nuevo a su amigo jsz para una improvisada charla:

```
Mensaje de
        Talk_Daemon@escape.com a
        las 17:20 …
conexión solicitada por
        jsz@ramon.bgu.ac.il
```

```
responda con: ntalk jsz@ramon.bgu.ac.il
martin: hola
jsz:    hola
martin: ¿qué bd estás tramando : -( :-) quiero decir
jsz:    :-) ¡veremos cuando esté hecho! ejecutaré la propia portd.
martin: estoy ansioso; ¿es sexy?
jsz:    sí sí, a dan farmer le encantaría
```

Sí, en vuestros sueños, tal vez. ¿Estos tipos no tendrán otra cosa que hacer?

```
martin: jejeje. ok te dejaré continuar con ello ahora salgo a comer y ocuparme en buscar un verdadero
```

trabajo.
jsz: mándame pizza :) (pero buena) :) ok.
martin: ¿con jamón?
jsz: buena suerte con tu búsqueda.
martin: ¿podrías indicarme algunos buenos libros de lectura sobre sadismo en cajas unix?
jsz: seguro: lee cyberpunk :)
martin: si si si

Daba la impresión de que Mitnick estaba usando *Cyberpunk* como c.v.

martin: trasladé un archivo a escape: —jsz/marty ok
jsz: eh, puedes usar —jsz/.elm/.4_m dir para ti… si quieres…

escribiré pero no leíble, así que tendrás que conocer el camino EXACTO para llegar.

martin: ok los mudaré más tarde

jsz: jejeje. ok.

martin: joderán conmigo por error y no quieren ahuyentarme :-)

jsz: jajajajaja. B-)

martin: ¡o sus teléfonos no tendrán tono de llamada!

jsz: adelante :) naah

martin: ok hablaremos más tarde, puesto que posse jode contigo tal vez yo deba.

jsz: Ok, te llamo más tarde…

martin: adiós

jsz: ¡adiós!

"Unos tipos estupendos", pensé.

“¿Será así como emplean su tiempo siempre que están despiertos?”. Empecé a recordar lo que sabía sobre la Posse, la pandilla que Jim Settle, el ex agente del FBI, creía autora del forzamiento de mis ordenadores. ¿Ante qué nos encontrábamos?: ¿Una guerra a muerte en el submundo cibernético? Mis especulaciones fueron interrumpidas por Robert, que se había levantado de su asiento y permanecía de pie.

“Tengo que dormir un poco, y tú tienes que irte, porque no puedo dejarte aquí”, dijo en tono que no admitía réplica. Robert llevaba en pie más de treinta horas, y las tres de la tarde era la

hora en que el transgresor solía tomarse un descanso. Me aseguró que tenía el busca activado y que si Mitnick volvía nos avisarían. Comprendí que tenía razón, y de todas formas, por primera vez en muchos días me sentía satisfecho con nuestra situación. El sistema de seguimiento estaba ahora funcionando, estábamos bastante seguros de saber quién era nuestro objetivo, y necesitábamos comer y descansar, pues tendríamos que estar preparados para ocuparnos más tarde de Mitnick. De aquí en adelante sería necesario trabajar con el FBI y las compañías telefónicas para ubicar con exactitud su localización

física. Convinimos en volver a reunirnos a las 8 de la tarde.

Una vez en la calle, Julia, Andrew y yo nos encontramos en ese estado como de zombi que sobreviene cuando se abusa de la falta de sueño, pero yo no podía hacer tiempo para dormir, porque había mucho que organizar si queríamos hacer avances esa noche.

Necesitaba hacer llamadas telefónicas, de modo que fuimos a un restaurante Hobie's situado a un par de manzanas de distancia, en un centro comercial. Hobie's es una cadena de comida sana al estilo de California que se especializa en servir desayunos todo

el día. Una vez allí, esparcimos nuestro equipo sobre la mesa. Tratábamos de no llamar la atención, pero con un teléfono móvil, los buscas y una terminal RadioMail resultaba difícil pasar desapercibidos, lo cual nos ponía a todos un tanto paranoicos. A Julia le parecía que las personas que nos rodeaban estaba escuchando nuestra conversación, aunque fingieran no hacerlo.

Finalmente, vino la camarera, echó una ojeada a la mesa cubierta de elementos electrónicos y dijo: "Parece que habéis estado trabajando".

"Y seguimos", contesté.

Le pregunté en qué se diferenciaban dos de las hamburguesas vegetarianas de la carta, y ella se embarcó en una detallada y entretenida disertación técnica sobre la distinción entre la hamburguesa de soja —Soy Burger— y la de la huerta o Garden Burger. Una de ellas venía con queso mozzarella. Sabía mejor, pero contenía más grasas.

La otra especialidad de la casa eran los *smoothies* de fruta, y pedimos uno para cada uno. Cuando los trajo, la camarera nos ofreció cubrirlos de nata montada de bote. Bajo mi punto de vista, eso expone básicamente la verdadera naturaleza del concepto californiano de

restaurante de comida sana. Son saludables, al menos en apariencia, pero en realidad tienden a ser lugares a los que uno puede acudir sin sentirse culpable de consumir comida-basura.

Después del pedido, salí al exterior a llamar a Kent Walker por el teléfono público. Ya había hablado varias veces con él durante el día con respecto a la situación de las autorizaciones para el rastreo y localización de llamadas en Denver.

“Tsutomu, ¿quiere que le dé primero la buena noticia o la mala?”, dijo, en un tono claramente afligido.

“Primero la mala”, repliqué.

“El ayudante del fiscal del estado en Denver llamó al FBI en Los Ángeles y le dijo que no hicieran nada sobre esto”, dijo.

“¿Debo pensar que hemos tropezado con un conflicto de competencia territorial?”, le pregunté.

Kent no respondió a la pregunta, pero no era necesario. “La buena noticia es que tenemos en Raleigh una operación de rastreo y localización que debe haber empezado a las cinco de esta mañana, tiempo del este”.

Contar con una autorización para Raleigh significaba que la próxima vez que Mitnick conectase con la Netcom

desde su POP en Raleigh, la compañía telefónica podría determinar de dónde provenía la llamada.

Yo igual no estaba dispuesto a renunciar a la autorización para Denver.

"¿Pueden realmente hacer esto? ¿No es obstrucción a la justicia o algo semejante?", le pregunté. "La más reciente actividad ha sido desde Denver, y sería importante que también pudiésemos rastrear allí el fin de semana".

"Oiga, Tsutomu, ahora son las cuatro y media en Denver", dijo él, "es casi el final de la jornada".

"Pues tiene todavía un cuarto de

hora", lo presioné, todavía esperanzado.

Tras una larga pausa, él dijo: "Lo intentaré, pero no le prometo nada".

Kent me dio el número del busca Skypager de Levord Burns y me dijo que la próxima vez que tuviésemos una conexión de Raleigh, Burns nos ayudaría a conseguir el rastreo de la misma por la compañía telefónica. Cuando me quejé preguntándole por qué no podía yo acudir directamente a la compañía telefónica me dio los números de teléfono de gente de la compañía, pero me dijo que debía tratar de comunicarme primero con el contacto del FBI.

Le di las gracias y colgué. El hecho

de que el FBI de Los Ángeles hubiera estado más de dos años persiguiendo a Mitnick no era un motivo para que no pudiésemos realizar también nuestra propia investigación. Era una cosa frustrante, pero me alegré de que Kent estuviese con nosotros.

Salimos de Hobie's, y Andrew se fue a recoger algunos efectos, incluida ropa, pues la noche anterior no había tenido tiempo de regresar a casa de Pei a buscar sus pertenencias. Julia y yo cruzamos el aparcamiento del restaurante hacia un campo cubierto de hierba verde mojada y amarillas plantas de mostaza en flor. El terreno estaba

mojado por la lluvia, pero era lo más cerca de la naturaleza que podíamos estar en medio de la expansión de hormigón de los alrededores de San José.

Faltaban aún varias horas para el regreso de Robert, así que nos metimos en el coche de Julia y nos echamos por encima las bolsas de dormir en los asientos delanteros. Al rato llegó Andrew y aparcó junto a nosotros. Dejó el motor de su Jeep +4 en marcha para conservar el calor, reclinó el asiento delantero y se quedó dormido.

Estaba casi oscuro, y al mirar hacia el coche de Andrew vimos que una

buena samaritana se asomaba a la ventanilla, preguntándose si la persona que parecía en estado comatoso, con el motor del coche encendido, necesitaba asistencia. Le aseguramos que se encontraba bien, que había pasado toda la noche levantado y estaba descansando.

Después de comer, Julia parecía haber recobrado energías, pero seguía estando muy tensa. Era casi su hora de partir para el fin de semana, pero no se sentía preparada para enfrentarse con John. Habría sido bastante difícil incluso en circunstancias ideales, pero ahora estaba exhausta y temerosa de no

ser capaz de mantenerse fuerte.

Dado su estado presente, también a mí me ponía nervioso el que ella pasase el fin de semana con John. A aquella altura de la investigación lo que menos deseaba era tener que lidiar con los conflictos de Julia. Me sentía tremendamente presionado y tratar de mantener la operación en funcionamiento era como hacer malabarismos con varias pelotas: una técnica, una legal y una política. Sentía que no era capaz de soportar un aumento del estrés.

Estuvimos un rato hablando de si verdaderamente debía irse el fin de semana. Al final me descubrí

experimentando un desencanto creciente, porque me parecía que Julia estaba intentando tranquilizarme a mí, en lugar de enfrentarse al desasosiego y la confusión en su interior.

"Mira", le dije, "que a mí me preocupe que vayas, es problema mío; pero el que debas ir o no, es algo que debes resolver por ti misma".

Ella lo pensó un momento.

"Tsutomu, estando a esta altura de la investigación, me gustaría llegar hasta el final", dijo.

"No te puedo decir que no va a ocurrir nada durante tu ausencia", repliqué. "No sé lo que va a ocurrir,

sólo sé que si no nos movemos con rapidez corremos el riesgo de perder a nuestro hombre".

"Si me voy ahora, ¿voy a perderme la última partida?", preguntó ella.

"Confío en recibir esta noche de Raleigh información del rastreo, y tan pronto como dispongamos de una pista sólida pienso trasladar nuestra base de operaciones. Si él viene desde Denver, iré en esa dirección; si es de Raleigh, es allí adonde iré".

Le dije que podía intentar ponerse al corriente, pero que no podíamos esperarla.

Ella vacilaba en cuanto a lo que

debía hacer, porque le había hecho una promesa a John y sentía que tenía que mantenerla.

Yo empezaba a sentirme más frustrado aún.

"Tú quieres nadar y guardar la ropa, y eso no es posible", le dije. "En determinado momento vas a tener que tomar una decisión".

Se iba haciendo cada vez más tarde mientras Julia luchaba entre ir o quedarse. Varias veces llamó a John para decirle que iba a retrasarse. Eran las 7:30 de la tarde cuando finalmente decidió partir. Yo salí del Mazda y transferimos mi equipo de esquí al Jeep

+4. Julia dijo que vendría a reunirse conmigo a su regreso, y yo le contesté que podía ponerse al habla con Andrew para dar conmigo.

Yo llevaba casi treinta y dos horas levantado. Andrew y yo volvimos a la Netcom y aguardamos un rato, dormitando, para después subir de nuevo a reanudar la vigilancia.

De nuevo adentro, bajo el suave zumbido incesante de las luces fluorescentes, examinamos los registros y vimos que Mitnick había estado ausente por más de una hora. Su última sesión, que había concluido a las 6:58

p.m., había venido por Denver.

Yo estaba preocupado. Teníamos capacidad para rastrearlo en una sola ciudad entre docenas de posibilidades, y ahora él parecía estarlo evitando. Mi esperanza era que lo que le hacía reconducir sus llamadas fueran únicamente los problemas técnicos que la Netcom estaba teniendo en Raleigh, pero no podía estar seguro de que él no estuviese a su vez rastreándonos a nosotros.

Tenía además los ojos enrojecidos y llorosos por el cansancio, y aunque habría sido un lujo increíble salir y encontrar un hotel donde dormir, yo

sabía que esa noche podía ser nuestra mejor y única ocasión de obtener su rastro. Desde que era muy joven siempre he tenido la capacidad de permanecer despierto por prolongados periodos aislándome y concentrándome en el problema. Pero sentado ese viernes ante mi ordenador tratando de extraerle el sentido a la información que habíamos recogido a lo largo del día comprobé que aquélla era una capacidad que iba perdiendo con la edad.

Mientras estaba allí con Andrew poniendo en orden nuestras herramientas de software y esperando el retorno de Mitnick, me di cuenta de que la

desaparición de Julia me había proporcionado una sensación de alivio. Me sorprendí, pues no había tenido conciencia de lo perturbado que había estado. Ahora tenía la sensación de poder concentrarme finalmente en la cacería. Aunque era viernes por la noche, la actividad en Netcom era más intensa que de costumbre, con un puñado de instaladores recorriendo los despachos para reemplazar los teléfonos en cada escritorio. En un momento dado me levanté y entré en el despacho de Robert y comprobé que sobre su escritorio descansaba una reciente pirámide de latas de Coke. Habíamos

pasado allí mucho tiempo.

Volví a mi puesto a revisar la información que habíamos registrado, cuando a las 10:44 se registró Mitnick. ¡Llamaba desde Raleigh!

"Andrew, ¿por qué no ves si puedes despertar a Levord?". Era el momento de comprobar si el FBI podía llevar a cabo la parte que le correspondía. Levord estaba durmiendo en su casa de Fairfax, Virginia, un barrio de Washington, pero dijo que se ocuparía. Quince minutos después llamó a su vez. Andrew habló brevemente con él y luego asomó la cabeza por la puerta del despacho: "Dice que los tíos de la GTE

le han dicho que el número que les dimos no existe".

Miré mis notas y marqué el número yo mismo. Por el auricular oí el familiar sonido de un modem de alta velocidad, semejante a la llamada de un animal para aparearse a alta velocidad. Entré en el despacho de Robert y cogí el teléfono de manos de Andrew.

"Oiga, a mí me contesta: ¿quiere oír el tono de portadora del modem?", dije, irritado. "¿Qué les pasa a esos idiotas?".

Aquello coincidía con todo lo que yo había oído sobre la GTE. "Vaya suerte", dije para mis adentros. Levord

sonaba como si estuviese más dormido que despierto, pero prometió pedirles que probaran de nuevo.

A diferencia de algunas de las sesiones de Mitnick, ésta fue prolongada, con una duración de casi treinta y cinco minutos.

Poco antes de que Mitnick se desconectara, Levord volvió a llamar y dijo: “Se ha ido, no consiguieron nada”.

“Ya. Bueno, su gente tuvo una media hora”.

Levord no se inmutó. “Si vuelve a aparecer, llámeme”, respondió. Ahora tienen el equipo de rastreo preparado”.

“¡Yo había entendido que iban a

tenerlo hace ocho horas!”, le dije.

“Parece que no estaban enterados de nada”, replicó él.

Fantástico.

Eran las 11:20, pero afortunadamente sólo tuvimos que esperar unos minutos. El busca de Robert volvió a zumbar y, cómo no, Mitnick estaba de regreso como gkremen, otra vez desde Raleigh.

“Vuelve a llamar a Levord y dile que ponga en acción a esos tíos, y que esta vez rastreen el origen de la llamada”, le dije a Andrew.

Hizo la llamada, y de nuevo esperamos.

Treinta minutos más tarde sonó el teléfono.

El agente especial Burns informaba que tenían un rastro: un número telefónico asignado a Centel, una empresa de teléfonos móviles recientemente adquirida por Sprint Cellular. Aparte de eso no nos diría nada más. ¡Pero teníamos un número telefónico, y eso podría conducirnos a una dirección material! Parecía que el FBI había tenido razón: Mitnick estaba efectuando sus llamadas vía teléfono móvil. Levord y yo convinimos en que por la mañana él se pondría al habla con Sprint y arreglaría para rastrear la

llamada a través del conmutador de ellos.

Mitnick estaba todavía rondando los ordenadores de la Netcom. Mientras Robert observaba, Mitnick conectó con uno de los ordenadores servidores de la compañía llamado Netcomsv. Era una máquina que procesaba servicios especiales disponibles para todos los usuarios tales como el sistema de conferencias del ordenador Usenet, y nos encontramos con que había instalado una puerta secreta. Se registró como raíz, utilizó la contraseña ".neill." —seguía obsesionado con Neill Clift—, y se fue después de hurgar un rato. Robert

estaba furioso. Se comunicó por teléfono con John Hoffman y se aseguró de que la puerta trasera fuera clausurada inmediatamente.

Continuamos siguiendo las sesiones de la noche y observamos el desarrollo de un notable ataque. Mitnick había conectado desde Netcom con CSN y se había hecho raíz poco después de las 11:30 p.m. Había estado probando con los archivos de los sistemas operativos de sus ordenadores principales, intentando instalar y ocultar el sistema que le habíamos visto construir la noche anterior. Al cabo de una media hora consiguió con éxito reinstalar NIT y a

continuación reinició el ordenador para que ejecutase su programa. ¡Lo había hecho bajo las propias narices de los administradores de CSN!

Mientras asistíamos a la sesión con nuestro software de seguimiento, Andrew se volvió hacia mí y exclamó: "¡Qué agallas!".

Como administrador de sistemas, Robert no podía creer lo que estaba viendo. "Quiero eso grabado en vídeo", me dijo.

Vigilamos unos minutos más, pero era visible que ninguno de nosotros iba a poder vencer el sueño por más tiempo. Habían transcurrido treinta y nueve

horas desde que me desperté en San Francisco la mañana del jueves, y el cansancio había hecho mella.

Busqué en la guía telefónica y encontré un hostal-residencia próximo. Reservé dos habitaciones, y Andrew y yo recorrimos en coche unos cinco kilómetros a través de las calles desiertas de San José. Eran las tres de la mañana cuando nos registramos y nos fuimos a dormir.

13. Kevin

Lo cierto es que yo había tenido conocimiento de la existencia de Kevin Mitnick mucho antes de que las huellas d e *oki.tar.Z* en Ariel lo hicieran sospechoso del ataque contra mí. A lo largo de un periodo de quince años que arrancaba allá por 1980 había adquirido un carácter de leyenda en el mundillo informático, habiendo tenido numerosos conflictos con las autoridades locales, estatales y federales, que en diversas

ocasiones lo metieron en la cárcel.

Mi primer choque con él tuvo lugar durante el verano de 1991, cuando intentó sonsacarme por teléfono información sobre seguridad informática, so pretexto de una emergencia. Se trata de una táctica empleada por elementos de este ámbito para acceder a un ordenador, y consiste en inducir a un desprevenido administrador de sistemas o funcionario de una compañía telefónica a proporcionar determinada información valiosa. Confían en el deseo de ayudar por parte de la gente. Cuando llama alguien diciendo que es un empleado

nuevo de la compañía, o uno de otro departamento que ha colocado mal una contraseña, o alguien que legítimamente necesita acceder temporalmente a un ordenador, la reacción natural de una persona es proporcionarle la información.

La llamada de Kevin llegó unos meses después de haber descubierto yo un fallo de seguridad bastante flagrante en el sistema operativo ULTRIX de la Digital Equipment Corporation. Cualquiera podía hacerse raíz en una estación de trabajo DEC enviando al ordenador un mensaje de correo electrónico a una dirección clave y

tecleando luego unas pocas instrucciones. Este fallo era lo que los diseñadores de software denominan "atoramiento de buffer", y el programa "virus"[36] de Robert Tappan Morris explotó un fallo similar en un servicio de red suministrado con el sistema operativo UNIX. El software estaba esperando una cadena de caracteres de no más de una determinada extensión, y al recibir una más larga, se podía conseguir que el programa reaccionara alterando su comportamiento de una forma especialmente aviesa y extraña, cuya consecuencia era la de otorgar al usuario todos los privilegios del

sistema.

Yo describí el fallo en un mensaje al CERT. En principio, se supone que el CERT está para servir de cámara de compensación para la información sobre puntos vulnerables en los ordenadores, de modo que los responsables de administrar redes puedan enterarse y subsanarlos antes de que lleguen a oídas del mundo informático. La realidad es que en lugar de hacer tal información libremente disponible para que los fallos de seguridad sean subsanados, el CERT ha intentado más bien restringir su difusión lo más posible. Jamás publicará los nombres de organizaciones

que hayan sufrido un ataque, con el argumento de que ésa es la única forma de poder conseguir cooperación. Tiende asimismo a producir comunicados tan genéricos que no resultan muy útiles.

Pocos meses después de haber informado yo del fallo en ULTRIX, el CERT emitió un comunicado que lo describía de una forma tan pasteurizada que el informe no brindaba los datos suficientes para que alguien pudiera reproducir el error. Para entonces, Brosl y yo nos habíamos trasladado de Los Álamos a San Diego, pero yo había hecho el vuelo de regreso a Los Álamos para pasar una semana en el Centro de

Estudios No-lineales. Una mañana mi secretaria en San Diego me comentó que estaba recibiendo reiteradas llamadas telefónicas de alguien de Sun Microsystems que quería hablar urgentemente conmigo. Varias horas después me encontraba instalado en un despacho prestado, cuando sonó el teléfono.

"Hola, soy Brian Reid. Soy especialista de campo de la Sun Microsoft en Las Vegas". Hablaba con soltura y rapidez. Me dijo que había visto el comunicado del CERT, que se encontraba en la sede de un cliente y que necesitaba más información. "No puedo

recrear el fallo", explicó.

Me puse en guardia de inmediato. Yo conocía de oídas a un Brian Reid, pero que trabajaba en la DEC, no en la Sun. Aquello no tenía sentido. En primer lugar, ¿por qué alguien de Sun Microsystems, en la sede de un cliente, iba a estar tan ansioso por obtener información técnica sobre un fallo de seguridad en uno de los ordenadores de la competencia?

"¿Cómo puedo verificar quién es usted?, pregunté.

"No hay problema", replicó él. "Llame usted a este número en la Sun y le confirmarán que trabajo para ellos".

Me dio el número de la Sun, así como un número con el prefijo de zona 702 para comunicarme con él, y colgó. Llamé a mi amigo Jimmy McClary, un funcionario de Computer Systems Security en el Laboratorio Nacional de Los Álamos, y le comenté la llamada. Él bajó y se sentó a mi lado mientras yo marcaba el número de Sun que me había dado el de la primera llamada. Le pregunté a la operadora por un empleado llamado Brian Reid, y ella me dijo que no había tal persona trabajando para la Sun. Colgué, y estaba charlando con Jimmy sobre qué hacer con la llamada cuando mi teléfono sonó de

nuevo.

Esta vez una voz que sonaba mucho menos profesional se identificó como un compañero de trabajo de Brian Reid en la Sun, y dijo que él también estaba interesado en la información que el señor Reid había solicitado.

"¿Por qué no me deja su dirección y se la pongo por correo en un disco flexible?", le sugerí. Aquello pareció sorprender a mi segundo interlocutor, que se puso a emitir "humms" y "aahs". Finalmente, salió con una dirección que tenía todo el aspecto de haber sido inventada en el momento, y colgó rápidamente.

Probé con el número del prefijo 702 que me había dado el primero, y me dio el silbido de un modem de ordenador. El prefijo 702 corresponde al estado de Nevada, de modo que le di el número y la dirección a Jimmy, que fue a telefonear a los funcionarios de seguridad del Departamento de Energía. Más tarde me enteré de que ellos habían localizado el número como de un teléfono público en el *campus* de la Universidad de Nevada en Las Vegas. Algunos de esos teléfonos no pueden recibir llamadas, pero tienen en cambio un modem para comunicar información y diagnósticos a cargar en cuenta.

Varias semanas después estaba hablando con Markoff, y cuando empecé a contarle lo de la llamada de alguien que decía ser Brian Reid, él se puso a reír.

"¿De qué te ríes?", le pregunté.

"Sólo existe una persona capaz de utilizar el nombre de Brian Reid al tratar de sonsacarte información", replicó.

Markoff, que había estado investigando a Kevin Mitnick para su libro titulado *Cyberpunk*, me explicó que en 1987 y 1988 Kevin y un amigo, Lenny Di Cicco, habían librado una batalla campal electrónica contra el verdadero Brian Reid, un científico del

laboratorio de investigación de la DEC en Palo Alto. Mitnick se había obsesionado por conseguir una copia del código fuente del sistema operativo del miniordenador VMS de la DEC, y estaba tratando de hacerlo logrando la entrada en la red informática de la empresa, conocida por Easynet. Los ordenadores del laboratorio parecían los más vulnerables, de modo que todas las noches, con notable persistencia, Mitnick y Di Cicco lanzaban sus ataques de modem desde una pequeña empresa en Calabasas, California, en la que el segundo trabajaba como técnico de ordenadores. Aunque Reid descubrió los

ataques casi inmediatamente, no supo de dónde venían, y tampoco la policía local ni el FBI, porque Mitnick manipulaba las centrales de la red telefónica para disfrazar la fuente de las llamadas de modem.

El FBI puede fácilmente emitir mandamientos y obtener información de las compañías telefónicas relativa a rastreo y localización, pero son pocos sus agentes capaces de interpretar los datos obtenidos. Si el delincuente reside efectivamente en la dirección que corresponde al número telefónico, estupendo. Pero si se ha introducido electrónicamente en la central de la

compañía telefónica y ha mezclado las tablas de dirección, están perdidos. Utilizando interceptores y trazadoras, Kevin había frustrado con facilidad los mejores intentos de seguirle el rastro a través de la red telefónica. Empleaba habitualmente dos terminales de ordenador cada noche, una para sus incursiones por los ordenadores de la DEC, la otra como centinela para explorar los de la compañía telefónica para ver si sus perseguidores se aproximaban. Una vez, un equipo de agentes y de la seguridad de la telefónica creyeron haberlo localizado, pero se encontraron con que Mitnick

había desviado las líneas y los había conducido, no a su escondite en Calabasas, sino a un apartamento en Malibú.

Mitnick era, al parecer, un cómplice indeseable, pues por más que hubieran trabajando juntos en un tiempo, había estado acosando a Di Cicco mediante llamadas falsas al patrón de este último, haciéndose pasar por un agente gubernamental y diciendo que Di Cicco tenía problemas con sus impuestos. El frustrado Di Cicco confesó ante su patrón, quien a su vez lo notificó a la DEC y al FBI, y Mitnick pronto acabó en el juzgado federal de Los Ángeles.

Aunque la DEC lo acusaba de haber robado software por valor de varios millones de dólares y haberle costado cerca de 200.000 más en tiempo invertido en procurar mantenerlo fuera de sus ordenadores, Kevin se declaró culpable de un cargo de fraude informático y uno de posesión ilegal de códigos de acceso a larga distancia.

Era la quinta vez que Mitnick era aprehendido por un delito informático y el caso despertó atención en todo el país porque, en sus descargos, propuso pasar un año en prisión y seis meses en un centro de rehabilitación para curarse de su adicción a los ordenadores. Era una

extraña táctica de defensa, pero un juez federal, tras oponerse de entrada, aceptó la idea de que existía un cierto paralelismo psicológico entre la obsesión de Mitnick por forzar su entrada en sistemas informáticos y la compulsión de un adicto por las drogas.

Kevin David Mitnick alcanzó la adolescencia en la zona suburbana de Los Angeles a finales de los años setenta, la misma época en que la industria de los ordenadores personales se expandía más allá de sus orígenes de objeto de aficionados. Sus padres estaban divorciados, y en un ambiente

de clase media baja en el que él era en buena medida un solitario y un mediocre, quedó seducido por el poder que era capaz de lograr sobre la red telefónica. La subcultura de los adictos al teléfono llevaba más de una década de florecimiento, pero estaba ahora en medio de la transición del mundo analógico al universo digital. Utilizando un ordenador personal y un modem resultaba posible apoderarse del conmutador de la oficina digital central de una compañía telefónica conectando a distancia la entrada, y Mitnick se aficionó a hacerlo. El dominio del conmutador de una compañía telefónica

local ofrecía más que simplemente llamadas gratuitas: abría una ventana para entrar en las vidas de otra gente; para fisgonear a los ricos y poderosos, o a sus propios enemigos.

Mitnick pronto se incorporó a una pandilla de viciosos del teléfono que se reunían en una pizzería de Hollywood. Buena parte de lo que hacían caía en la categoría de travesuras, como suplantar al servicio de información de la guía y responder a llamadas diciendo "Sí, el número es ocho-siete-cinco-cero y medio. ¿Sabe cómo se marca el medio, señora?"; o cambiando el tipo de servicio del teléfono de una casa

privada por el de un teléfono público, con lo cual cada vez que el abonado levantaba el auricular, una voz grabada le pedía que depositase veinte céntimos. Pero al parecer el grupo tenía también una veta dañina. Uno de sus miembros destruyó archivos de una compañía de ordenadores a tiempo compartido con sede en San Francisco, un delito que permaneció sin resolver durante más de un año, hasta que un ataque en un centro de conmutadores de una compañía telefónica de Los Ángeles guió a la policía hasta la pandilla.

Ese forzamiento ocurrió durante el fin de semana del Memorial Day[37] en

1981, cuando Mitnick y dos amigos resolvieron entrar físicamente en la central telefónica COSMOS de la Bell, en Los Ángeles. COSMOS, o Computer System for Mainframe Operations, era una base de datos utilizada por muchas de las empresas telefónicas del país para controlar las funciones básicas de conservación de registros del sistema telefónico. El grupo logró con argucias superar el control de seguridad y finalmente dio con el recinto donde se hallaba el sistema COSMOS. Una vez dentro, cogieron listas de contraseñas de ordenadores, incluyendo las combinaciones de las cerraduras de las

puertas de acceso de nueve oficinas centrales de la Pacific Bell, y una serie de manuales de operador para el sistema COSMOS. Para facilitar ulteriores actividades del grupo, "plantaron" nombres falsos y números telefónicos en un fichero rotatorio que encontraron encima de uno de los escritorios del recinto. En un alarde final, uno de los nombres falsos fue el de "John Draper", que era el de un programador de ordenadores real, también conocido como el Capitán Crunch, legendario fanático del teléfono. Los números de teléfono eran en realidad números desviados para sonar en un teléfono

público de una cafetería en Van Nuys.

Pero el delito no fue perfecto. El gerente de una empresa telefónica pronto descubrió los números falsos e informó de los mismos a la policía local, que inició una investigación. El caso fue efectivamente resuelto cuando la amiguita despechada de uno de los miembros de la pandilla acudió a la policía y Mitnick y sus amigos fueron a parar a la cárcel, siendo acusados de destruir información en una red informática y de robar manuales de operador de la compañía telefónica. Mitnick, que tenía por entonces diecisiete años, fue relativamente

afortunado, y fue condenado a sólo tres meses de estancia en el Centro de Detención para Jóvenes, de Los Ángeles, más un año de libertad condicional.

Puede que un encontronazo con la policía hubiera persuadido a la mayoría de los chicos despiertos a explorar las numerosas formas legales de correr aventuras informáticas, pero Mitnick parecía obsesionado por una visión distorsionada de los hechos. En lugar de desarrollar sus habilidades informáticas de un modo creativo y productivo, pareció interesarse únicamente en aprender bastantes métodos expeditivos

para forzar su entrada en un ordenador y jugarretas para continuar representando una fantasía que lo condujo a tener choque tras choque con la policía a lo largo de los años ochenta. Era obvio que le encantaban la atención y la mística producidas por su creciente notoriedad. Muy pronto, después de ver la película de Robert Redford de 1975 *Los tres días del Cóndor*, había adoptado "Cóndor" como *nom de guerre*. En la película, Redford desempeña el papel de un fugitivo investigador de la CIA que utiliza su experiencia en el Cuerpo de Señales del Ejército para manipular el sistema telefónico y evitar su captura.

Al parecer, Mitnick se veía a sí mismo como la misma clase de individuo audaz huyendo de la ley.

Su siguiente detención ocurrió en 1983 y la realizó la policía del *campus* de la Universidad de California Meridional, donde había tenido problemas menores unos años antes, cuando lo pescaron utilizando un ordenador de la universidad para acceder ilegalmente a la red ARPAnet. Esa vez lo descubrieron sentado ante un ordenador en una sala de terminales del *campus*, forzando su entrada en un ordenador del Pentágono, y fue condenado a seis meses en una prisión

para delincuentes juveniles en Stockton, California. Tras ser puesto en libertad, consiguió una placa de matrícula "X HACKER" para su Nissan, pero siguió muy metido en la actividad de forzar ordenadores. Varios años después estuvo más de un año escondido, acusado de uso indebido de un ordenador TRW de referencias de créditos; hubo una orden de detención, que más tarde desapareció inexplicablemente de los registros policiales.

Hacia 1987 pareció que Mitnick estaba haciendo un esfuerzo por enderezar su vida, y empezó a vivir con

una mujer a la que daba clases de informática en una escuela profesional local. Pero al cabo de un tiempo su obsesión volvió a poseerlo, y esta vez su uso ilegal de números de tarjetas de crédito telefónicas condujo a los detectives al apartamento que compartía con su amiguita en Thousand Oaks, California. Fue acusado de robo de software a la Santa Cruz Operation, una empresa californiana, y en diciembre de 1987 lo condenaron a treinta y seis meses de libertad vigilada. Esta escaramuza con la ley y el ligero castigo consiguiente no parecieron sino acrecentar en él la sensación de

omnipotencia.

En el verano de 1988 Markoff consiguió, a través de un adolescente hacker, copia de un memorándum confidencial de la Pacific Bell. La compañía telefónica no tenía idea de cómo se había filtrado, pero confirmó su autenticidad. El memorándum, escrito el año anterior, concluía que "el número de individuos capaces de entrar en los sistemas operativos de la Pacific Bell va en aumento" y que "los ataques de los hackers se están volviendo más sofisticados". En consecuencia, reconocía el documento, los usuarios de ordenadores personales podían conectar

ilegalmente sus máquinas con la red telefónica y mediante las órdenes adecuadas fisgonear, añadir llamadas a las facturas de cualquiera, alterar o destruir información, interceptar documentos facsímiles en proceso de trasmisión, hacer que todas las llamadas a un determinado número fueran desviadas automáticamente a otro, o hacer que una determinada línea pareciese permanentemente ocupada. En uno de los casos citados, un grupo de adolescentes aficionados al ordenador consiguió hacer algo tan tonto como "controlar recíprocamente sus líneas por diversión" o tan irresponsable como

“apoderarse del tono de llamada de un abonado y hacer aparecer llamadas en su cuenta”. Uno de los piratas usaba sus conocimientos para desconectar y ocupar los servicios telefónicos de personas que no le gustaban. Además, “añadía diversos servicios adicionales a la línea, para inflar las facturas”.

El memorándum filtrado fue descrito en un artículo de primera plana del *New York Times* escrito por Markoff y Andrew Pollack. Aunque entonces no lo sabía, Markoff se enteró después que la fuente del documento había sido Mitnick. Éste, cuyo instrumental técnico incluía la radio amateur, se había

enterado del memorándum a través de un colega radioaficionado. Mediante una llamada a la secretaria de su autor, un ejecutivo de seguridad de la compañía telefónica, se hizo pasar por otro ejecutivo de la Pacific Bell y le pidió que le enviara por fax una copia del documento. Lo que la secretaria no sabía era que Mitnick había desviado el número telefónico, con lo que la comunicación, en vez de ser recibida por un fax de la Pacific Bell, no tardó en salir por uno en la oficina de un amigo suyo. El amigo había incluso programado la máquina para que la secretaria recibiese la confirmación de

que el documento había llegado al número de fax correcto.

Aunque la prensa de California del Sur pronto estaría refiriéndose a Mitnick como el "Hacker del Lado Oscuro" y el "John Dillinger del hampa informática", en realidad él era más un estafador o un timador que un hacker en el verdadero sentido de la palabra. Antes de la película de 1983 *Juegos de guerra*, en la que Matthew Broderick retrataba a un joven con algunos de los rasgos de Kevin Mitnick, la palabra "hacker" se había empleado para referirse a una cultura informática surgida en el MIT a finales de los años cincuenta. Dicha

cultura estuvo mayoritariamente formada por jóvenes obsesionados por los sistemas complejos como un fin en sí mismos, una cultura que se basaba en el principio de compartir liberalmente con los amigos los diseños de software y hardware, y en el de crear ingeniosos "hacks" o programas creativos que hicieran avanzar la informática.

Los verdaderos hackers eran gente como Richard Stallman, que siendo estudiante en el MIT escribió durante los años setenta EMACS, una herramienta de edición para programadores. EMACS proporcionó a los programadores la forma de revisar

reiteradamente los programas para aproximarlos a una condición perfecta, y versiones del mismo son todavía utilizadas ampliamente por muchos, si no por la mayoría, de los mejores programadores actuales de la nación. Pero después de que *Juegos de guerra* se convirtiese en un exitazo, en 1983, se popularizó la definición de "hacker" como un adolescente con un modem y la audacia suficiente como para meterse en un ordenador del Pentágono. Desde entonces la verdadera comunidad *hacker* ha intentado reivindicar el espíritu y el sentido original de la palabra, pero sin ningún éxito. Un

incidente especialmente desalentador ocurrió en 1987, cuando una pequeña reunión anual de la Hacker's Conference invitó a un equipo de periodistas de la CBS a asistir a sus deliberaciones en las colinas que dan a Silicon Valley. La conferencia es un acontecimiento de perfil bajo, y tal vez la única convención de profesionales que ofrece a los asistentes una segunda comida completa, a medianoche, para respetar los hábitos nocturnos de los hackers. Lamentablemente, el reportero de la CBS no era partidario de que la verdad terrenal se atravesara en el camino de una buena historia. Inició su emisión con

la alarmista advertencia de que había visitado el campamento de una guerrilla resuelta a socavar la seguridad del país con un nuevo tipo de guerra de la información.

El mundo que describía poco tenía que ver con los verdaderos hacker, pero empezaba a existir para un creciente número de personas como Kevin Mitnick.

Después de cumplir el periodo de prisión y el de libertad vigilada impuestos por la sentencia de 1989 por el caso de la DEC, Mitnick se trasladó a Las Vegas y cogió un discreto empleo de

programador de ordenadores para una empresa de ventas por correo. Su madre se había mudado allí, lo mismo que una mujer que se hacía llamar Susan Thunder, que había formado parte de la pandilla de Mitnick a principios de los ochenta y con la que ahora volvió a relacionarse. Fue durante este periodo cuando intentó sonsacarme por teléfono.

A comienzos de 1992 Mitnick regresó al valle de San Fernando tras la muerte, al parecer por sobredosis de heroína, de su medio hermano. Trabajó durante poco tiempo con su padre en la construcción, pero luego, a través de un amigo de éste, encontró un empleo en la

Tec Tel Detective Agency. Al poco tiempo de empezar a trabajar allí se descubrió que alguien estaba utilizando ilegalmente una base de datos comercial en nombre de la agencia, y Kevin fue objeto una vez más de una investigación por parte del FBI. En septiembre, el Bureau registró su apartamento, así como la casa y el lugar de trabajo de otro miembro de la pandilla original. Dos meses después un juez federal emitió una orden de detención contra Mitnick por violación de los términos de su libertad condicional de 1989. Los cargos fueron dos: acceso ilegal al ordenador de una empresa telefónica y

asociación con una de las personas junto a las cuales había sido detenido en 1981. Sus amigos aseguraron que la agencia de detectives lo había hecho aparecer como culpable; sea cual fuese la verdad, cuando el FBI fue a detenerlo, Kevin Mitnick se había esfumado.

A finales de 1992 alguien llamó a la oficina del Departamento de Vehículos a Motor, en Sacramento, y utilizando un código de solicitante de aplicación de la ley legítimo intentó conseguir que las fotografías del carné de conducir de un informador de la policía le fueran enviadas por fax a un número en Studio City, cerca de Los Ángeles. Como

aquello olía a fraude, los funcionarios de seguridad de la DVM comprobaron el número y descubrieron que correspondía a un local de fotocopias, sobre el que establecieron vigilancia antes de enviar las fotografías por fax. Por alguna razón, los vigilantes no vieron a su presa hasta que iba saliendo por la puerta de la tienda. Le persiguieron, pero él fue más veloz atravesando el aparcamiento y desapareció por una esquina, dejando caer los documentos en la carrera. Más tarde los agentes precisaron que los papeles estaban cubiertos de huellas digitales de Kevin Mitnick. Su huida, de

la que inmediatamente informaron los periódicos, dejó a los agentes de la ley como unos chapuceros incapaces de estar a la altura de un brillante y escurridizo cyberladrón.

La desaparición de Mitnick puso a los agentes del FBI ante una serie de callejones sin salida. Durante su periodo de prófugo, Mitnick utilizó sus habilidades de manipulador social para reanudar el acoso a Neill Clift, un investigador informático británico a quien había robado información mientras se batía con la DEC, unos años antes. En 1987 uno de los más ricos tesoros a disposición de Mitnick había

consistido en la lectura del correo electrónico de los expertos en seguridad de la DEC. Allí había encontrado mensajes privados que detallaban fallos de seguridad descubiertos en el sistema operativo VMS de la compañía. Clift, que exploraba las debilidades del sistema como una especie de *hobby*, informaba a la DEC de sus hallazgos para que la compañía pudiera solucionar los problemas.

Mitnick empezó una vez más a forzar su entrada en ordenadores usados por Clift. En una serie de prolongadas llamadas internacionales, Mitnick, que posee el talento de un actor para

modificar la voz, convenció a Clift de que era un empleado de la DEC interesado en obtener detalles de nuevos fallos de seguridad que Clift había descubierto en la última versión del sistema VMS. A solicitud de Clift, Mitnick le suministró manuales técnicos de la DEC que él creía que sólo podían provenir directamente de la compañía. Los dos hombres convinieron entonces en iniciar un intercambio de datos, codificándolos con PGP. Clift le envió a Mitnick una detallada relación de los fallos de seguridad encontrados últimamente, pero en una conversación telefónica posterior le entró la

desconfianza y se dio cuenta de que lo habían timado. Sin interrumpir el vínculo con Mitnick, Clift se puso en contacto con el FBI, que estuvo varias semanas intentando rastrear las llamadas, sin resultado. Fue aproximadamente por entonces cuando la Oficina de Delitos Económicos de Finlandia se dirigió a Clift, sospechando que Mitnick había robado software del código fuente de Nokia, una compañía finlandesa de teléfonos móviles que tenía una factoría en California.

Habiendo recibido una misteriosa llamada telefónica solicitando un manual técnico de Nokia, la compañía lo envió

por correo a la dirección indicada, un motel en California, pero alertó al FBI. Los agentes rodearon el motel, con el único resultado de encontrar que alguien había llamado a la recepción y se había hecho enviar el paquete a un segundo motel, desactivando así la trampa. Varias semanas después Mitnick descubrió de algún modo los intentos de rastreo telefónico del FBI, e indignado telefoneó a Clift llamándole "delator", tras lo cual volvió a desaparecer.

En marzo de 1994, el FBI se puso públicamente en ridículo al presentarse en una reunión de defensores de los derechos civiles y la libertad

informática que participaba en una conferencia anual y detener a un infortunado asistente cuyo único delito fue el error de registrarse bajo uno de los alias de Mitnick. Lo prendieron en paños menores en su habitación del hotel, y aunque él y sus compañeros de cuarto protestaron afirmando que no era Mitnick, lo esposaron y se lo llevaron a la oficina local del FBI. Le tomaron las huellas digitales, y al cabo de media hora recibieron la comprobación de que no eran del fugitivo. Tuvieron que llevarlo de vuelta al hotel y disculparse reiteradamente.

Más o menos por la misma época,

Markoff recibía una llamada de Qualcomm, una firma de San Diego que estaba desarrollando una nueva tecnología digital en telefonía móvil conocida por CDMA. Esta tecnología es especialmente valiosa porque permite a los proveedores de servicios de telefonía móvil empaquetar muchas veces el número de llamadas en el mismo espacio del espectro de radio frecuencia. Qualcomm estaba en vías de instalar en San Diego una planta industrial conjunta con la Sony para fabricar los nuevos teléfonos digitales manuales con empleo de tecnología CDMA.

Los ejecutivos de Qualcomm habían leído *Cyberpunk*, en cuyo primer tercio se detallan las hazañas de Mitnick hasta su detención en 1988, y querían saber si Markoff poseía alguna información que les sirviese para confirmar lo que ellos creían: que Mitnick estaba detrás de un reciente y bien ejecutado forzamiento informático durante el cual alguien había robado copias del software que controlaba los teléfonos móviles Qualcomm.

El robo se había iniciado con una serie de llamadas telefónicas a funcionarios técnicos nuevos por parte de alguien que se presentaba como un

ingeniero de la Qualcomm perteneciente a otro grupo. Estaba de viaje, decía, y necesitaba acceder a un determinado servidor pero había olvidado llevarse las contraseñas. Deseosos de ser útiles, los nuevos empleados le complacían con mucho gusto. Con las contraseñas en la mano, el otro sólo tenía que acceder a uno de los ordenadores del sistema de la Qualcomm, que estaban conectados a Internet, y descargar el código fuente de los nuevos teléfonos. Cuando descubrieron que su seguridad había sido violada, los directivos de la Qualcomm notificaron al FBI, que los remitió a su oficina de Los Ángeles. Un

grupo de agentes de ésta estaba ya investigando un caso de robo de software de telefonía móvil que afectaba a más de media docena de empresas, incluyendo a Motorola y Nokia. Los agentes del FBI se presentaron en la Qualcomm, anotaron las pruebas en sus libretas de apuntes y se fueron. Transcurrieron unas semanas, y nada pasó. Los directivos de la Qualcomm llamaron reiteradamente preguntando si se estaban registrando progresos en el caso, pero encontraron al FBI reacio a decirles nada sobre la investigación o el sospechoso. "Lean *Cyberpunk*", decían.

Los de Qualcomm, cada vez más

frustrados, intentaron averiguar por su cuenta algo más acerca del forzamiento. ¿Cómo había podido el intruso identificar sistemáticamente a los nuevos empleados, probablemente los más susceptibles de entregar sin querer los secretos de la compañía? Llegaron a la conclusión de que alguien se había infiltrado en el edificio y se había llevado un ejemplar del boletín interno mensual, que normalmente contenía nombres, fotos y breves biografías de los nuevos empleados.

En la Qualcomm había predominado desde siempre entre los técnicos una cultura basada en la confianza mutua y

en un compartido espíritu de equipo, pero el robo hizo sentir a los ejecutivos que la empresa estaba sometida a asedio y creó una atmósfera paranoica en su interior. En un momento dado, con la esperanza quizá de encontrar un empleado con quien "charlar", alguien llamó sucesivamente a todos los teléfonos de una determinada zona de trabajo, y se vio a varios nerviosos ingenieros de la Qualcomm ponerse de pie y escuchar a medida que los aparatos sonaban uno tras otro.

Los ingenieros de la Qualcomm no tenían claro qué se proponía hacer el ladrón con el software. La simple

posesión del mismo, incluyendo el código fuente, no permitiría a quien quisiera manipular la nueva red digital conseguir llamadas gratuitas ni reproducir números telefónicos existentes, como hubiera sido posible con la anterior tecnología analógica. Se podía pensar, le comentaron a Markoff los directivos de la Qualcomm, en la posibilidad de venderle el software, tal vez en Asia, a algún falsificador del mercado negro que quisiera hacer copias baratas del teléfono de ellos, pero eso no parecía justificar el esfuerzo. No obstante, según el FBI, alguien se estaba tomando un montón de

trabajo para robar software de todos los principales fabricantes de teléfonos móviles. ¿Por qué?, era la pregunta que se hacían.

Exceptuando el breve incidente de 1991, nada de esto me afectó directamente hasta octubre de 1994, cuando a Mark Lottor le robaron del ordenador parte del software de su teléfono móvil Oki. Él me advirtió que estuviese en guardia, y efectivamente, varios días después Andrew empezó a ver sondeos en Ariel. En un momento dado, alguien se puso a explorar electrónicamente los accesos de red a nuestros sistemas. Andrew vio que, en

su esfuerzo por entrar en nuestras máquinas, el intruso repasaba archiconocidas brechas en la seguridad de las redes. Para repeler al invasor, Andrew empezó a clausurar diversas rutas potenciales de acceso en respuesta a los ataques. Una noche los sondeos continuaron hasta cerca de medianoche. Evidentemente, alguien estaba interesado en nuestros ordenadores, y por lo que nos había contado Mark, después supusimos que podría ser Kevin Mitnick. De una en una, las piezas del rompecabezas habían ido lentamente cayendo en su lugar. Por las transcripciones que habíamos visto en la

Netcom, comprendí que Mitnick tenía conciencia de mi existencia; y aunque él no lo supiera aún, ahora yo le seguía el rastro.

14. "Alcance táctico nuclear"

En cierto momento de la mañana del domingo me despertó el pitido de mi busca. En la oscuridad de la habitación del hotel estiré el brazo para cogerlo, y mirando la pantalla vi que el número era el de John Markoff.

"¿Qué pasó anoche?", preguntó él cuando hube cogido a ciegas el teléfono y marcado su número.

“Conseguimos una pista. Hay un número de teléfono. Creo que deberías venir a ver algo de esto. Tenemos la transcripción de una conversación que él sostenía con alguien en Israel, y hablaban de ti. Quiero que la veas”.

“¿Él dónde está?”.

“Los indicios sugieren que en Raleigh, Carolina del Norte”.

“¿Y tú?”.

Era una buena pregunta. Le dije que estaba en un Residence Inn, en alguna parte de San José. Encendí la luz y le leí la dirección. Él dijo que cogería el coche y se reuniría conmigo al cabo de una hora.

Colgué, giré hacia el otro lado y me volví a dormir. Cuarenta y cinco minutos después salí de la cama y me puse de pie bajo la ducha, tratando de despejarme y preparar mi estrategia para la jornada. Un número telefónico era una buena pista y nos daba un punto de partida. Pero tampoco era más que eso, una solitaria pista. Sabiendo que nuestro adversario era Kevin Mitnick, yo era consciente de que un número telefónico en sí mismo tenía un valor limitado. Sospechaba que Mitnick podía haber tratado de enmascarar su ubicación electrónicamente, manipulando el equipo de conmutación

de la compañía telefónica para que los intentos de rastreo proporcionaran una información falsa. En 1988, cuando unos agentes estatales y del FBI habían tratado de localizarlo en California, sus propios esfuerzos de rastreo telefónico los habían confundido por completo. Un número que se suponía era de Mitnick condujo al allanamiento de un apartamento en California del Sur, donde los investigadores de la telefónica encontraron a un cocinero inmigrante viendo la televisión en paños menores.

En el cine uno consigue un rastro telefónico y a partir de éste una

dirección y ya está. Pero en la vida real, el rastreo por una red telefónica es un proceso mucho más sutil y menos predecible. Poner una llamada es como dar instrucciones a alguien para encontrar una dirección determinada: ve por esa calle tres manzanas, luego tuerce a la derecha, etc. Rastrear una, en cambio, es como seguir las instrucciones pero a la inversa, y puede resultar un ejercicio frustrante. Mientras estaba bajo la ducha, supe que no podía estar seguro de que Kevin estuviese en Raleigh: el rastreo podía ser erróneo, o la llamada podría estar simplemente pasando a través del conmutador de la

compañía de telefonía móvil procedente de alguna otra parte.

La última detención de Mitnick, en 1988, ocurrió sólo porque su socio Di Cicco confesó ante un investigador de la DEC. Yo le había oído decir a gente del mundillo informático que la lección que Mitnick sacó de aquel incidente fue que en el futuro operaría en solitario, minimizando la posibilidad de ser traicionado.

Por el seguimiento de la semana pasada podría asegurar que seguía siendo sumamente engreído, un poquitín descuidado y una criatura de costumbres. Y por lo que hasta el

momento yo había visto, no me parecía que fuese un hacker tan brillante como proclamaba la leyenda.

Sin saberlo, él había cometido el mismo error que el señor Slippery, el protagonista de *True Names*[38], el estupendo clásico de 1987 sobre el cyberespacio, de Vernon Vinge: había desvelado accidentalmente su identidad. En su novela, Vinge describe un mundo virtual de poderosos ordenadores y redes veloces muy semejante a éste en el cual yo perseguía a Mitnick. Y la primera regla de ese mundo era mantener en secreto tu nombre verdadero (de ahí el título) en el mundo

real.

Aunque se esforzaba por permanecer inencontrable introduciéndose en la red de la Netcom desde diferentes ciudades, se había vuelto perezoso, y su reiterado uso del POP de Raleigh era una señal de que estaba por creer que podía operar con impunidad. Por supuesto me daba cuenta de que el engreído podía ser yo. Era posible que para protegerse él hubiera hecho algo suficientemente complicado como para no tener que preocuparse. Mi corazonada era que estaba apostando a que las compañías de telefonía móvil estarían más inquietas por el coste del fraude —el tiempo

robado en llamadas a larga distancia—que por las llamadas fraudulentas locales. Jugaba a que si él mantenía un uso discreto y hacía sólo unas pocas llamadas de larga distancia, evitaría llamarles la atención.

Me senté en la cama ante mi terminal RadioMail a leer mi correo electrónico del día anterior. Un mensaje me saltó inmediatamente a los ojos: otra solicitud de David Bank, el reportero del *Mercury News* de San José. En los últimos días había recibido de él numerosas llamadas por el busca, y no había hecho caso. Era evidente que él no iba a renunciar a su historia.

De: Dbank@aol.com
Recibido: por mail02.mail.aol.com
(1.38.193.5/16.2) id AA22563; Fri, 10 Feb 1995 21:35:42 -0500
Fecha: Fri, 10 Feb 1995 21:35:42 -0500
Mensaje-Id: {950210213540_18414375@aol.com}
A: tsutomu@ariel.sdsc.edu
Asunto: SJ Merc News preguntas
Status: RO

Saludos. Lamento no hayamos llegado a conectar el jueves o el viernes. Sigo interesado en reunirme con usted personalmente y puedo ir a San Diego si le es más conveniente.

El quid del asunto es que hay una cantidad de personas que tuvieron motivos suficientes para forzar la entrada en su ordenador. Resulta que una de ellas es usted. No intento faltarle al respeto, pero es necesario que hablemos.

Le ruego que me llame a casa el sábado o me deje un mensaje en el trabajo, para ponernos de acuerdo.

Gracias.
David.

Bueno, puede que él tuviera necesidad de hablar conmigo, pero yo no tenía necesidad de hablar con él. La

idea de que yo hubiese forzado mis propios ordenadores y luego detectase el forzamiento para llamar la atención era para ponerse furioso. Habría tenido que estar loco para presentar una ponencia técnica en una conferencia auspiciada por la NSA menos de tres meses después.

En cualquier caso, si él quería escribir su historia y tirarse por aquel acantilado en particular, yo estaba perfectamente dispuesto a permitírselo. No tenía la menor intención de telefonearle en un futuro próximo, por más agresiva que fuese su persecución.

Todavía estaba secándome el

cabello cuando llegó Markoff. Mientras juntaba mis cosas le describí lo que había ocurrido el jueves y el viernes. Hablados de la conexión israelí con el estudiante, jsz.

"Creo que la conexión israelí es significativa", dijo él. "Si yo fuera una agencia de inteligencia extranjera, o, si vamos al caso, alguien que quisiera robar tecnología a empresas de Estados Unidos, ¿qué mejor cobertura que tener a un delincuente informático fugitivo como tapadera?".

Markoff estaba sentado en mi cama jugueteando con mi terminal RadioMail. Había una única luz encendida en la

diminuta cocina, pero la habitación estaba aún bastante oscura. Aunque afuera estaba gris, no me había molestado en abrir las cortinas.

"Quizá se trate efectivamente de una operación del Mossad", continuó. "Digamos que ese tipo se hizo amigo de Kevin a través de uno de esas tertulias en Internet, a través de Hacktic en Holanda. Ahora lo incita a atacar diversos ordenadores americanos. Después se reparten los despojos".

Yo no lo veía especialmente claro. Sería fácil para jsz disfrazar su identidad en Internet, y fácilmente podría estar conectando con los

ordenadores de la escuela desde cualquier parte del mundo. Y en todo caso, ¿por qué una agencia de inteligencia israelí habría de tener un interés tan grande en software de telefonía móvil y en herramientas de desarrollo? A mí me parecía más creíble que Mitnick pensara que pirateando el código del teléfono móvil podía hacerse efectivamente invisible, pues su apuesta mayor consistía en no ser capturado. Otra posibilidad podría ser la de que estuviera implicado de alguna forma en actividades de espionaje industrial, tal vez robando el software para alguien que tuviera una

posibilidad real de darle uso.

Era la una de la tarde cuando abandonamos el hotel. A Robert no lo esperábamos de vuelta en la Netcom hasta una hora tardía del día y habíamos acordado reunirnos para comer con Mark Seiden en algún sitio entre San José y su casa en San Mateo. Convinimos en que fuera en Buck's, un restaurante y bar informal del Woodside frecuentado por los empresarios capitalistas y los altos ejecutivos de Silicon Valley que vivían en aquel exclusivo barrio-dormitorio.

Mientras esperábamos a Seiden llamé por el busca a Kent Walker.

Cuando respondió a mi llamada, dije que buscaría una línea para telefonearle. Crucé la calle hasta una cabina telefónica, le conté lo de la conexión israelí y lo puse rápidamente al tanto de dónde nos encontrábamos en nuestros esfuerzos por conseguir una pista. Convinimos en encontrarnos en Menlo Park, en la oficina de Seiden, ya que Walker estaba de camino a Stanford para una reunión y después podía acercarse a hablar con nosotros. Planeaba abandonar el Departamento de Justicia en sólo tres semanas, y me di cuenta de que esperaba ver resuelto este caso antes de retirarse del servicio.

A continuación llamé a Levord Burns, que había estado en contacto con Sprint Cellular, uno de los dos proveedores de teléfonos móviles en Raleigh. Los técnicos de la GTE le habían dicho que la llamada había provenido de Sprint. Él había hablado con un técnico en Sprint, que le comunicó que el número de teléfono no pertenecía a ellos, que era en realidad de la GTE.

"Es un número raro", dijo. "No va a ninguna parte".

Eso no tenía sentido para mí, porque un número telefónico tiene que ir a alguna parte. Mi primer pensamiento

fue: ¿Quién es el inepto aquí? "¿La llamada es desde Spring, o no?", le pregunté con impaciencia.

Escuché mientras Levord intentaba repetir lo que había oído por parte del técnico de Sprint.

"Disculpe, pero creo que no ha entendido usted bien lo que él le dijo", apunté lo más cortésmente que pude. "Quiero hablar directamente con la gente de Sprint".

Él dijo que preferiría pasarle mi mensaje personalmente al técnico.

"Levord, eso no va a funcionar", respondí yo. "Lo siento, pero necesito hablar directamente con él".

Por más que inicialmente se resistió a darme el número de teléfono, tras engatusarlo un poco accedió a intentar verse con el ingeniero de la Sprint y concertar una conferencia telefónica para los tres.

Apareció Seiden, nos sentamos todos en un reservado y pedimos la comida. Seiden nos contó su propio choque con los administradores de la Colorado SuperNet. Mientras hacía el seguimiento, Mark pudo ver ataques contra la CSN, pues algunos fueron lanzados a través de Internex. Había llamado y acabó hablando con una persona distinta de la que había hablado

conmigo, a la que le advirtió que un intruso estaba metiéndose con los ordenadores de la CSN. Le describió cómo había observado al intruso modificar el núcleo de su sistema operativo y después volver a arrancar de nuevo el ordenador. Mark tenía varias sugerencias para ellos, así como diversas preguntas, pero el del personal de apoyo técnico de la CSN no estuvo por la labor de aceptar aquella historia así como así, y le dijo a Mark: "Quisiera su inicial de apellido materno, su fecha de nacimiento y su número de la seguridad social".

"¿Cómo dice?", exclamó Mark,

“¿Para qué quiere esa clase de información?”.

“Quiero someter sus datos a una comprobación por el NCIC antes de volver a llamarle”, fue la respuesta. El NCIC es la base de datos del centro nacional de información sobre antecedentes delictivos, que supuestamente sólo está a disposición de los agentes de la ley.

“¿El NCIC?”. Mark estaba anonadado. “¿Y por qué habría de tener acceso al NCIC *usted*?”.

“Tengo mis contactos” respondió el otro.

Obviamente, sus contactos eran los

agentes del FBI en Los Ángeles que creían estar acorralando a Kevin Mitnick en Colorado.

"No podía creer lo que estaba oyendo", dijo Mark, pero le dio al hombre la información pedida y colgó. Horas más tarde, como no recibía respuesta alguna de la CSN, volvió a llamar.

"¿Pero qué demonios está pasando?", preguntó. "¿No se da cuenta de que ese individuo acaba de volver a entrar en vuestro sistema?".

Fue inútil. Al igual que antes Andrew y yo, Mark llegó a la conclusión de que tratar con la gente de la CSN era

perder el tiempo.

Mark había pasado algún tiempo examinando cuidadosamente los archivos de material robado que habían sido escondidos en la Well. Después de haber observado al intruso atacar reiteradamente a Internex —valiéndose en cada ocasión, para penetrar en los sistemas, de una serie de herramientas traídas de la cuenta dono en la Well— había decidido entrar él en la cuenta y descargar el directorio completo, con el fin de estar preparado para cualquier herramienta con la que pudiera ser atacado. En uno de los escondrijos encontró sesiones de husmeo desde la

CSN que indicaban que el ordenador administrativo de ésta las había sufrido; pues los archivos contenían tanto contraseñas de usuario como de administrador. Otra de las cosas de las que se enteró fue que la Colorado SuperNet conservaba el número de la seguridad social de sus clientes, que es un dato obviamente privado. Si se tiene el nombre, dirección, teléfono, número de seguridad social y de la tarjeta de crédito de una persona no hace falta más para hacerle la vida imposible.

Mientras esperábamos la comida llamé por mi busca a Kathleen Cunningham, que al poco rato me

respondió. Esta vez fui al teléfono público que había al fondo del restaurante. Necesitaba más información sobre el *modus operandi* de Mitnick, y tenía la esperanza de que ella fuese más comunicativa que los neuróticos agentes del FBI con los que habíamos estado tratando.

Estaba de suerte, pues Cunningham se mostró totalmente dispuesta a darme información sobre sus esfuerzos para capturar a Mitnick por una evidente violación de la libertad condicional que databa de fines de 1992. Me contó que el FBI había enviado a Colorado a un equipo de seguimiento con una unidad

Triggerfish de localización por ondas de radio para seguir sus huellas.

"Kevin es un descarriado, pero no es especialmente peligroso", dijo.

Parecía tener lástima del fugitivo y considerarlo un pobre chico extraviado a quien tenía la obligación de encontrar. Sospechaba que todavía se mantenía en comunicación con la familia, y dijo que recientemente había hablado con ellos, en un esfuerzo por convencerles de pedirle a Mitnick que se entregase. Hablamos de la vez en que escapó por los pelos en Seattle, en buena medida porque la policía local y los investigadores de la compañía

telefónica no conocían al que estaban vigilando. Cunningham se había enterado de que en octubre pasado un investigador de la McCaw Cellular y un consultor en seguridad de la compañía telefónica le habían seguido el rastro durante varias semanas. Lo habían seguido a pie mientras él iba por su barrio llevando un teléfono móvil y una bolsa de deportes, y lo observaron entrar en un Safeways y en el Taco Bell local. Varias noches habían llegado a subir hasta la puerta de su apartamento (el nombre en el buzón era Brian Merrill) y lo habían escuchado hablar por teléfono de apoderarse de unas

contraseñas.

En otra ocasión interceptaron sus comunicaciones por el teléfono móvil y escucharon fragmentos de una conversación sobre ajustar cuentas con el representante de alguien.

“Los vamos a hacer polvo”, le decía Kevin a su amigo.

También mencionó Denver, como si hubiera estado allí recientemente.

Cuando Mitnick huyó, la policía hizo un inventario de lo que encontró en su apartamento. Entre las pruebas que hallaron había material para fabricar reproducciones ilegales de teléfonos móviles. También encontraron un

ordenador portátil, así como una factura por 1.600 dólares correspondiente al tratamiento de una úlcera gástrica y una receta de Zantac. En la mesa de la cocina hallaron un escáner de radio y discos compactos de Aerosmith y Red Hot Chili Pepper.

Cunningham dijo que al parecer el FBI creía que Mitnick había estado hacía poco en San Francisco, cuando menos brevemente. Un agente del FBI había escuchado una conversación telefónica de un socio de Mitnick que vivía en la zona de la bahía, y en el curso de la misma el hombre se había apartado del auricular para hablar con

alguien, a quien el agente había oído claramente que decía, “Hey, Kevin”.

Llevaba veinte minutos al teléfono cuando Markoff vino a decirme que se me estaba enfriando la sopa. Le di las gracias a Cunningham por su colaboración y convinimos en mantenernos en contacto.

Cuando regresé a la mesa, Mark expuso otra interesante pista: la conexión Paul Kocher. Mark se había interesado en Kocher tras encontrar correo de febrero y marzo de 1994 sacado de su ordenador. Paul Kocher, estudiante superior de biología en la Universidad de Stanford, se había

interesado en la criptografía desde que estaba en bachillerato, convirtiéndose en un experto criptógrafo por afición, y después transformó su afición en actividad retribuida complementaria. Era consultor de la RSA Data Security, Inc. —la empresa más importante de Silicon Valley en el ámbito de la criptografía— y de Microsoft.

Además había escrito un artículo con el criptógrafo israelí Eli Biham esbozando un modo de descodificar el PKZip, un programa de compresión y archivo de software ampliamente utilizado que lleva incorporado un elemento de codificación. Biham trabaja

en el departamento de ciencia informática en la Technion, una prestigiosa institución de enseñanza de ciencia e ingeniería en Israel, y se le reconoce como uno de los mejores criptógrafos del mundo. En diciembre de 1991 había publicado con Adi Shamir, otro criptógrafo israelí, una comunicación en la que expusieron uno de los primeros esfuerzos de investigación parcialmente acertados en demostrar potenciales debilidades en el U. S. Data Encryption Standard, el estándar nacional de codificación utilizado por el Gobierno, la industria y por los bancos y otras instituciones

financieras.

Después de haber publicado la comunicación, Kocher había hecho público en la red un fragmento de la misma en que se describía el método para descodificar contraseñas que empezaran por la letra *z*. Su intención había sido probar que la técnica Kocher/Biham era un modo eficaz de romper el código, sin hacerlo accesible para todas las contraseñas. Al parecer, Mitnick había visto el material expuesto y se había fijado como objetivo los archivos de Kocher con el fin de obtener la versión completa del programa.

Mark telefoneó a Kocher, y el

estudiante de Stanford se dirigió a su casa en Belmont a mirar los archivos. Tenía una singular historia que contamos. Más o menos en la misma época de diciembre en que atacaron mis ordenadores, Paul Kocher había recibido un mensaje de Eli Biham por correo electrónico: "Paul, ¿puedes enviarme una copia del programa de descodificación del PKZip? Me hace falta para mi investigación".

Kocher no respondió al mensaje, porque la solicitud le pareció fuera de lugar. Seguramente Biham sabía que transmitir software criptográfico al exterior del país sin un permiso de

exportación constituía una violación de las leyes americanas sobre control de exportaciones.

Una semana después llegó una nota más estridente de Biham, que decía: "Paul, dónde está ese código fuente que te pedí?".

Esta vez Kocher le respondió con una nota en la que decía: "Eli, tú conoces las leyes sobre criptografía mucho mejor que yo. ¿Por qué me pides eso?".

Pocos días más tarde recibió una respuesta de Biham dirigida a una extensa lista de personas: "Cualquiera que haya recibido correo de mi parte

durante el último mes debe desconfiar del mismo. Tengo motivos para creer que mi cuenta fue forzada y ocupada".

Cuando nos levantábamos para irnos, entró en el restaurante Laura Sardina, una de las primeras empleadas de Microsystem y amiga de muchos años. Es una persona que realmente sabe cómo conseguir que se hagan las cosas en la compañía y le pregunté si podía prestarme algunas SPARCstations, pensando que si esto resultaba ser una cacería prolongada íbamos a necesitar más hardware para establecer seguimientos en diferentes lugares. Ella deseaba colaborar y me dijo que me

pasara el lunes por su oficina.

Después de salir de Buck's seguimos a Seiden a Menlo Park para reunimos con Kent Walker, tomando por Woodside Road, que se extiende desde las colinas hasta la bahía, y sobre la que los más prósperos magnates de la informática tienen sus mansiones y sus ranchos de caballos.

Con los tejanos, Walker parecía aún más joven que con su vestimenta formal de los días de trabajo. Yo hice un resumen de lo que habíamos sabido en las dos noches pasadas y a continuación lo presioné para que colaborase más, consiguiendo autorizaciones de las

compañías telefónicas de Denver, así como una orden de rastreo de la Sprint Cellular en Raleigh.

"No puedo ayudarle en Denver", dijo él, "pero si quiere una autorización en Raleigh, la tiene".

Eran más de las cinco de la tarde y ya empezaba a oscurecer. En la Netcom, Robert y Andrew habían reanudado su vigilancia, y nosotros volvimos a la autopista para dirigirnos a San José a reunimos con ellos. Cuando llegamos descubrimos que teníamos lo que podría convertirse en un problema más apremiante. Andrew había llamado a Pei a la Well, y ella le había dicho que la

noche anterior, a eso de las diez y media, el seguimiento había revelado la contraseña que Mitnick estaba utilizando para acceder a su cuenta en *escape.com*. Después de que él se fue, Pei había decidido por su cuenta acceder como Mitnick y echar una ojeada.

El problema era que al hacer eso podía haber estropeado nuestro elemento sorpresa. La mayoría de los sistemas operativos alertan al usuario cada vez que éste conecta de la hora exacta en que se registró previamente. Es una simple precaución de seguridad que puede advertir al usuario de un ordenador si alguien está usando su

cuenta.

"¿Por qué hizo eso Pei?", dije irritado. "¿De qué esperaba enterarse?"

"No tengo ni idea", dijo Andrew.

"¿Y limpió sus huellas?", pregunté.

"No", respondió él.

Me parecía increíble que alguien hubiera hecho algo tan estúpido, sobre todo tratándose de una persona supuestamente familiarizada con los ordenadores y la seguridad informática. Ahora nuestro problema era que, a menos que fuera completamente descuidado, en el mismo instante en que utilizara su cuenta en *escape.com*, Mitnick descubriría que alguien estaba

al tanto de su presencia.

Peor aún, si no teníamos suerte y él tenía en funcionamiento sus propios sniffers en *escape com* o en la Well, sabría exactamente quién lo estaba siguiendo. No podíamos hacer nada por enmendar el error de Pei, y nuestra única opción era vigilar y esperar. Tal vez tuviéramos suerte.

"Llámala y explícale qué fue lo que hizo mal", le dije a Andrew. "Pídele que por favor nos dé unos días más antes de que vayan agitando una bandera roja ante la cara de Kevin Mitnick".

En nuestros ordenadores portátiles instalados en el despacho de Robert

pasé para Markoff la conversación de teclado entre Mitnick y jsz del viernes, y cuando él vio que el fugitivo pensaba que era posible falsificar un artículo de *New York Times* forzando la entrada en *nytimes.com*, se rió. "Si hubieran sabido", dijo, "que la dirección del *Times* tiene tal desconfianza de que pueda ocurrir algo así, que el sistema editorial Atex no tiene conexión interactiva con la Red…".

De la nueva lectura de la conversación entre Martin y jsz dedujimos otra pista. Martin había mencionado haber visto la película *Los fisgones*, y Markoff reconoció el

significado del nombre de usuario marty y de control-f bishop. Aparentemente, Kevin Mitnick tenía una persistente obsesión con el actor Robert Redford. Primero fue Cóndor, y ahora parecía haber adoptado otro de los papeles de Redford. En *Los fisgones*, el actor había hecho de Marty Brice, un activista contra la guerra y hacker informático a quien habían perseguido en los años sesenta y que años después había adoptado el nombre de Marty Bishop. En la película, Bishop ha creado su propio grupo de hackers, que termina trabajando bajo contrato para la Agencia Nacional de Seguridad.

La conexión Marty fue una confirmación más de que nuestro objetivo era Mitnick, y yo esperaba que fuera también una importante pista sobre su ubicación. Telefoneé a un amigo en Boulder para pedirle que se fijara en el programa de televisión si la película había sido exhibida recientemente, pues eso podría indicarnos en qué región se encontraba Mitnick. Desgraciadamente, resultó que *Los fisgones* se había pasado por televisión de un extremo al otro del país.

Los registros de entrada indicaban que la última aparición de Mitnick por la Netcom había sido a media tarde.

Revisamos nuestros datos de filtrado y encontramos que había conectado con un ordenador llamado mdc.org, el dominio en Internet para la Lexis-Nexis, la empresa de base de datos online. Utilizó una contraseña robada para acceder a su base de datos de noticias actuales y luego tecleó la siguiente orden de búsqueda: MITNICK W/30 KEVIN. ¡Estaba buscando cualquier mención de su nombre en artículos recientes! Nuestra transcripción mostró que había examinado el texto completo de una historia después de recorrer los titulares de las más recientes incorporaciones a la base de datos.

NIVEL 1 - 46 ARTÍCULOS

1. Newsweek, febrero 6 de 1995, EDICIÓN NACIONAL, NEGOCIOS; Pg.38, 270 palabras, EL MÁS GRANDE GOLPE DE PIRATEO

2. Deutsche Presse-Agentur, enero 24 de 1995, martes, Noticias Internacionales, 614 palabras, EE UU da caza al capo de los “piratas" informáticos, Washington

3. United Press International, enero 24 de 1995, martes, ciclo BC, Noticias de Washington, California, 605 palabras, EE UU da caza a prominente "pirata" informático, POR MICHAEL KIRKLAND, WASHINGTON, enero 24.

4. United Press International,

enero 24 de 1995, martes, ciclo BC, Noticias de Washington, California, 608 palabras, EE UU da caza a prominente "pirata" informático, POR MICHAEL KIRKLAND, WASHINGTON, enero 24.

5. U.S.News & World Report, enero 23, de 1995, CIENCIA & SOCIEDAD; ARTÍCULO PRINCIPAL; ; Vol.118, N°3; Pg. 54, 3.666 palabras, Vigilando el Cyberespacio, Por Vic Sussman

6. Pittsburgh Post-Gazette, diciembre 20 de 1994, martes, PRIMERA EDICIÓN, Pg. B1380 palabras, Seis internos denuncian castigos en la cárcel, Marylynne Pitz, Post-Gazette Staff Writer

NIVEL 1 - 2 DE 46 ARTÍCULOS

Deutsche Presse-Agentur

Enero 24 de 1995, martes, Ciclo BC
23:04 Tiempo Europa Central

SECCIÓN: Noticias Internacionales
EXTENSIÓN: 614 palabras
TÍTULO: EE UU da caza a prominente "pirata" informático

PROCEDENCIA: Washington
CONTENIDO:
Las autoridades estadounidenses pidieron el martes la colaboración del público para dar con la pista de un

legendario y experto manipulador de la superautopista de la información. Los funcionarios declararon que *Kevin David Mitnick*, 31, originario de Sepúlveda, California, está haciendo uso de su destreza como hacker para ir un paso por delante de la ley…

A eso de las 7 todo el mundo tenía hambre. Robert, que el jueves se había mostrado tan entusiasmado con la posibilidad de rastrear a su enemigo, estaba ahora con sueño y taciturno. Como daba la impresión de que íbamos a pasar otra larga noche, Markoff y yo decidimos salir a buscar cena para los

cuatro. Recorrimos en coche varias manzanas pasando por delante de cines y centros comerciales, hasta que finalmente localizamos una pizzería Round Table. Pedimos dos pizzas, y mientras aguardábamos nos sentamos a una larga mesa en el comedor casi vacío. Hablamos del viaje de fin de semana de Julia, y le conté mi sensación de alivio del viernes cuando ella partió, pero también que la echaba de menos.

Poco después de que hubiéramos regresado a la Netcom llamó por fin Levord para anunciar que en un par de minutos iba a iniciar la conferencia telefónica a tres. Cuando volvió a llamar

yo apenas podía oír al técnico de la Sprint al otro extremo de la línea.

"Tsutomu, soy Jim Murphy, ingeniero de comunicaciones de Sprint Cellular en Raleigh".

Su voz era débil porque era una conferencia telefónica múltiple, y le pregunté si estaba usando un teléfono móvil. Dijo que sí.

"Perdóneme, pero la verdad es que no quiero mantener esta conversación estando usted en un teléfono móvil", dije. Levord había arreglado la conferencia, pero me asombraba que no hubiese tenido en cuenta el problema de seguridad que implicaba. En el

apartamento de Mitnick en Seattle habían encontrado un radio escáner; ¿nadie se había dado cuenta de que él podía interceptar fácilmente esta conversación?

Murphy explicó que estaba en medio del campo y que le llevaría unos diez minutos regresar a la oficina principal de conmutadores de la compañía. Cuando reanudamos la conversación siguió sonando tan débilmente al otro extremo de la línea que hablábamos a voces.

Ninguno de los dos tenía una buena explicación de por qué los conmutadores de la Sprint y de la GTE

estaban demostrando que la llamada debía haber venido del otro, pero ambos comprendíamos que no era posible. Le expliqué con quién creíamos estar tratando, y que Kevin Mitnick tenía una historia de quince años de manipular los conmutadores de compañías telefónicas. A él lo indignó la idea de que alguien manipulase *su* conmutador, y en el curso de la conversación resultó que Murph, como prefería que lo llamase, era en realidad muy competente, de modo que enseguida nos enfrascamos en detalles técnicos.

Empecé yo haciéndole preguntas sobre el conmutador telefónico que

estaba utilizando el sistema de Sprint. Los conmutadores de las compañías telefónicas son en realidad ordenadores con su propio sistema operativo especializado. A menudo tienen puertos de discado para diagnósticos y mantenimiento a distancia. Es frecuente que adictos al teléfono y miembros del submundo informático utilicen esos puertos como puerta secreta para manipular los conmutadores. Pueden así conseguir llamadas gratis o crear líneas de tertulias a las que cualquiera puede incorporarse. La máquina de Sprint era una Motorola EMX 2500, en tándem con un conmutador DSC 630, algo sobre lo

cual yo no sabía nada. Yo había tenido alguna experiencia con conmutadores de pequeñas compañías telefónicas y conmutadores PBX, pero no mucha con grandes conmutadores de oficina central como aquel. Murph me dio una clase sobre el funcionamiento del mismo y qué clase de datos tenía a su disposición. Tenía que ser cuidadoso, porque aunque nosotros teníamos autorización para la información de GTE, Kent todavía no había preparado una para Sprint, de modo que Murph estaba limitado en cuanto a qué clase de datos sobre llamadas podía ofrecerme.

Le pregunté por el número de la

GTE. Resultó que el número que había sido captado merced a la autorización de rastreamiento de la GTE era 919-555-2774. "¿Es un número celular, o es una mezcla de la información de la identificación del número de origen (ONI)?". ONI se usa también para suministrar el Caller ID, el elemento que pasa el número de teléfono del que llama por la red al teléfono llamado e identifica al emisor.

"No es uno de nuestros números", respondió. "Ese prefijo ni siquiera es de un teléfono móvil".

A estas alturas supe que algo andaba mal. Normalmente, los técnicos pueden

obtener información de rastreo de llamadas buscando un número en una base de datos que se conserva en el centro telefónico de conmutación. Si se trata de un número local controlado por la centralita, la base de datos mostrará precisamente el grupo de cables telefónicos por el que la llamada está entrando.

En el caso presente los registros de llamada de la GTE mostraban que la llamada venía de una conexión digital T-1 permanente entre el conmutador de GTE y el conmutador celular de Sprint al otro lado de la ciudad, utilizada para encaminar llamadas entre ambos

conmutadores. Una llamada de entrada a un conmutador desde otro entra por lo que se denomina un línea de enlace, en este caso la T-1. Esta puede transportar simultáneamente veinticuatro llamadas. El conmutador se fija en su base de datos de tablas de traducción y encamina cada llamada individual de acuerdo a la información encontrada. Si se trata de una llamada transmitida localmente, las tablas de traducción dirigirán la llamada sea a una línea telefónica determinada o en el mundo celular a su equivalente, conocido como MIN (número de identificación de móvil).

Mientras hablábamos, Murph

comprobaba su conmutador para ver si encontraba algo obviamente fuera de lugar o que hubiera sido manipulado. Mientras esperábamos al otro lado de la línea él exploró las tripas del ordenador, examinando sus tablas de traducción comentándome al pasar lo que veía. Dijo que tenía la teoría de que Mitnick podría de algún modo haber creado un número especial que encaminara sus llamadas a través del conmutador celular, y de ahí al número de llamada local de Netcom. Todo número telefónico tiene una ruta directa y una alternativa, y Murph se preguntaba si una de estas últimas había sido

manipulada. Pasó un largo rato investigando su base de datos para ver si podía encontrar alguna huella de una ruta oculta de ese tipo.

Pero no apareció nada claro, y empezamos a buscar explicaciones alternativas. Murph tenía en una base de datos registros que podían ser revisados y clasificados según muchos parámetros distintos. Cada una de tales operaciones, no obstante, llevaba más de media hora.

Hablamos de formas útiles de distribuir los datos, y luego se me ocurrió preguntar: "¿Qué pasa cuando marco el número de rastreo de GTE?". Lo hice, y oí ese misterioso "click-

click", "click-click", "click-click", que continuó repitiéndose, volviéndose cada vez más débil hasta que desapareció y la llamada se cortó.

Volví al teléfono y le describí a Murph lo que había oído.

"Supongo que lo que oye es la llamada que va y viene sin cesar entre el conmutador de ellos y el nuestro", dijo. "En cierto momento, la energía baja de un determinado nivel y la llamada se interrumpe".

Probé de nuevo, y esta vez Murph vigiló la llamada desde su conmutador. De nuevo oí el "click-click", pero al mismo tiempo oía a la impresora en su

oficina, que registraba cada vez que su conmutador celular trataba de establecer una llamada, “Kerchank”, “Kerchank”, “Kerchank”.

“Me sorprenderé mucho si ha estado manipulando nuestro conmutador”, dijo Murph. “Tenemos sí instalaciones distantes, pero todos los accesos remotos están registrados. Cuando Motorola, por ejemplo, conecta con nuestro conmutador, nosotros primero le damos una contraseña, supervisamos sus actividades y cambiamos la contraseña inmediatamente después del término de la sesión”.

“Déjame probar otra cosa”, dije.

Marqué el número telefónico que estaba una unidad por encima de nuestro número misterioso. Al otro extremo de la línea oí el conocido murmullo de una máquina de fax. Esta vez, Murph no vio pasar la llamada por su conmutador. Eso me hizo sospechar aún más de la GTE. Nos decía que solamente un número en un bloque entero de líneas telefónicas había sido encaminado a Sprint. Había algo raro en aquel particular número telefónico.

"Lo que yo deduzco es que el conmutador de la Sprint ha sido manipulado", dije.

Continuamos especulando. Él dijo

que como disponía de tres terminales, podía iniciar tres búsquedas simultáneas para intentar encontrar un equivalente de la información de registro de entrada de Netcom que yo tenía.

"Probemos una estrategia diferente", sugerí yo. "¿Qué alcance hacia atrás tiene tu base de datos, y qué tipo de cosas puedes buscar?" Él dijo que podía retroceder hasta las 3 de la tarde del jueves 9 de febrero, y me dio una larga lista de categorías de ordenación, incluyendo hora de inicio y final de llamada, duración de la misma, número llamado, etcétera. Examinando mi lista de registros de entrada de gkremen

desde los POP de Netcom, vi que habían varias sesiones prolongadas.

"¿Puedes buscar llamadas de más de treinta y cinco minutos el viernes?", le pregunté. Había decidido que aunque a Mitnick le hubiera sido posible ocultar de dónde llamaba, le sería mucho más difícil ocultar el hecho mismo de la llamada. En eso consistía la belleza del análisis de tráfico. La segunda solicitud que tenía para Murph era que buscase todas las llamadas de teléfono móvil hechas a la serie de los números que eran encaminados a los números de teléfono de llamada de la Netcom en Raleigh. Finalmente, le pedí que buscase

todas las llamadas de teléfono móvil al número de Netcom en Denver.

Pocas personas usan un modem celular para transmitir datos, así que cualquier llamada celular a un POP de Netcom sería algo inusual. Y en cualquier caso, dado que Netcom era una llamada local, una llamada de larga distancia a un número de conexión sería todavía más sospechosa. De todas formas, si Mitnick había estado haciendo llamadas usando el sistema celular de Sprint deberíamos poder encontrarlas aquí, aun si la GTE era incapaz de rastrearlas.

Había hecho mis tres preguntas.

Mientras ponía en acción sus ordenadores, Murph dijo que la búsqueda en la base de datos iba a llevar tiempo, de modo que yo le dije que le llamaría de nuevo después y colgué. Tardé un poco en darme cuenta de que los dos habíamos olvidado por completo que Levord había estado escuchando en la línea.

Como los instaladores de PXB estaban aún trabajando en la Netcom y los teléfonos seguían desconectados, me mudé al extremo del edificio opuesto al del despacho de Robert, y allí me instalé en un despacho vacío en el que había un teléfono que todavía funcionaba. Al

cabo de aproximadamente un cuarto de hora llamé de nuevo a Murph para saber el resultado de sus indagaciones.

Empezamos por las llamadas locales al POP de Netcom en Raleigh.

“Creo que he visto aquel primer número”, dijo él.

“¡Estupendo! ¿Puedes darme todas las llamadas al POP de Raleigh?”.

“No puedo decirte los números de llamada porque no tienes una autorización”, replicó. “No puedo darte los pares MIN-ESN”. MIN y ESN son los dos números por separado que definen un teléfono móvil en particular. El MIN en el número asignado al

teléfono y el ESN es el número de serie grabado en el propio aparato.

"Yo no quiero el número", le expliqué, y le dije que lo que intentaba era comparar las llamadas con las sesiones que habíamos visto provenientes de conexiones de Netcom en Raleigh. Estaba más interesado en el patrón de las llamadas que en la propia información. No buscaba el número mismo, tenía curiosidad por ver si había un patrón, una pauta en relación con las llamadas que Mitnick pudiera estar haciendo a Netcom a través de Sprint. Si teníamos suerte, podríamos descubrir que todas las llamadas venían de un

pequeño número de MINs o de la misma localización física.

Comenzamos a jugar una partida que se parecía mucho al clásico juego infantil conocido por "batalla naval". Él no podía decirme cuál era el número, pero podía decirme, bajo ciertas condiciones, si era el mismo que otro.

Lo que yo podía decir era, "¿Ves tal llamada a tal hora?". Cogí dos listas, la lista de números marcados de Netcom de todo el país y el resumen de las sesiones registradas de gkremen.

"El viernes a las 15:29, ¿ves una llamada al 404-555-7332 que dura aproximadamente 44 minutos?".

“Sí, la tengo”.

“¿Tienes una llamada de 49 minutos como a las 20:22 el viernes al 612-555-6400?”.

“La tengo”.

“Provienen las dos del mismo MIN?”, pregunté.

“Sí”, fue la réplica.

“Tienes una llamada el 11 de febrero a las 02:21 al 919-555-8900?”.

“Sí, también tengo ése”.

Hice la misma pregunta con cinco registros de entrada tomados al azar. En cada uno de los casos la respuesta fue la misma: habían sido hechas desde el mismo número de teléfono móvil.

Occam tenía razón.

"Entonces, ¿dónde está?", pregunté.

Murph cruzó la habitación hasta un mapa de los emplazamientos de Spring en Raleigh.

Todas las llamadas venían del número 19, ubicado en las afueras al noreste de la ciudad, cerca del aeropuerto. Ahora contábamos con otro importante elemento de información: Mitnick estaba en un sitio fijo. Yo pensaba que era improbable que las llamadas fueran hechas mientras él conducía, pero me había preocupado que pudiera estar cambiando de ubicación con cada llamada.

“¿Tienes información sectorial?”, pregunté. Algunos sistemas celulares pueden determinar en qué dirección está efectivamente situado el teléfono que llama en relación con el emplazamiento de la célula, es decir, una torre de transmisión-recepción en particular en determinada zona.

“No, no tenemos esa información, pero al este del emplazamiento de la célula está el parque estatal de Umstead, y al noroeste el aeropuerto. Basándome en la ubicación de nuestras otras células, supongo que está transmitiendo desde alguna parte al sur o al oeste de la célula”.

Era casi la una de la mañana. Cuando terminamos, habíamos estrechado su posible localización a un radio de menos de un kilómetro.

"Saldré en avión a primera hora", le dije. "Te veré mañana".

Él me dio sus números y me dijo que me iría a recibir al aeropuerto.

Aunque era tarde, llamé de nuevo a Kent y le dije que era más importante que nunca conseguir órdenes de rastreo para ambas compañías de telefonía móvil. Cuando estaba lejos del teléfono recordé que habían pasado horas desde que hablara con el agente especial Burns. Eran las cuatro de la mañana en

la costa Este cuando lo llamé para decirle que habíamos localizado a Mitnick.

"Ustedes me cortaron", dijo él cuando lo desperté.

Yo sospeché que en realidad se había quedado dormido escuchándonos y no se había dado cuenta, pero me excusé por olvidarnos de él.

"Lo tenemos localizado en un área de un kilómetro", le dije. "Yo vuelo a Raleigh mañana por la mañana, y vamos a necesitar un equipo de detección de ondas radiales".

Era tarde. Lo único que logré fue un neutro "Aahhmm".

Yo había visto irse a Markoff media hora antes y lo llamé al teléfono de su coche. Puesto que no sabía quién estaba escuchando en el Valley, fui discreto.

“Estamos en situación de alcance táctico nuclear”.

15. Raleigh

Esa noche dormí muy poco. Andrew y yo regresamos al Residence Inn, pero yo me quedé levantado haciendo llamadas telefónicas para tener las cosas organizadas en Raleigh. Estaba intentando persuadir al FBI de enviar allí agentes y un equipo de radiogoniometría a la mayor brevedad. Quería ir a Raleigh con el fin de estar mejor situado para obtener información y tomar decisiones en caso de que el

comportamiento de nuestro objetivo cambiase.

A las 4:30 a.m. localicé a Kathleen Cunningham, en un esfuerzo por conseguir que enviasen a Raleigh un equipo Triggerfish de seguimiento de ondas radiales. Ella dijo que haría cuanto pudiese, pero después de colgar el auricular tuve un momento de pánico al preguntarme si se pondría en comunicación con el FBI en Los Ángeles y si éstos intentarían interferir. Por lo que yo había visto hasta ahora, Kevin Mitnick era una criatura de costumbres en el mundo de las redes informáticas. Se iba haciendo evidente que no era tan

listo y que era propenso a cometer errores. Al mismo tiempo, parecía creerse invulnerable. Todo esto debería haberlo convertido en una presa fácil. Pero para el FBI, que dominaba las técnicas de investigación tradicionales pero era ignorante en materia de ordenadores y redes informáticas, bien podría haber sido Casper el Fantasma. No obstante, si el FBI de Los Ángeles resolvía actuar, yo poco podía hacer al respecto. Kent Walker me estaba ayudando, y yo tendría que ver qué tipo de colaboración podría agenciarme cuando llegara a Raleigh.

Llamé a la American Airlines e hice

una reserva para el vuelo de las 9:29 a.m. a Raleigh por Chicago, cuya llegada estaba señalada para las 7 de la noche. Pedí un asiento en primera clase porque Kent me había recomendado que tuviera fácil acceso a un AirFone y yo quería poder estirarme y dormir.

Muerto de cansancio, me levanté por la mañana y tomé a duras penas el desayuno continental del hotel. Andrew me llevó en coche al aeropuerto poco después de las 8 y cuando nos deteníamos junto a la puerta de salidas le pedí que se comunicara con Julia y le dijese adonde me había ido. Pero otra cosa me inquietaba, y era la

preocupación de que, si Mitnick tenía un cómplice, era posible que perdiésemos el software robado y lo encontrásemos esparcido por toda Internet entre miembros del mundo informático.

"¿Podrías hacer una lista de todos los sitios de la red en los que Mitnick ha ocultado software, e idear un plan para reunir pruebas y hacer limpieza una vez que él sea detenido?", le pregunté. "No hagas nada aún: déjame primero aclarar el aspecto legal con Kent Walker".

Cuando me instalé en mi asiento en el avión, pensé, "Esto tiene algo de irreal, es como una película". Llevaba más de dos semanas tras una quimera

electrónica, y ahora en las últimas horas se había transformado de una tenue imagen en Internet en una persona real en el mundo real. No es la clase de situación en la que suela verse inmerso un investigador académico. Hemos rastreado a ese tipo, y cinco horas después salgo en el primer vuelo a tratar de localizarlo.

Sólo dormité un poco en el vuelo a través del país. Cuando llevaba un par de horas en el aire descubrí que Andrew se las había arreglado para introducir secretamente unas manzanas y unos plátanos en mi mochila gris. Era un bonito detalle, y explicaba por qué mi

equipaje se había vuelto de pronto tan pesado.

Durante el cambio de aviones en Chicago dispuse de un poco de tiempo y volví a llamar a Levord. Le pregunté si había conseguido comunicarse con Cellular One, el otro operador en Raleigh. Todavía íbamos a necesitar también su colaboración. Levord dijo que aún no había podido conseguir un número telefónico.

"¿Ha probado el 1-800 CELL-ONE?", le pregunté intencionadamente.

"No, ése todavía no", me contestó, evidentemente enfadado por la sugerencia. Las cosas entre él y yo no

habían empezado demasiado bien y se estaban deteriorando rápidamente. Me daba cuenta de que a él no le gustaba recibir órdenes de un civil, pero se encontraba en una posición incómoda, ya que el Departamento de Justicia le había dicho que cooperase conmigo. Yo tenía la sensación de que Levord estaba técnicamente superado y comprendía que le fastidiase que yo me hubiera hecho cargo de la búsqueda.

A continuación llamé a Kent y le pregunté sobre la legalidad de hacer limpieza después de la detención. Me dijo que él creía que sí lo era, porque estábamos protegiendo la propiedad de

la víctima.

Cuando el avión iniciaba la aproximación final a Raleigh, llamé a Murph, que prometió ir a recibirme en la terminal con uno de sus socios. Aunque en el este era pleno invierno, yo seguía con mi atuendo californiano: *shorts* de excursionista, chaleco Gore-Tex color púrpura y sandalias Birkenstock, sin calcetines.

Julia me había hablado de su adolescencia en Durham envuelta en el aroma del tabaco, y atravesando la terminal percibí por doquier ese perfume dulzón.

"Ya no estamos en Kansas", Toto,

pensé.

Mientras esperaba a Murph fui hasta un grupo de teléfonos y llamé nuevamente a Levord. Todavía no había logrado sacarle un compromiso de apoyo, pero él empezaba a decir que estaba pensando presentarse. Yo aspiraba a estar listo para el caso de que Mitnick saltase de un sistema celular al otro en Raleigh, pero Levord dijo que todavía tenía problemas para comunicarse con Cellular One. Yo seguía recordando lo que había dicho Kent sobre no recibir órdenes de agentes de la ley, y que en nuestro caso la ley nos proporcionaba respaldo legal y

administrativo. No hice partícipe de esto a Levord, pues no veía motivos para restregarle aquello por la nariz. Hacia el final de la conversación él aceptó ponerse en comunicación con un agente local en Raleigh.

No obstante mi tenacidad, todavía no estaba seguro de que Mitnick estuviese efectivamente en Raleigh. ¿Y si había instalado algún ingenioso tipo de repetidor? Imaginaba a agentes del FBI yendo a un apartamento para encontrarse únicamente con un complicado sistema de comunicaciones y una alarma para hacer saber a Mitnick el descubrimiento. Estaríamos como al principio, pero

sería una puerta más que tendríamos que derribar.

Me encontraba todavía en los teléfonos del aeropuerto cuando entró Murph con otro ingeniero, Joe Orsak, a recibirme. Murph era un hombre grande y fornido, que parecía haber jugado al fútbol de joven. Sus modales eran directos y sin rodeos, y tenía un leve toque de acento sureño. Su acompañante era todavía más voluminoso, un tío corpulento, de semblante amigable y bigote. Ambos parecían entusiasmados con la perspectiva de una aventura que los apartaba de la tarea cotidiana del uso y mantenimiento de centrales de

telefonía móvil. Recientemente habían intervenido con el éxito en el desmantelamiento de un grupo celular ilegal en la zona de Raleigh que había estado empleando teléfonos copiados y vendiendo tiempo de llamadas internacionales desde una granja en las afueras de la ciudad, y aquel incidente parecía haberles abierto el apetito por perseguir más fraudes telefónicos. Mientras salíamos para dirigirnos a la furgoneta de Sprint Cellular aparcada junto a la acera, pensé para mis adentros: "Si Mitnick creía que podía ocultarse aquí en algún lugar tranquilo, está claro que se equivocó".

Necesitaba recoger un coche alquilado y acabé con un Green Geo Metro en el cual seguí a la furgoneta de la Sprint. Las autopistas son todas iguales en todos los EE UU, pero lo que noté inmediatamente en Raleigh fue que había muchas obras en marcha. Por todas partes estaban reparando y construyendo nuevas autopistas.

La MTSO de Sprint, que Murph pronunciaba "mitso", el término que en el argot de la industria telefónica celular se emplea para Mobile Telephone Switching Office (Oficina de Conmutación de Telefonía Móvil), estaba situada al otro lado de la ciudad,

en un solar arbolado al borde de una zona de oficinas de reciente creación. Estaba oscuro cuando llegamos, pero alcancé a ver un edificio de hormigón de dos plantas detrás de una alta valla de seguridad. Detrás del edificio se elevaba una antena con una luz roja intermitente en lo alto.

Adentro conocimos a Lathell Thomas, de la agencia local del FBI en Raleigh, a quien todos conocían por L. B. Cuando entré estaba al teléfono tratando de obtener más información sobre la situación en la que lo habían metido. Era un negro de unos sesenta años, y había venido provisto del mismo

memorándum confidencial de la AirTel sobre Kevin Mitnick que habían tenido los agentes del FBI en la reunión en la Well. Parecía agradable y profesional, pero enseguida me di cuenta de que en materia de fraude telefónico y delito informático no era precisamente un experto.

Llamé a Andrew y establecí dos códigos para utilizar en el busca en el caso de una detención. Uno fue una señal de "alerta". Le pedí al agente del FBI la fecha de nacimiento de Mitnick, pero estaba ocupado, así que me acerqué y apoderándome del memorándum de AirTel leí la fecha: 080663. A

continuación se me ocurrió para el segundo número la fecha del primer ataque a mis ordenadores en San Diego —122594— como señal de "adelante" para que Andrew empezara a limpiar el software robado.

Andrew me contó que Mitnick había estado de nuevo en acción y que habían visto un par de sesiones de charla que los habían intrigado. La primera tuvo lugar cerca de mediodía con un amigo que era miembro de la vieja pandilla de Mitnick en Los Ángeles. La casa de este amigo había sido asaltada por el FBI al mismo tiempo que Mitnick desaparecía. El amigo había puesto pleito al

Departamento de Justicia por el allanamiento y decía públicamente pestes de los agentes del FBI que perseguían a Mitnick. Gran parte de la conversación era indescifrable, dijo Andrew. El amigo se refería a Mitnick como "Kremlin", y éste a él como "banana". Hablaban de una señal preconvenida que vendría después y les permitiría mantener una conversación telefónica directa.

Era una conversación extraña y Andrew y yo especulamos sobre el significado de otras palabras, que parecían parte de un código. El amigo se quejaba de un "mosquito", y poco

después Mitnick tecleaba: “hahaha. no entendí tu mensaje: noticia, mosquito. Supongo”. ¿A qué se refería mosquito? ¿Quería decir que les preocupaba ser “pinchados”? Al final, Mitnick tecleó: “Oí que ayudante de jl estaba en lo de hottub”. Los dos reconocimos “hottub”. En mensajes que el mismo amigo había puesto en conferencias por Usenet en el pasado, incluía una línea al final de cada mensaje, refiriéndose a uno de los agentes que buscaban a Mitnick como Kathleen “Hottub” Carson.

Después de nuestra conversación, Andrew me envió por fax parte del material de las sesiones de seguimiento.

Esa mañana, Mitnick había conectado con *escape.com* con una nueva contraseña —Yoda, el personaje de *La guerra de las galaxias*— y había encontrado una carta de jsz. Éste le avisaba que su padre había sufrido un grave ataque cardiaco y que no estaría en la red los siguientes tres o cuatro días.

"Una cosa más", me dijo Andrew antes de colgar. "Puede que haya metido la pata y haya enviado a Julia a Denver en vez de a Raleigh".

"¡Vaya!", respondí. "¿Qué pasó?".

El viernes por la noche, cuando Julia partió, todavía pensábamos que la más

probable ubicación de Mitnick sería Denver. El domingo por la mañana, después que yo salí para el aeropuerto, Andrew la llamó para transmitirle el mensaje de que si quería viniera a reunirse conmigo. Como el lugar donde ella se alojaba era sumamente rústico, ninguna de las habitaciones tenía teléfono, y el teléfono público no funcionaba, Andrew había dejado un mensaje urgente en la oficina para que Julia lo llamase por el busca. Estaba preocupado por las historias que había oído sobre la pericia de Mitnick para intervenir líneas, y cuando por fin se comunicó con Julia mantuvieron una

conversación especialmente críptica para evitar el peligro de revelar nada.

Andrew dijo: “Tsutomu fue al lugar al que planeaba ir luego”.

Al rato de colgar se dio cuenta de que no tenía la menor idea de si ella creía que estaban hablando de Denver o de Raleigh, pero para entonces era demasiado tarde para volver a encontrarla. Tampoco yo podía hacer nada al respecto, pues no sabía cómo dar con ella. Sólo me quedaba esperar a ver si Julia se reunía con nosotros.

Poco después, me llamó al busca. La llamé enseguida y me dijo que había reservado pasaje para Denver y me

llamaba para comunicármelo.

"Bueno", dije, "pero no estoy en Denver, sino en Raleigh". Le conté brevemente lo que había ocurrido en su ausencia, y ella dijo que haría una reserva para el siguiente vuelo que saliese. Pocos minutos más tarde llamó para decirme que cogía un vuelo de madrugada y llegaba por la mañana.

Dentro del centro de conmutación de Sprint empezamos otra vez el juego de la espera. Mitnick había desaparecido del sistema de la Sprint. Andrew veía actividad en la Netcom, pero hoy Mitnick no aparecía en las consolas de Murph. El miniordenador Motorola de

Sprint que controlaba el conmutador era de una lentitud exasperante para clasificar los detalles de registros de llamada que necesitábamos para comparar con el perfil de las actividades del día anterior que teníamos en nuestro poder. Al cabo de un rato una cosa estuvo clara: no había Mitnick. El número que llamaba el día anterior había desaparecido. Sugerí ampliar la red de búsqueda para ver si sencillamente él había cambiado su comportamiento o si estaba usando otro número. Cada indagación llevaba tiempo y más tiempo. Era evidente que aquel ordenador no había sido diseñado

para efectuar esta clase de búsqueda, sino para facturar las llamadas de los clientes.

"¿Se pueden volcar parte de los datos de llamadas en un disco flexible?", pregunté finalmente. "Si se pueden sacar del sistema, nosotros podemos meterlos en mi RDI y efectuar una búsqueda más precisa".

Murph dijo que se podía y nos pusimos a descargar su información. Pero entonces él se detuvo y después de pensarlo un instante resolvió probar antes otra cosa. Llamó a un ingeniero conocido suyo en Cellular One y le pidió que buscase entre sus registros

alguna actividad sospechosa. Le dimos un perfil de las cosas a buscar, pero el técnico dijo que él tampoco encontraba ninguna coincidencia.

Había realizado el largo viaje aéreo hasta la costa Este, y ahora Mitnick empezaba a parecerse un poco a Houdini. Si aparecía en la Netcom pero no a través de Sprint ni de Cellular One, *¿dónde* estaba? La cosa era exasperante: él tenía que estar en uno de los dos sistemas.

"Inténtalo un poco más", dije. "Tiene que estar ahí".

Busqué otros varios números de llamada de Netcom en distintas partes

del país y se los leí. El ingeniero de Cellular One hizo un nuevo repaso a sus datos, y un ratito después volvió al teléfono a decir que no tenía actividad de llamada que casara con nuestra descripción. Mitnick estaba en el aire, pero ¿dónde?

"No puedo ayudaros más, tíos, a menos que haya una autorización", dijo el ingeniero.

Estábamos otra vez bloqueados por el mismo problema que Murph y yo habíamos tenido el sábado por la noche, pues no teníamos la autorización necesaria para los registros de Cellular One. Aunque el domingo por la mañana

la Sprint había recibido una autorización para el rastreo, localización e información de registro de llamadas, así como una orden judicial autorizando el seguimiento en tiempo real, entre tanto Mitnick debía haber "secado" su teléfono móvil. Era obvio que había intercambiado el fraudulento par MIN-ESN de Sprint por uno que debía haber pertenecido a un suscriptor de Cellular One. Llamé a Kent y con ayuda de Murph él redactó una segunda autorización, que se pasó por fax a Cellular One.

En este punto, no obstante, todo parecía detenido. Mi plan había sido

reunir un equipo de representantes de la ley, ir al emplazamiento de la célula y, cuando Mitnick saliera al aire, utilizar un dispositivo direccional para localizarle. De nuevo el FBI había echado el freno. Al agente especial Thomas, a quien habían llamado un domingo por la noche para ocuparse de un caso del que no sabía nada, dejó claro que no estaba dispuesto a tomar ninguna decisión sobre el siguiente paso a dar, sin intervención de alguna autoridad superior.

No me lo podía creer. Teníamos a Mitnick, y podíamos rastrearlo inmediatamente. Pero cuanto más

tardásemos en hacerlo, más probable era que saliesen mal. “Por eso es que Kevin Mitnick anda suelto todavía, tras su desaparición en 1992 para eludir la búsqueda por parte del FBI”, mascullé.

Fui a la parte trasera de la oficina de la central y llamé de nuevo a Kent para manifestarle mi frustración. “Esto es realmente un desastre”, le dije. “Estoy hasta el gorro de esto”.

Él se estaba acostumbrando a mis enfados y prometió hacer unas llamadas para ver si podía acelerar las cosas. Pero la situación no hacía más que empeorar. Cuando dejé el teléfono empezamos a discutir los detalles

operativos relativos al seguimiento y la detención. El agente especial Thomas me aseguró que los agentes de la ley no tendrían problemas para mantenerse en contacto entre ellos, pues todos ellos llevaban radios con frecuencia alterada.

"No pueden usar esas radios", tuve que explicarle. "Ese individuo no es un delincuente corriente. Trabaja con el escáner puesto".

"No se quedará ni un momento si oye tráfico codificado por los alrededores", intervino Murph, y finalmente la cosa quedó clara.

Eran casi las 10:30 p.m. A pesar de las dudas de los agentes del FBI,

resolvimos que todavía podíamos ir al emplazamiento de la célula y utilizar el equipo de diagnóstico de Sprint para conseguir una localización exacta de Mitnick. Murph sugirió que siguiésemos la pauta de la reciente investigación de fraude telefónico. Cada vez que un teléfono móvil establece una llamada, ésta es asignada a su propia frecuencia. Esa frecuencia era visible para los ingenieros que hacían el seguimiento en el conmutador de la compañía, que por eso habían utilizado un sistema según el cual, cada vez que cambiaba la frecuencia, ellos la enviaban a un busca en poder del técnico de campo. Entonces

el técnico sintonizaba el radiogoniómetro según esa frecuencia. Parecía una buena idea. Era improbable que Mitnick estuviera vigilando las frecuencias celulares y también las de busca. Aun si así fuera, era improbable que le diera importancia a una ocasional llamada de busca de tres dígitos.

Llamamos nuevamente al técnico de Cellular One para que nos ayudase alertándonos cuando se hacían nuevas llamadas. Él estaba vigilando su conmutador desde su casa y podía ver la información del que llamaba y también la del sector. Como había una célula o emplazamiento de antena repetidora de

Cellular One inmediatamente al lado de la célula 19 en el sistema de Sprint, ahora pudimos determinar que las llamadas de Mitnick en el sistema de Cellular One estaban siendo puestas desde un teléfono ubicado en la misma área que las de la noche anterior. ¡Estábamos de suerte!

Las llamadas venían de una zona inmediatamente al sur del transmisor celular, confirmando la previa sospecha de Murph sobre la ubicación de Mitnick. Murph, Joe y yo fuimos a examinar un gran mapa de la zona de Raleigh. El transmisor estaba situado sobre la ruta 70, conocida también por avenida

Glenwood. Directamente hacia el sur se encontraba el cementerio Raleigh Memorial: al este y al sureste estaba el parque estatal William B. Umstead.

Nuestros ojos se dirigieron inmediatamente a Duraleigh Road, que corría casi directamente hacia el sur desde su intersección con Glenwood. Sobre la margen de la Duraleigh que daba al este se extendía aproximadamente un kilómetro un vecindario llamado Duraleigh Woods. Parecía un buen lugar para iniciar la cacería. Murph no estaba seguro sobre la distancia a la que Mitnick se hallaba de la célula, pero trazó un arco con

centro en al emplazamiento de la antena repetidora y dijo que probablemente estuviese dentro de aquella área.

Sobre el asiento trasero de la furgoneta de Joe Orsak había un dispositivo, de aproximadamente el tamaño de un PC de mesa, llamado Cellscope 2000, que en realidad era un transreceptor de radio de aficionado conectado a un ordenador personal portátil. Empleado por las compañías de telefonía móvil para probar la calidad de la señal, podía funcionar también como goniómetro. Orsak tenía asimismo una antena Yagi manual conectada al Cellscope, que podía mantener dentro de

la cabina de la furgoneta. La Yagi no fue diseñada para tareas de detección de señales de radio, pero realizaría una tarea semejante.

El software de Mark Lottor estaba funcionando en mi PC HP100 en combinación con un teléfono celular de bolsillo Oki 1150, un arreglo que realizaba en parte las mismas funciones, pero más económico y ocupando menos espacio. No era direccional, pero para mis fines eso no importaba. En el mundo de la telefonía celular, la conexión que va del punto de partida o base a un teléfono celular se llama canal de ida y la que viene del teléfono al punto base

se llama canal de vuelta. El Cellscope podía rastrear uno u otro canal, pero no los dos simultáneamente. Pero utilizándolo en tándem con mi sistema portátil, podíamos rastrear los dos extremos de una llamada.

Mark y yo habíamos preparado un cable personalizado para conectar el ordenador al teléfono Oki. En su interior había un chip microprocesador que hacía la conversión de la información entre el Oki y el ordenador HP de forma que los dos dispositivos pudieran hablar entre sí. El pequeño chip posee tanta capacidad de procesamiento como los primeros ordenadores personales. Es el

protagonista de una historia que a Dany Hillis le gusta contar a menudo. Durante una conferencia que tuvo lugar por los años setenta en el Hilton de Nueva York, un orador formuló una estimación aparentemente exagerada del número de ordenadores que habría en el mundo de allí a una década. Alguien de la audiencia se puso de pie y dijo: "¡Eso es una locura! Para que eso fuera así, ¡tendría que haber un ordenador en cada puerta!".

Una década más tarde, Hillis volvió al Hilton para otra conferencia, y efectivamente, había un ordenador en cada puerta: ¡en las cerraduras

electrónicas que acababan de instalar en el hotel!

Mientras nos dirigíamos al emplazamiento de la célula me puse a montar mi equipo y a manipular el Cellscope mientras Joe me daba instrucciones sobre su uso. El interceptar llamadas de teléfonos móviles con un dispositivo como ése está prohibido a los particulares por la Ley de Protección de la Intimidad de las Comunicaciones Electrónicas, pero las compañías de telefonía móvil están autorizadas a efectuar rastreos con el fin de detectar e impedir fraudes.

Previendo la posibilidad de un cerco

prolongado, paramos en un Seven-Eleven y yo compré algo de comer y de beber mientras Joe se tomaba un café. El ingeniero de Cellular One informó que Mitnick no estaba activo, de modo que llegamos al emplazamiento de la célula y esperamos. El agente especial Thomas nos había seguido en un llamativo turismo Crown Victoria del FBI. Aparcamos frente al muro de hormigón sin ventanas de una nave oculta tras una cerca alambrada. Dentro estaban los bastidores de transceptores de radio para controlar el tráfico de llamadas en la célula.

Joe y yo salimos a dar una vuelta

con la furgoneta para comprobar el equipo de seguimiento y a reconocer el terreno. Le pedimos al agente especial Thomas que aguardara hasta nuestro regreso, pero cuando volvimos, a los veinte minutos, el Crown Victoria se había ido.

Alrededor de las 11:30 p.m. Markoff me llamó por el busca. Yo lo había llamado desde el aeropuerto en San José antes de partir, y él, que había volado a Raleigh varias horas después, se había alojado en el Sheraton Imperial, próximo al aeropuerto. Le pasé el teléfono a Joe y éste le explicó cómo llegar al local de la célula. Mientras lo

esperábamos, volvimos a salir para ocuparnos del equipo de exploración direccional. Un domingo cerca de medianoche en los suburbios de Raleigh, las cosas están realmente tranquilas en todas las frecuencias de telefonía celular.

Era una fría y serena noche invernal. Joe estaba de pie fuera del vehículo escuchando el Cellscope con la antena Yagi bajo el brazo, y no conseguía detectar tráfico alguno. De pronto captó una llamada en un canal de Cellular One. Prestó atención y enseguida oyó que alguien con marcado acento de Long Island, hablaba de “Phiber Optik”.

“¡Lo tenemos!”, exclamé. “¡Vamos!”.

Phiber Optik era el pirata informático que había estado un año preso y ahora trabajaba como administrador de sistemas para Echo, un servicio on-line de la ciudad de Nueva York.

Nos metimos de un salto en el interior de la furgoneta y salimos rápidamente del sendero de acceso a la calle. Un coche venía lentamente hacia nosotros.

“Apuesto a que es John Markoff”, dije.

Joe hizo parpadear las luces de la

furgoneta, y cuando el coche se detuvo junto a nosotros reconocí a Markoff tras el volante.

"¡Aparque el coche y venga, acabamos de captarlo!", le grité por la ventanilla. Él lo hizo y saltó al asiento trasero. La voz con acento de Long Island salía por el altavoz de la unidad Cellscope. Sólo podíamos escuchar un extremo de la conversación, el que venía de la estación celular base; el teléfono móvil estaba demasiado lejos y era demasiado débil para poder captarlo.

"¡Esa voz la conozco!", exclamó inmediatamente Markoff. "¡Es Eric Corley!".

Yo había oído hablar de él. Como director de *2600* había defendido públicamente a Kevin Mitnick en muchas ocasiones, aduciendo que se trataba de un hacker incomprendido y maltratado que se entrometía en los sistemas por pura curiosidad. Afirmaba que cuando un hacker robaba software no se producían víctimas. Ahora estábamos oyéndole charlar con alguien sobre cómo mejorar su imagen pública.

Unos años antes, *2600* había publicado la refutación del propio Mitnick a *Cyberpunk*, el libro del que Markoff había sido coautor. En la misma aquél argumentaba que su socio Lenny

Di Cicco le había tendido una trampa. Ahora lo que captábamos daba a entender que Corley estaba aconsejando a su interlocutor sobre cómo hacer frente a la persecución por parte de los representantes de la ley. Me pregunté si Corley sabía que Mitnick seguía mintiéndole a la gente, leyendo su correo electrónico y robando su software.

Joe condujo la furgoneta hasta la avenida Glenwood y luego torció a la derecha y avanzó hacia el sur por Duraleigh Road. Al tiempo que conducía ajustó el Cellscope para captar el canal de vuelta y pudimos oír brevemente la

voz al otro extremo de la comunicación. Aunque había hablado con Mitnick años antes por teléfono y una vez le había oído hablar como "consultor" en seguridad informática, Markoff no pudo identificar como suya la segunda voz, de forma concluyente.

Yo estaba vigilando el indicador de potencia de la señal, que de pronto descendió del todo. "Se ha perdido", dije.

Continuamos captando fragmentos hasta que en un momento dado la voz dijo "adiós" a Corley y le preguntó si seguiría levantado a las 5 de la mañana. A partir de ese punto, la llamada se

perdió.

"Tengamos paciencia", me dije. Ahora tenía la convicción de que Mitnick se encontraba en las inmediaciones. Puede que hubiera podido preparar un complejo sistema con un par de modem de datos, pero habría sido mucho más difícil disponer un relé que manejase voz y datos. Joe buscó un lugar para girar en redondo y volvimos lentamente por Duraleigh esperando captar otra llamada.

Cuando nos aproximábamos a la intersección vimos una urbanización relativamente nueva de bloques bajos de apartamentos. A nuestra derecha había

un centro comercial y una gasolinera. Durante la marcha íbamos mirando los mapas especializados de Joe. Parecía posible que la señal proviniese de algún lugar dentro de uno de los apartamentos. Elegimos el más lejano sobre el camino y nos introdujimos en su aparcamiento mientras continuábamos explorando. Era fácil porque no había ninguna otra conversación en la célula. Era casi la una de la mañana.

Ahora nuestros monitores captaron otra llamada mientras estaba siendo establecida. Esta vez oímos el pitido de un modem, lo que significaba que era una llamada de información. Vi en mi

pantalla el MIN, el número telefónico celular, 919-555-6523. Programé rápidamente el monitor para rastrearlo más adelante.

La señal era potente. En algún lugar, a pocos cientos de metros de donde íbamos marchando, se encontraba Kevin Mitnick sentado, probablemente inclinado sobre un ordenador portátil, afanándose en husmear contraseñas, instalar puertas secretas y leer el correo de otras personas. Cada pocos minutos la señal caía, y tras una pausa de unos treinta segundos se iniciaba una nueva llamada.

“Pobre bastardo”, dije. “Está

consiguiendo una recepción celular realmente paupérrima".

Joe regresó a Duraleigh girando al norte e inmediatamente se internó en el camino de acceso de un grupo más grande de apartamentos llamado el Player's Club.

Mientras lo rodeábamos todos empezamos a sentirnos incómodos. El aparcamiento estaba lleno de coches, pero no se veía gente y casi todos los apartamentos exteriores tenía las ventanas sin luz. ¿Qué habría pensado alguien que se asomara a la ventana, al ver a tres hombres en una furgoneta rodeando el aparcamiento a esas horas?

Avanzábamos despacio, en dirección opuesta a la de las manecillas del reloj. En la parte posterior del complejo de apartamentos vimos aquellos que tenían campo abierto a sus espaldas. “Si yo fuese Mitnick tendría planeada mi huida a través de esos campos”, comentó Markoff. “Además, instalaría el ordenador de forma que tuviera una buena visión por la ventana”.

Yo iba girando la antena Tagi mientras nos movíamos. Al entrar en el camino de acceso del Player’s Club había visto aumentar la intensidad de la señal en la pantalla del Cellscope. Habría jurado que Mitnick se encontraba

en algún lugar a nuestra izquierda. Ahora, en la parte de atrás del complejo de apartamentos, la señal decreció. La antena no era demasiado precisa porque yo estaba dentro de la furgoneta con el propósito de no llamar la atención. Estaba intentando además mantener una imagen mental de la dirección de donde provendrían las señales en el espacio real, más bien que en el espacio de la furgoneta, dejando de lado la situación de ésta. Al mismo tiempo, los tres buscábamos una ventana con las luces encendidas.

El Player's Club estaba circundado por hileras de plazas de aparcamiento.

La urbanización en sí parecía un cuadrado del que se proyectaban unas alas laterales separadas por otros aparcamientos. Al aproximarnos a la esquina suroeste del complejo la señal volvió a dar un salto. Era evidente que la llamada venía de una de las extensiones laterales, o bien de una esquina interior de la urbanización.

Resolvimos que circundar nuevamente el complejo sería demasiado arriesgado, de modo que Joe atravesó la calle y aparcó en el solar del centro comercial. Yo estaba convencido de que habíamos localizado a Mitnick y ahora lo único que necesitábamos era al

FBI.

"¿Por qué no volvemos a la sede de la célula a ver si podemos persuadir al FBI para salir otra vez?".

De nuevo en la célula llamé a Murph al conmutador de la oficina central y él llamó al FBI para insistir en que actuasen. Después que le contestaron que no tenían agentes disponibles, llamé yo mismo a la oficina local del Bureau.

"El sujeto está operando ahora mismo", le dije al oficial de guardia. "Es como tener una linterna iluminando el camino hasta la puerta".

"Lo siento", respondió él. "En este momento no hay aquí ningún agente, lo

único que puedo hacer es tomar nota de su mensaje".

Yo colgué y llamé al agente especial Thomas, a quien no le produjo la menor alegría escucharme a las 2:30 de la mañana. "Esta noche me temo que no puedo ayudarle", me explicó. "El hombre está buscado por orden de la policía judicial, no del FBI: no es un problema del FBI".

Me puse a medir a grandes pasos la pequeña habitación para arriba y para abajo. Volví a llamar a Kent, que me prometió que los refuerzos pronto estarían en camino, pero cada vez estaba más claro que esa noche no iba a ocurrir

nada. Aguardamos otros cuarenta y cinco minutos mientras las llamadas informativas de Mitnick iban y venían. Finalmente resolvimos abandonar y regresar al conmutador de la Sprint.

Por el camino pensé en hacer otra llamada a Levord, pero decidí que emplear el teléfono móvil era demasiado riesgo. Probablemente, estábamos fuera del alcance del escáner, pero si Mitnick estuviera utilizando software robado a Mark Lottor tendría acceso al canal de control de ida, y podría ver aparecer mi número en el sistema en Raleigh. Era sumamente improbable, pero ése era el tipo de

cosas que pueden causarte un tropiezo.

Joe me dejó y yo monté en mi coche para seguir a Markoff al Sheraton. Entramos en el vestíbulo desierto a las 4 de la mañana. Yo había tenido la esperanza de que Mitnick fuera detenido esa noche, y ahora me preocupaba la posibilidad de que el nuevo retraso le permitiera escurrirse.

16. El cerco

Julia dio conmigo.

Había llegado las 8:30 de la mañana al Sheraton, en cuya recepción yo había dejado instrucciones para que cuando ella se presentase le proporcionaran una llave. Yo dormía cuando entró sin hacer ruido en mi habitación de la cuarta planta, pero me sentí muy feliz al ser despertado suavemente por ella. Estaba exhausto, pero encantado de verla, y nos abrazamos.

“¿Descubriste algo anoche?”, me preguntó.

Le conté que casi con seguridad habíamos encontrado a Kevin, pero al relatarle con detalle nuestra investigación, mi frustración con el FBI no tardó en reaparecer. “Es increíble”, dije. “Esos tipos van a permitir otra vez que se les escurra de entre los dedos”.

Pero vi que también Julia estaba agotada. “¿Qué tal el fin de semana?”, le pregunté.

“Sorprendentemente, como la seda”, murmuró. “Hacía muchísimo tiempo que no nos comunicábamos de una forma tan clara”. Hizo una pausa. “Fue realmente

duro", continuó por fin, "pero estuvimos de acuerdo en que la separación es lo más razonable".

Se metió en la cama y no tardamos en quedar los dos profundamente dormidos.

Dos horas más tarde, cuando desperté, mi mente volvió inmediatamente al caso y me puse a hacer llamadas telefónicas.

La primera fue a Washington, con Levord Burns, que me dijo que planeaba venir a Raleigh más tarde ese mismo día. "Por fin, pensé, el FBI entra en acción". Le pregunté si pensaba contar con un equipo que pudiera vigilar el

complejo de apartamentos.

"No, Tsutomu, soy yo solo", replicó, en el tono de quien se mueve a su aire sin preocuparse de lo que ocurre a su alrededor. "Partiré dentro de dos o tres horas".

Su aparente desinterés me resultaba sencillamente inaceptable. En realidad consideraba a Levord no tanto como un problema, sino como un síntoma de la actitud cansina del FBI, de modo que en cuanto colgó resolví llevar mis quejas a un nivel más alto.

Kent Walker, en San Francisco, me aseguró una vez más que seguía en el caso y que la ayuda estaba en camino.

Yo diría que él también estaba impaciente con la lentitud de esta cacería ahora que nos hallábamos tan cerca del objetivo. Dijo que hablaría con John Bowler, un ayudante de la oficina del procurador general en Raleigh, para ver si podía interesarse en el caso, y también me prometió presionar al FBI, aunque ambos sabíamos que no podía hacer demasiado desde el otro extremo del país.

A continuación telefoneé a Marty Stansell-Gamm, la fiscal del Departamento de Justicia que se había mostrado tan bien dispuesta en la conferencia CMAD en Sonoma, y la

puse en antecedentes. “¡Éste es precisamente el principal motivo por el cual nunca me molesté en acudir al FBI!”, terminé diciendo.

“¿Con quién ha estado tratando?”, preguntó ella.

“Con Levord Burns”.

“Oh, le comprendo”, dijo, “siempre que se habla con él da la impresión de estar medio dormido”.

“Tal vez sea porque siempre le estamos despertando en mitad de la noche”, contesté. Le conté que nuestra necesidad más perentoria era contar con un equipo Triggerfish en el lugar para poder determinar precisamente la

ubicación de Mitnick. Marty me aseguró que haría lo que pudiese.

Julia se había levantado, recuperada sólo en parte de su noche de viaje, pero tan hambrienta como yo. A eso de las 2 bajamos a reunimos con Markoff en el restaurante del Sheraton. No tenía pinta de ser el más incitante lugar para comer, pero como estábamos a menos de cinco kilómetros del apartamento de Kevin Mitnick, y habiendo salido mi foto en todos los periódicos y revistas del país, no podía arriesgarme a ir a un sitio donde él pudiera verme. Y puesto que la foto de Markoff había aparecido en la solapa de *Cyberpunk*, había motivo para

suponer que Mitnick pudiese reconocerlo también a él. De la poco inspirada carta, Julia escogió un sandwich de pan blanco, yo me arriesgué con un queso a la parrilla y lo que pareció ser una sopa de verduras sacada directamente de la lata, y Markoff se las arregló con un sandwich de pechuga de pollo. Él estaba más ansioso de administrarse su dosis diaria de noticias repasando el *Times* y *The Wall Street Journal* que en la comida. Julia y yo estábamos mordisqueando la nuestra y charlando distraídamente, cuando sonó mi busca. Era Mark Seiden en Internex.

“¿Qué pasa?”, preguntó Seiden cuando lo llamé desde la cabina telefónica del vestíbulo. “La limpieza está terminada de este lado, pero parece que Mitnick todavía anda suelto”.

“¿Cómo?”, atiné a decir.

Seiden me explicó que la noche anterior lo había llamado Andrew diciéndole que, puesto que Mitnick estaba a punto de ser aprehendido, él tenía que empezar a limpiar y asegurar los ordenadores de Internex.

“¡Joder!”, exploté. “El FBI no está todavía ni cerca de agarrar a Kevin. ¿Y si lo espantamos?”.

Daba la impresión de que ya lo

habíamos hecho. Seiden contó que después de haber realizado concienzudamente una operación de clausura de las puertas secretas de Mitnick, Kevin había retornado por una que a Mark se le había pasado y había empezado a hacer travesuras, incluyendo un intento de excluir a Seiden de su propia cuenta. Después, en lo que tenía visos de ser una provocación deliberada, había depositado un archivo de 140 megabytes llamado *japboy* que era una copia de un archivo mío con el que Bruce Koball había tropezado hacía unas semanas en la Well.

"No tengo idea de por qué Andrew

le dijo que empezara a limpiar", dije yo, incrédulo.

Seiden, que es un profesional de la seguridad informática, estaba irritado por haber sido inducido a cometer un error. "Es la última vez que recibo órdenes de Andrew", masculló. Convinimos en que ahora su tarea era reanudar la vigilancia de las actividades de Mitnick en Internex para calcular el alcance actual de sus sospechas. Seiden continuaba indignado cuando terminamos la conversación.

Yo marqué el número de Andrew. "¿Qué demonios está pasando?"

"Lo siento, la jodí", dijo Andrew,

que supo inmediatamente de qué le estaba hablando. Se daba cuenta de que había entendido mal mi mensaje cuando yo lo había llamado la noche anterior, y de que se había precipitado con Seiden. Era una caso de exceso de cansancio y optimismo exagerado.

"Mira", le dije, "estamos realmente cerca de coger a Mitnick, pero aún no lo hemos cogido, y puede que ahora hayamos estropeado todo el asunto". Le indiqué que se pusiera a vigilar la Netcom en busca de señales de que Mitnick hubiera detectado nuestras operaciones allí, y que más tarde me informara.

Cuando volví a la mesa del restaurante meneando la cabeza, le conté a Julia y a Markoff lo que había ocurrido. “Es una lástima una metedura de pata como ésta estando tan cerca”, comenté.

Podría resultar que localizar a Mitnick, al parecer, hubiera sido mucho más sencillo que cogerle efectivamente.

Con varias horas todavía pendientes para la llegada de Levord, regresamos a nuestras habitaciones, donde Julia volvió a dormirse, mientras yo empezaba a utilizar el teléfono acuciado por una renovada sensación de urgencia.

Mis esfuerzos no tardaron en ser recompensados con una buena noticia: Marty Stansell-Gamm me dijo que la División de Servicios Técnicos del FBI en Quantico estaba despachando un equipo de vigilancia formado por dos hombres con una unidad Triggerfish de localización de ondas, que llegaría a Raleigh esa noche. Me dio el número del SkyPager de uno de los agentes, y al poco rato me puse en comunicación con él y su compañero.

Como suele ser el caso con los técnicos especialistas de la autoridad, los dos agentes estaban más interesados en formular preguntas que en

contestarlas. Intentaban determinar qué elementos llevar consigo, y una de las cosas que quisieron saber fue si las células de Cellular One o de Sprint soportaban NAMPS, una tecnología analógica de telefonía móvil capaz de duplicar la capacidad de una célula sede estrechando la banda de frecuencia que utiliza cada teléfono. Las empresas celulares que emplean NAMPS suelen compensar al usuario con tarifas menores como contribución al mantenimiento del espectro de frecuencia, pero la utilización del sistema requiere un teléfono especial, y su comprobación regular exige un

equipamiento especial del que ellas carecen. Le dije al agente que Joe Orsak había desconectado NAMPS en la célula 19 la noche anterior y que yo creía que la sede de Cellular One no contaba con esa tecnología. Antes de colgar los puse en comunicación con la gente de Sprint, que podría proporcionarles información más detallada sobre las células base con las que iban a encontrarse.

Poco después de las 5 de la tarde hablé con Levord, que acababa de llegar a la oficina del FBI en Raleigh. Estaba intentando encontrar alojamiento para él y el equipo de Quantico, de cuya inminente llegada se había enterado, y

parecía irritado por tener que hacer de agente de viajes.

"¿Por qué tiene que encargarse de eso usted, Levord?", dije para expresarle mi comprensión.

Él no me contestó.

Sin revelarle que un error cometido por nosotros era el motivo de que me sintiese más nervioso que nunca, le manifesté mi impresión de que, si iba a haber un asedio y una detención, necesitaríamos un equipo de agentes mucho más numeroso.

"No vamos a tener más agentes esta noche", declaró, como quien dice algo obvio.

“Vea, *tenemos* que estar listos para movernos esta noche”, argüí yo, pero él no parecía dispuesto a hacer nada a menos que la situación estuviese bajo su control. No obstante, convinimos en reunimos a las 8 en la oficina de conmutación de la Sprint, donde podríamos recoger a Murph y a Orsak e ir a cenar por allí cerca mientras esperábamos a los dos agentes de Quantico.

A las 7:30, cuando Julia y yo nos disponíamos a abandonar el hotel, llamó Seiden, que parecía preocupado. Hacía menos de una hora, Mitnick había vuelto a Internex, y era evidente que sabía que

se tramaba algo. “Parece que ha agregado una cuenta llamada Nancy, ha borrado Bob y ha cambiado un montón de contraseñas, incluyendo la mía y la de raíz”, dijo Seiden. “Parece una venganza. Se está poniendo destructivo”. Y, en un despliegue de malicia, Mitnick había hecho accesible a cualquiera la cuenta de Markoff en Internet.

Cuando llamé a Andrew para comprobarlo, me dijo que él también había observado la sesión de Mitnick en Internex, y que su actitud denotaba un claro recelo. Después de abandonar Internex, Mitnick había ido a comprobar su puerta trasera en Netcomsv, que John

Hoffman había clausurado el viernes. Era sólo una de las diversas formas de entrada de Mitnick en Netcom, pero al encontrarla cerrada se había puesto verdaderamente en guardia.

Su siguiente paso, según Andrew, fue dirigirse directamente a otra dirección de Internet que no le habíamos visto utilizar antes, operado por la Community News Service en Colorado Springs, donde tenía guardada una copia de test1. Ése era el programa que le permitía utilizar Netcom como base de operaciones sin dejar rastro. Al parecer Mitnick recuperó aquella nueva copia de test1 para compararla con la que ya

había escondido en Netcom, presumiblemente para ver si nosotros habíamos alterado la versión para que ya no pudiera ocultar sus huellas. Comparando ambas copias, encontró la versión de Netcom intacta. Estaba usando una cuenta llamada Wendy, con una contraseña "fuckjkt".

"¿Quién es jkt?", preguntó Andrew.

"No tengo ni idea", dije en tono impaciente.

Andrew describió seguidamente una serie de acciones que en Mitnick eran de rutina, lo cual nos indicó que una vez que hubo verificado que su copia de test1 no había sido alterada, empezó a

tranquilizarse, quizá por llegar a la conclusión de que lo de la puerta secreta clausurada era una casualidad, sin relación alguna con sus problemas en Internex. Al menos eso esperábamos: a aquella altura de la partida se estaba volviendo difícil decir qué era calculado y qué era mera coincidencia. Unos minutos después, Mitnick había retornado a Internex y Andrew abandonó la vigilancia. Seguro que estaba tratando de ver si había sido detectado, y en tal caso, dónde.

"Sigue en actividad, así que está bien", le dije a Andrew. "Pero tiene sospechas. Eso es precisamente lo que

menos falta nos hace. Después de haber conseguido traer aquí al equipo con el Triggerfish, sería verdaderamente engorroso que él estuviera una semana sin presentarse".

Markoff tenía dudas sobre si acompañarnos a Julia y a mí a la oficina de Sprint. Estaba seguro de que cuando los del FBI descubrieran en la escena a un periodista del *New York Times* se pondrían quisquillosos.

"No te preocupes", le dije. "Diles sólo que eres de nuestro equipo".

"De ninguna manera voy a mentirles", replicó él. "Ese tipo de

cosas siempre te explota en la cara". Pero no estaba dispuesto a perder su reportaje, así que decidió venir con nosotros, aunque en su propio coche por si en algún momento tenía que largarse.

Mientras iba con Julia en mi Geo Metro alquilado, recibí un mensaje en el busca desde un número local que no reconocí. Cuando llamé, descubrí que era el teléfono privado de John Bowler, el fiscal adjunto a quien Kent Walker había prometido llamar.

"Kent dice que necesita usted ayuda", dijo Bowler. "¿En qué puedo serle útil?".

"Estoy en un teléfono móvil", le

advertí.

"Ah, vale".

"Hay alguien que viene de Washington", dije.

"Dígale que me llame", replicó Bowler, y rápidamente cortamos.

Joe Orsak y Murph nos estaban esperando en la oficina de Sprint con un tercer técnico que era todavía más grande que ellos: Fred Backhaus, un hombre fornido con la barba descuidada, el cabello recogido en una cola de caballo y chaleco de motociclista. A pesar de su aspecto de Ángel del Infierno, resultó ser tan afable y amistoso como los otros, y los tres

estaban ansiosos por participar en la cacería. Hablamos un rato de teléfonos móviles, hasta que llegó Levord Burns.

El agente especial Burns era un negro atlético con un corte de pelo militar, y a mi juicio al final de la treintena. El bien cortado traje gris, la camisa blanca bien planchada, el reloj tipo Rolex y los zapatos negros de ejecutivo no le habrían dejado fuera de lugar en Wall Street. Pero el gran Ford Crown Victoria, con su ominosa antena de látigo, era inconfundiblemente un coche policial: un coche policial con matrícula de Virginia. "Cuidado, Kevin, pensé, los Federales andan por la

ciudad".

Los tres ingenieros y yo nos presentamos, y yo le di a Levord el mensaje de que llamase a John Bowler a la oficina local del fiscal. Él asintió con aire indiferente, no muy feliz de tener todavía otra persona a quien rendir cuentas.

Burns nos dijo que sus jefes en Washington le habían ordenado traer un juego de teléfonos Clipper, el nuevo dispositivo estándar del Gobierno para mantener una conversación codificada digitalmente a través de una línea telefónica normal. Estaban en el maletero del coche. "En rigor, son

inútiles a menos que se hable con alguien que tenga uno al otro extremo de la línea", dijo, con una mueca de fastidio.

"El maletero es un buen sitio donde dejarlos", asentí. Después de todo, podía resultar que Levord fuese un buen tipo.

Antes de abandonar el aparcamiento de la Sprint se lo presenté a Julia y a Markoff, empleando únicamente sus nombres de pila. Levord no hizo preguntas, y yo prescindí de explicaciones.

Fuimos en tres coches a Ragazzi's, un restaurante italiano a unos dos

kilómetros del conmutador de Sprint. Cuando nos sentamos todos a una larga mesa, noté que Markoff elegía el asiento más alejado del agente especial Burns.

El restaurante estaba adornado con botellas de Chianti y ristras de ajo, pero las paneras eran de plástico. Y en tanto que los palitos de pan eran frescos, la ensalada resultó ser estrictamente congelada. Durante la cena Levord comentó que el FBI en esos momentos rastreaba de forma rutinaria las llamadas de teléfono móvil durante las investigaciones. Reconoció que habitualmente vigilaban a personas que no sabían nada sobre la tecnología que

ellos estaban utilizando, y no a tipos que lo sabían todo sobre la telefonía móvil, como Kevin Mitnick. Oyéndole hablar de su trabajo, quedaba claro que Levord Burns era un tío abrumado por sus ocupaciones. "Este tipo de viajes implica bastante presión sobre la vida familiar. Mi esposa está embarazada, y a mí no se me ve mucho por casa".

Los de Sprint lo imitaron hablándonos de su trabajo y nos dieron más detalles sobre las llamadas fraudulentas que habían desmantelado. La redada había tenido lugar en la vivienda de una granja cuyo salón no tenía muebles, sino un montón de

teléfonos celulares por el suelo. La conversación derivó hacia el fraude telefónico en general, y Markoff hizo un relato de parte de la historia de Kevin en la manipulación del sistema telefónico, y de cómo lo habían visto por última vez saliendo a la carrera de una tienda de fotocopias en Los Ángeles.

En un momento dado, Levord fue a una cabina telefónica a responder a varias llamadas de su busca. En su ausencia pasamos al tema de la capacidad de Mitnick para sonsacar información, y yo traje a colación su intento de hacerlo conmigo en Los Álamos.

“Nosotros tuvimos un problema como ése en el último par de semanas”, dijo Murph, sorprendido. “Alguien llamó a uno de nuestros encargados de mercadotecnia fingiéndose empleado de Sprint y consiguió sonsacarle varios pares MIN-ESN”.

“¿No recuerdas qué nombre dio el tío?”.

Murph se volvió hacia Joe. “¿Te acuerdas tú?” Ninguno de los dos lo recordaba.

“¿Sería Brian Reid?”, aventuré.

“Ajá, ése era”, dijo Joe.

“¡Kevin!”, exclamamos al unísono Markoff y yo.

¡Qué apego a los hábitos, seguir utilizando el mismo nombre que había empleado conmigo varios años antes! El verdadero Brian Reid era ahora un directivo de la DEC en el negocio de las conexiones de redes de Internet.

Los técnicos de la Sprint quedaron visiblemente afectados al enterarse de que Kevin había robado información de su empresa. No era culpa suya, pero para ellos constituía una cuestión de honor estar a cargo de una empresa segura, y les irritaba el error de un colega.

Cuanto más se centraba en Mitnick la conversación, más nervioso me ponía

yo. Si nuestra seguridad operativa fuera buena, no habríamos estado sosteniendo una conversación como aquella en un restaurante público. Miré detrás de mí y vi en un reservado próximo a una pareja con aspecto de americanos corrientes visiblemente interesada en nosotros. Eso aumentó mi inquietud. Empecé a hacerles preguntas técnicas a los de la Sprint, para encaminar la charla en otra dirección.

Hacía menos de veinte minutos que habíamos vuelto de la cena cuando por fin el equipo de dos hombres de Quantico se presentó en la oficina de la

central, conduciendo una vieja camioneta cargada de equipo.

Más que Hombres G, se parecían a Simon y Garfunkel. Uno era alto, de complexión más bien liviana, y el otro era bajo, con la nariz y las orejas carnosas. Ambos parecían andar por los cuarenta, tenían una pinta ligeramente descuidada —de académico rural, con algo de caballerizo—, y el bajo llevaba el tipo de gorra preferido por los británicos que conducen coches deportivos.

Una vez efectuadas las presentaciones, resolvimos que el mejor plan sería utilizar la furgoneta familiar

blanca de Fred Backhaus para transportar al equipo y sus elementos de búsqueda direccional. Cuando ellos empezaron a descargar la camioneta, Levord fue a cambiarse a la sala de descanso, de la que salió con ropa de trabajo y con gorra de béisbol, un atuendo que le hacía parecer un pintor de casas, aunque un pintor algo grueso de cintura, gracias a la faja protectora que llevaba debajo.

Yo me ofrecí para ir con ellos, pues ninguno de los dos tenía la menor idea de cómo era realmente el terreno. Levord me miró con atención, y en su estilo lento e inexpresivo, dijo:

“Tsutomu, no cabe en forma alguna que venga con nosotros. Su foto ha aparecido por todas partes. Si él lo ve y lo reconoce, desaparecerá”.

Yo insistí. “Vean”, argumenté, aun sabiendo que no me estaba haciendo simpático con ninguno de ellos, “tengo que ir con ustedes. Hemos prometido a un montón de gente del mundo informático que velaríamos por ellos. Nadie sabe cómo podría reaccionar Mitnick. Si hace alguna faena antes de que ustedes lo cojan, necesito ver qué hay en su ordenador para poder decirle a mi gente cómo contrarrestarlo. Hasta ese momento puedo mantenerme al

margen".

Levord no se inmutó. "Esta noche no va a pasar nada". Capté el mensaje de que no iba a quererme cerca aun cuando creyese que algo pasaría. Sospeché que toda aquella tecnología que no entendía lo intimidaba, además de no querer llevarse la culpa si yo me asustaba en una persecución o un tiroteo.

Los del equipo de Quantico sí me hablaron un poco sobre la tecnología que habían traído en la camioneta, en particular sobre algo llamado un simulador de emplazamiento de célula, que estaba embalado en un gran baúl de viaje. El simulador era un dispositivo

utilizado normalmente por los técnicos para comprobar el funcionamiento de los teléfonos móviles, pero también podía emplearse para llamar al teléfono celular de Mitnick sin hacerlo sonar, siempre que lo tuviese encendido pero no efectivamente en uso. El teléfono actuaría entonces como un transmisor que ellos podrían localizar con la antena direccional Triggerfish.

Por ingeniosa que sonara la técnica, yo señalé que sería arriesgado utilizarla con Mitnick. “Están ustedes tratando con alguien que posee el código fuente para toda clase de teléfonos celulares”, dije. “Podría detectarlo”.

Ellos concedieron que podría no valer la pena arriesgarse, aunque añadiendo sin enunciarlo un "Vete de aquí, chaval, que estás molestando". No creo que les gustase la idea de tratar con un civil, especialmente con uno que estaba en condiciones de entender de todo lo relacionado con sus técnicas.

En ese momento Backhaus ya había arrimado la parte posterior de la furgoneta a la puerta principal del edificio de la Sprint, y los agentes iniciaron un ir y venir entre la camioneta y la furgoneta, instalando su equipo. El localizador direccional Triggerfish, una caja rectangular de elementos

electrónicos de cerca de medio metro de alto, controlado por un ordenador portátil Macintosh Powerbook, fue colocado en el centro del asiento trasero de la furgoneta. Por uno de los agentes, que estaba instalado en la furgoneta calibrando la unidad, logré saber que Triggerfish era un receptor de cinco canales, capaz de controlar simultáneamente ambos extremos de una conversación. A continuación tendieron un cable coaxial negro entre la ventanilla de la furgoneta y la antena direccional que habían colocado en el techo. Ésta constaba de una base negra de unos 30 centímetros cuadrados y

varios de espesor, que sostenía cuatro extensas astas de antena plateadas, cada una de las cuales se alzaba hasta cerca de 30 centímetros hacia el cielo.

Aquel aparato no parecía en absoluto disimulable, y yo hice notar nuevamente que no se enfrentaban a un vendedor de cocaína técnicamente analfabeto. "Este individuo es desconfiado, y se sabe que ha utilizado escáners para detectar a la policía antes de ahora", dije. "Ha interceptado incluso las comunicaciones del FBI".

Ahora no querían hablar conmigo para nada, pero yo no iba a ceder. "No, esto es ridículo", dije. "Ustedes van a

aparcar allí fuera, y el tío no es estúpido. Estoy seguro de que sabe qué aspecto tiene una antena direccional".

No se convencieron. "No es tan visible", replicó el más bajo.

Lo miré con tristeza. "¿No pueden ponerla adentro?".

"No, eso perjudicaría el rendimiento", dijo el más alto.

"¿Por qué no la cubrimos con una caja?", sugirió Murph.

"No, eso sería demasiado evidente", dijo el otro.

Miré otra vez al techo de la furgoneta, que tenía dos barras paralelas que iban de un costado al otro, a la

manera de una baca. Lo que necesitábamos era una caja que pareciese hecha para ser transportada allí.

"Un momento", les dije. "Murph, tú tienes tubos fluorescentes. ¿Te queda alguna de esas cajas en las que vienen?".

Tuvimos suerte, estaban en un armario del cuarto de recambios frente a la sala principal del centro de conmutación. Regresamos con una caja de dos metros y medio de largo que se podía amarrar a lo alto de la furgoneta. Le hice un agujero para que pudiera colocarse encima de la antena,

ocultándola por completo en caso de que Mitnick estuviera en un apartamento de la planta superior y pudiese ver la furgoneta desde arriba.

Cuando terminamos el arreglo, la furgoneta parecía el irreprochable vehículo de un electricista. Yo estaba seguro de que los agentes habían aceptado lo del camuflaje sobre todo para contentarme, pero tuvieron que admitir que el disfraz funcionaba estupendamente.

Era cerca de medianoche cuando los tres agentes del FBI estuvieron preparados para salir.

"¿Y qué hacemos si le vemos fuera

del apartamento?", preguntó uno de los del equipo de Quantico. Parecía posible que Mitnick frecuentase las tiendas del centro comercial que quedaba enfrente de los apartamentos. "¿Le cogemos?".

"Es un violador de la libertad condicional, de modo que podemos detenerle", dijo Levord, "pero ¿alguno de ustedes lo reconocería al verle?". Las fotos que teníamos todos eran viejas, y los documentos del FBI indicaban que su peso había variado.

Resolvimos que parecía improbable que esa noche fueran más allá de identificar cuál era su apartamento, de modo que el equipo de Quantico partió

con Orsak y Backhaus, mientras Joe y Levord los seguían en mi alquilado Geo verde, que les pareció el vehículo menos sospechoso de nuestra flota. Levord dijo que harían un rápido reconocimiento y regresarían enseguida.

Mientras esperábamos, Murph nos llevó a recorrer la central, una construcción sin ventanas llena de elementos muy semejantes a las unidades centrales de proceso de los ordenadores, estanterías con baterías del tamaño de impresoras y equipo generador de emergencia. Después nos pusimos a esperar, primero contando los minutos y después, con ansiedad

creciente, las horas.

Una pequeña cantina frente al centro de operaciones principal nos proporcionó un lugar donde sentamos, y matamos el tiempo comiendo galletitas y bebiendo refrescos de una pequeña nevera. Un cartelito escrito a mano indicaba los precios de las distintas bebidas, incluyendo Gatorade, del cual desgraciadamente no quedaba. El pago se basaba en la confianza, y el gran tarro que habían colocado a ese fin se fue llenando lentamente con nuestros dólares. Para mantenerme ocupado, me leí todas las notas importantes del boletín mural, incluido un recorte de

periódico sobre el desmantelamiento del locutorio telefónico celular en la granja en el que habían intervenido Murph y Joe.

Markoff y Julia empezaron a jugar con el HP 100 que formaba parte de mi terminal RadioMail. En cierto momento Markoff puso en marcha un programa destinado a editar iconos para el interfaz del usuario del dispositivo, lo cual no se sabe cómo hizo que el ordenador dejase de repente de funcionar, corrompiendo todo mi software de comunicaciones inalámbricas.

Grrrrr.

Markoff se disculpó profusamente,

pero el sistema de comunicaciones del ordenador estaba completamente muerto. Recordé que todos los archivos de seguridad estaban a salvo en San Diego, donde ahora no me servían de mucho, y eso me trajo a la memoria una cita que leí una vez, de alguien que no recuerdo: "El destino se enamora del que es eficiente".

Mitnick no estaba utilizando el sistema Sprint. Y si bien podíamos descubrir si estaba activo en Cellular One mediante periódicas llamadas a Gary Whitman, un ingeniero de esa empresa que vigilaba el emplazamiento celular desde la base, en cambio no

podíamos seguir las llamadas de Mitnick tan de cerca como habríamos podido si fueran procesadas a través del conmutador del edificio en el cual estábamos instalados.

A eso de las 3 de la mañana envié un mensaje al busca de Joe Orsak. Me llamó rápidamente pero no pudo decirme gran cosa, aparte de que estaba llamando desde una de las cabinas públicas en el centro comercial que estaba en Duraleigh Road frente al complejo de apartamentos.

Le pedí que hiciera venir al teléfono a uno de los agentes del FBI. Al cabo de un par de minutos se puso uno de ellos y,

sin esperar a oír qué quería yo, preguntó furioso: "¿Quién es ese tipo de nombre John que está con usted?".

"Es un escritor", le expliqué.

"¿Qué escribe?".

"Es un escritor. Escribe libros".

"¿Escribe alguna otra cosa?".

"Montones". Pensé que comprendía su problema: se vería en un grave aprieto ante sus superiores si hubiera dejado a sabiendas que un reportero de periódico observase las actividades del equipo. Yo intentaba proporcionarle la opción de una negativa creíble, pero él insistía.

"No será John Markoff, el reportero

del *New York Times*, ¿verdad?".

"Sí, es él", tuve que admitir.

"¿Y fue el que escribió ese libro sobre los hackers?

"Sí. *Cyberpunk*. El libro sobre Kevin Mitnick. Es nuestro experto en Mitnick".

Ahora estaba realmente furioso. "¿Y por qué está aquí? ¿Por qué ha venido?", preguntó. "¡Está usted poniendo en peligro la operación! ¡Los periodistas no están autorizados para intervenir en las actividades del FBI! ¡Usted me mintió!".

"No", respondí. "No le mentí. Usted no me preguntó quién era".

Mi explicación no lo satisfizo, y colgó.

Markoff había oído la conversación a mi lado y decidió que era el momento de emprender una rápida y elegante retirada. La noche anterior había dejado absolutamente en claro su identidad ante Murph y Joe, incluso habían intercambiado tarjetas profesionales, y al parecer uno de ellos se lo había mencionado a los del FBI.

"No quiero que me pesquen en medio de esto y tener que explicarle mi presencia a un agente del FBI", dijo Markoff antes de partir hacia el Sheraton.

Cuarenta y cinco minutos más tarde, a eso de las 5 de la mañana, Levord Burns regresó con Joe Orsak.

Levord, esta vez sin su habitual lentitud, entró como una tromba y se encaró conmigo en cuanto me vio. "Vea, usted me ha estado haciendo perder el tiempo, y ahora descubro que tiene a ese reportero del *New York Times* siguiéndonos. ¿Qué significa esto?".

"Vamos a hablar", dije. Vi que tenía que bajarle los humos a Levord y pensé que no le haría ningún favor arremeter contra mí delante de Murph, Joe y Julia. Le hice una seña indicándole el depósito de materiales.

Cerramos la puerta detrás nuestro y Levord se puso a medir la habitación a grandes pasos. “¿Qué se propone?”, dijo. “¿Cuál es su programa?”.

Le dije que no estaba intentando lograr notoriedad trayendo conmigo a un periodista, sino que simplemente me apoyaba en un amigo de confianza, que hacía años que escribía sobre Mitnick y tenía un cierto conocimiento de sus hábitos y motivaciones.

Estaba claro que yo había chocado con la obsesión del FBI por la seguridad operacional, compartida por Levord, quien me hizo saber que a los agentes de Quantico les aterrorizaba que los

secretos de sus procedimientos de seguimiento y vigilancia fueran a aparecer en un artículo del *New York Times*. Ellos iban a tener que informar del encuentro a sus superiores, y eso no les hacía ninguna gracia. Aunque parecía exhausto, Burns me dio una conferencia de veinte minutos sobre los protocolos específicos del Bureau acerca de las relaciones con la prensa, y dijo que muchos habían sido violados por nosotros.

"¿No irá Markoff a advertir a Mitnick, para que pueda escapar y así él tener un reportaje mejor?".

"Ni hablar", le aseguré. Era obvio

que, como periodista, Markoff estaba aquí porque iba a haber material para un buen reportaje, pero el mejor posible sería el del apresamiento de Mitnick. De modo que los intereses de Markoff y de Levord eran del todo coincidentes, y así se lo expliqué a este último.

"¿Por qué no me lo presentó como periodista? ¿Por qué no jugó limpio conmigo?".

"Usted no me lo preguntó", repliqué.

"¿Dónde está él ahora?".

"Se volvió al hotel".

Finalmente, cuando la irritación de Levord pareció haber amainado, le pregunté si había localizado la

ubicación de Mitnick.

"Estamos cerca", dijo con aspereza, "pero aún no hemos situado el apartamento con precisión". Los agentes de Quantico lo seguían intentando.

Yo estaba bastante seguro de que aunque todavía le habría gustado echarme, Levord probablemente sabía que en ese momento era cuando más me necesitaba. Iba a tener que confeccionar un atestado para la orden de arresto. Y eso requeriría buena parte de la información que nosotros habíamos reunido hasta el momento, que él no tenía forma de interpretar sin mi ayuda.

Con eso in mente, se la ofrecí.

“Vale”, dijo él, “pero no más sorpresas… ¿de acuerdo?”.

Yo asentí con la cabeza, y seguidamente sugerí la clase de datos que podía reunir para él en orden correlativo: los registros de entrada en Netcom, las grabaciones de la compañía de telefonía celular y las propias sesiones de Mitnick recogidas en nuestro seguimiento electrónico. El cruce entre aquellos datos demostraría irrefutablemente que Mitnick era nuestro hombre. Llamé a Andrew y le pedí que me enviara por fax otras partes del material necesario.

Cuando Levord y yo nos dirigíamos

a la cantina, apareció Julia, vio que al parecer habíamos alcanzado un cese del fuego, y se encaminó al depósito de materiales a echar una cabezada.

"Disculpen", dijo. "Necesito dormir un poco".

Al poco rato el material complementario de Andrew empezó a salir por la máquina de fax. Pasé la siguiente hora y media seleccionando datos, mientras que Levord estuvo casi todo el tiempo al teléfono poniendo en antecedentes a diversos funcionarios del Bureau para que tomasen las disposiciones necesarias en cuanto a apoyo y refuerzos.

Elaboré un listado de treinta sesiones distintas, ocurridas entre la tarde del 9 y la madrugada del 13 de febrero, sobre las que podíamos cotejar las horas de los registros de entrada de Netcom con los registros detallados de las llamadas proporcionados por Cellular One o Sprint. De aquéllas seleccioné unas cuantas para Levord, y empecé a explicarle la correspondencia entre los registros de llamadas telefónicas y las sesiones en Netcom, y lo que las propias pulsaciones del teclado por parte de Kevin para cada sesión nos revelaban acerca de sus actividades. Para cualquiera sin una

buena base de conocimientos sobre redes telefónicas y comandos de Internet y Unix, era una cantidad abrumadora de información que digerir; habida cuenta las relaciones entre Levord y yo en aquel momento, el proceso resultaba particularmente penoso. Pero Julia no tardó en despertarse y hacerse cargo de la tarea, demostrando ser un instructor mucho más paciente.

Cuando terminaron, ella y yo salimos a tomar un poco de aire fresco, después de una noche entera en aquel agujero con luz fluorescente y sin ventanas. Me sorprendí: estaba claro, el cielo lucía plomizo y encapotado, pero

de todas formas era de mañana, casi las 8.

De nuevo adentro, llamé a Andrew y a Robert Hood, que seguían aún esperando en la Netcom que ocurriese algo y no parecían muy contentos. Les comuniqué que Levord decía que probablemente antes de mediodía, tiempo del este, tan pronto como su exposición y las órdenes de arresto y allanamiento estuvieran listas, el FBI cogería a Kevin. Les aseguré que las señales de "atención" y "adelante" podían llegarles en las próximas horas.

Poco después regresaron los dos agentes de Quantico, con el aspecto de

agotamiento de dos hombres de mediana edad que han pasado la noche en vela. Me miraron con inquina, pero ni ellos ni yo teníamos energías para ponemos a discutir sobre Markoff. Acababan de ser relevados por agentes de la oficina de Raleigh y sólo querían irse al hotel a dormir un poco mientras Levord se encargaba del papeleo. Éste iba a ir a la oficina del Bureau en el centro, y como la operación no había conseguido aún dar con el apartamento buscado, quería que alguien fuera al complejo a realizar una discreta vigilancia a pie, al viejo estilo. Le hice prometer a Levord que se pondría en comunicación conmigo antes

de efectuar la detención. No creía que fuera a hacerlo, pero continué subrayando la vulnerabilidad de la Well, la Netcom y otras y mi necesidad de alertar a su gente.

Con la llegada del reducido grupo de trabajadores que cumplía el turno de día, el centro de conmutación de telefonía móvil estaba empezando a cobrar vida. Julia y yo nos volvimos al Sheraton en el Geo, y ella me hizo notar que era 14 de febrero, el día de San Valentín.

Me desperté sobresaltado. Las cortinas estaban echadas, y tuve que

girarme en la cama para mirar el reloj y ver la hora: casi las 2. Cogí el busca de la mesilla para ver si había algún mensaje nuevo: nada. *Joder*. Deben haber ido a arrestar a Kevin sin avisarme. La acción había tenido lugar, y probablemente Andrew y Robert estuvieran profundamente dormidos.

Rebusqué en la riñonera, encontré la nota donde había garabateado el número de la oficina local del FBI y marqué.

"Estoy buscando a Levord Burns", dije en cuando descolgaron.

Una voz somnolienta al otro extremo de la línea dijo, "Mm-jm". Sólo podía ser Levord.

“¿Qué pasa con la orden de arresto para Mitnick? ¿Ya ha sido el asalto?”.

En lugar de una respuesta, lo que escuché fue un sonido como si mi llamada estuviese siendo transferida. Después la línea enmudeció.

¿A quién acababa de hablarle? ¿Me habían embaucado?

Me tocaba el turno de ponerme paranoico. ¿Y si Kevin Mitnick había podido manipular los teléfonos del FBI para que las llamadas le llegaran a él? Si era Mitnick, yo acababa de revelarle todo. Volví inmediatamente a llamar al mismo número, y una voz masculina diferente respondió “FBI”.

Pregunté por Levord Burns.

“¿Quién?”.

“Levord Burns. Ha venido de Washington”.

“No creo que esté aquí, aunque hay como treinta y cinco personas. Hay bastante jaleo”. Le di las gracias y colgué.

¿Estarían llevando a cabo en ese momento la detención? Julia se había despertado y le dije: “Creo que deberíamos ir a ver si está pasando algo en el complejo de apartamentos”.

Los apartamentos del Player’s Club se encontraban al otro lado del aeropuerto saliendo del Sheraton, y Julia

nos condujo hasta allí atravesando lo que parecía un laberinto de caminos en construcción y desvíos. Cuando finalmente llegamos a la urbanización, pasamos una vez por delante, pero no vi nada que recordase ni remotamente a una operación de vigilancia, un asedio o la intensa actividad que podía esperarse si un arresto por los federales hubiera tenido lugar en el curso de las últimas horas.

Como no queríamos seguir rondando por la zona, arriesgándonos a ser vistos, recorrimos el breve trecho por la avenida Glenwood hacia Raleigh y en una gasolinera encontramos una cabina

telefónica.

Llamé a Kent Waller, quien dijo que ese día no había sabido nada de Raleigh. Parecía que nada había ocurrido aún, cosa que a él le sorprendía y a mí me desconcertaba. Por sugerencia de Kent, llamé a John Bowler, cuyo mensaje le había pasado yo a Levord la noche anterior.

"No he tenido noticias" dijo Bowler. "Esto me ha caído de pronto en las manos. Pero no he visto ningún papel y no he tenido noticias del agente especial Burns". A pesar de ir a ciegas, Bowler me pareció dispuesto a colaborar.

"Creo que es necesario que

hablemos cuanto antes", dije.

Bowler me dio indicaciones sobre cómo llegar al Edificio Federal en el centro. El tráfico lento de la tarde ya había empezado, de modo que nos llevó un buen rato llegar al edificio de los tribunales. Aparcamos en la calle delante de la fachada acristalada del moderno edificio y entramos, dejando atrás el puesto de control en el vestíbulo.

Poco después de las cuatro Julia y yo alcanzamos por fin las oficinas del fiscal en la última planta, donde firmamos y nos proporcionaron distintivos de visitante. Tuvimos que

aguardar un rato mientras Bowler daba fin a una reunión, hasta que salió a la zona de recepción, se presentó y nos invitó a pasar a su despacho.

El fiscal era un cuarentón calvo con sonrisa de dentífrico y aspecto saludable, casi juguetón. Andaba como un atleta y era evidente que era una especie de fanático de la bicicleta, pues había revistas de ciclismo por todo el despacho y una caricatura enmarcada de la extraña vestimenta de los ciclistas. También había varias fotografías de su esposa y sus dos hijos preadolescentes.

Nos sentamos en dos sillones delante de su escritorio y empezamos a

explicarle el motivo de nuestra comparecencia en su despacho en una deprimente tarde de martes.

"¿Qué conoce usted ya de este asunto?", pregunté.

"Muy poco", dijo Bowler, pero dejando entrever su curiosidad ante el hecho de que dos hackers californianos hubieran peregrinado hasta su oficina con una historia que contar.

Le dije que estábamos persiguiendo a Kevin Mitnick, que estaba buscado por el FBI y los tribunales, y le mencioné lo más concisamente posible los acontecimientos de las pasadas semanas, hasta el rastreo de Mitnick en el

complejo de apartamentos del Player's Club el sábado por la noche.

"El FBI está en la ciudad desde anoche", dije, "y dado que todos sabemos dónde está Mitnick, no comprendo porqué las cosas no se desarrollan con mayor rapidez. Él lleva más de dos años eludiendo al FBI, y da la impresión de que le estuvieran dando la oportunidad de volver a escaparse".

"¿Va armado, o es peligroso en algún sentido?", preguntó Bowler.

Le dije que no creía que fuese armado, pero que era peligroso en un sentido impredecible. Fuera o no a esgrimir efectivamente ese potencial, de

momento estaba en condiciones de dañar sistemas informáticos utilizados por decenas de miles de personas y que contenían información valorada en cientos de millones de dólares. Varias compañías de Internet estaban operando con considerable riesgo en un esfuerzo por colaborar en la caza del delincuente, y no era probable que continuaran exponiéndose durante mucho más tiempo.

"Mitnick no es el delincuente al que las autoridades suelen enfrentarse", subrayé. "Para Mitnick esto es un juego, y él conoce la tecnología telefónica e informática mucho mejor que los agentes

de la ley que lo persiguen".

Le comenté a Bowler que el agente especial del caso, Levord Burns, había esperado tener a mediodía un mandamiento judicial y una orden de registro, pero que yo no había tenido noticias de él desde la mañana temprano. Me preocupaba que eso dilatara las cosas un día más, porque tenía motivos para creer que Mitnick podría estar alertado sobre nosotros.

"Parece que tendré que hablar con Levord Burns", dijo Bowler. Llamó a la oficina del FBI en Raleigh, donde lo remitieron al hotel de Levord.

Cuando dio con él, Bowler le dijo,

en tono amable pero firme: “Tengo entendido que está redactando el atestado”. Hizo una pausa para escuchar. “¿Puede venir lo antes posible?”.

Bowler miró su reloj —era casi la hora de cierre del Edificio Federal— y dijo: “Será mejor que tenga preparado a un juez para esas órdenes”. Llamó al despacho del juez Wallace Dixon, a quien seguidamente localizó en el gimnasio del edificio. Bowler y el juez convinieron en que más tarde le llevásemos los papeles a su casa.

Las siguientes llamadas de Bowler fueron a un amigo, que aceptó reemplazarle esa noche como entrenador

del equipo de fútbol de su hijo, y a su esposa, para decirle que iba a faltar al partido y que probablemente regresaría a casa un poco tarde.

A continuación se puso a reunir documentos y a asignar tareas a dos ayudantes. La más joven de las dos mujeres parecía andar por los treinta, era llenita, con el cabello rubio rizado, las uñas bien pintadas y un pañuelo Betty Boop al cuello. La mayor, que parecía además llevar la voz cantante, era más corriente y tenía la ronquera típica de los fumadores inveterados. Mientras ellas trabajaban, el busca me anunció un mensaje de Pei.

“Ha ocurrido algo nuevo”, me informó cuando la llamé. Kevin había destruido unos datos de cuentas, dijo, y aunque pudieron recuperarlos, a los jerarcas de la Well les preocupaba que se volviera vengativo y se propusiera causar un daño irreparable. “Tsutomu”, añadió, “a la dirección le inquieta continuar en esta situación vulnerable”.

Lo de “la dirección” a mí me sonó a “Claudia”, así que le di a Pei un informe de cómo estaban las cosas, afirmando al final: “Sabemos dónde está, y ahora mismo estamos cumpliendo los trámites para la detención”. Agregué que tan pronto como pudiese llamaría a Bruce

Katz.

El oír aquella conversación pareció galvanizar aún más a Bowler, que volvió a llamar a Levord, a quien dijo, esta vez con mayor firmeza y menos amabilidad: "¡Estamos necesitando ese atestado!".

Yo le estaba agradecido a Kent Walker por haberme puesto en contacto con Bowler, de modo que lo llamé para ponerle al corriente. Él también se alegró de oír que alguien en Raleigh reconociese por fin la urgencia del caso, y se quedó pasmado al enterarse de que Levord todavía no había acabado con la documentación necesaria. "¿Qué le pasa

a este hombre?", dijo Kent. "No es necesario escribir un libro sobre el tema. El atestado no tiene porqué ser tan minucioso".

Como Julia y yo no habíamos comido nada desde la cena de la noche anterior, y en vista de que el Edificio Federal estaba a punto de cerrar, ella bajó hasta un puesto del Metro y trajo unos bocadillos. Nos sentamos en el suelo del despacho de Bowler y los compartimos con él y sus ayudantes, que seguían trabajando.

Telefoneé a Katz, que volvió a contarme lo que me había dicho Pei sobre el archivo de registros borrados.

“Tsutomu, quiero su consejo”, dijo. “¿Hasta qué punto somos vulnerables?”.

Katz planteó una serie de interrogantes. ¿Mitnick había detectado, efectivamente, que el personal de la Well lo estaba vigilando, y había decidido que cayeran juntos si él iba a ser capturado? ¿Qué riesgo estaban corriendo ellos al no desconectar sus sistemas o expulsarle inmediatamente? “¿Qué está pasando, Tsutomu? ¿Está Mitnick tratando de vengarse?”, preguntó Katz.

“No hemos hecho nada para poner a Mitnick contra la Well”, respondí honestamente. “Estamos a punto de

cogerle. Dennos un poco más de tiempo".

Si bien yo no creía que Mitnick tuviera algún motivo para pensar que la Well lo hubiera descubierto, no podía decir lo mismo en cuanto a Netcom. Telefoneé a Andrew, que me informó de más señales de desconfianza en Mitnick. Continuaba moviendo sus reservas de datos y cambiando contraseñas, y en un gesto de desprecio hacia quienes se ocupasen de revisar los archivos de registro, había intentado entrar en Netcomsv con la contraseña .fukhood, sin duda para suscitar la especial atención de Robert Hood. Y

desgraciadamente, había también algo que indicaba que de pronto se aproximaba a la Well con una cautela nueva: la cuenta dono, que él había utilizado durante semanas con la misma contraseña, fucknmc, tenía súbitamente una nueva. Puede que hubiera algún significado oculto en la elección de la nueva contraseña —no, panix—, pero lo que a nosotros nos importaba mucho más era que al parecer Mitnick había considerado necesario adoptar una medida de contraseguridad en la Well, por más que resultase ineficaz, dado el nivel de nuestra vigilancia. ¿Acaso algo o alguien lo había puesto sobre aviso?

¿Habría descubierto el uso de su registro de entrada por Pei?

Por fin llegó Levord, que me dirigió una mirada de enojo al entrar a paso aún más lento que el acostumbrado. Depositó el atestado sobre el escritorio de Bowler y declaró que podía haber venido antes, pero que había pensado que para hacer las cosas bien sería una buena idea organizar su equipo.

"Me he tomado además un tiempo extra para estar seguro de que el atestado estaba correcto. Puede que ustedes quieran capturarlo", dijo, con los ojos puestos en mí, "pero para mantenerlo preso es necesario hacerlo

todo según las reglas".

El obstáculo por superar, le dijo Levord a Bowler, era el de determinar cuál era la dirección correcta entre las varias posibles a las que habían quedado reducidas por el equipo de Quantico la noche anterior. La disposición del edificio estaba dificultando captar con precisión las radio señales celulares.

Esa mañana el agente local del FBI, L. B. Thomas, había ido al Player's Club a hablar con el gerente, con la esperanza de revisar su lista de inquilinos y descubrir si un hombre de unos treinta años se había mudado

recientemente a alguno de los apartamentos sospechosos. Dos inquilinos habían entrado en las últimas dos semanas, pero uno de ellos era la novia del gerente, y el otro vivía en otra parte del complejo. De modo que a Levord le habían quedado tres direcciones posibles. Cualquiera de ellas podía ser la buscada, pero también existía la posibilidad de que ninguna de las tres fuese la del apartamento del que efectivamente provenían las ondas de radio.

La dificultad, nos explicó Bowler a Julia y a mí, no estribaba en obtener una orden de arresto, que podía expedirse

para todo el complejo del Player's Club en tanto Mitnick estuviese en algún lugar del recinto. Lo peliagudo sería la orden de registro. Para encontrar y secuestrar pruebas era necesario contar con autorización del juez para revisar una residencia, la cual en este caso había que especificar con número del edificio y el apartamento.

Levord salió a la zona de recepción a hacer más llamadas para ver si su equipo había encontrado nuevos indicios. Entretanto, Bowler y sus ayudantes, ahora que contaban con el atestado, se dedicaron a preparar órdenes para cada una de las

direcciones de la lista de Levord. Por si acaso, Bowler les hizo preparar una cuarta, con la dirección en blanco. Esperaba poder persuadir al juez de que firmara las tres que estaban completas, y dejar la restante para autorizar después, en caso necesario, mediante una llamada telefónica al juez, si los agentes en el lugar determinaban que Mitnick vivía en otro apartamento.

Ayudé a Bowler a hacer una lista de elementos para incluir en la orden de registro, tales como ordenadores, documentación de software y hardware, discos flexibles, modems, teléfonos móviles y componentes de los mismos.

Era bastante surrealista tratar de imaginar la guarida de Mitnick y lo que podría haber dentro. Las noticias relativas a sus últimas maquinaciones en la Netcom y en la Well habían subrayado una vez más su potencial para lo malo. Y cuando una de las ayudantes de Bowler fue a imprimir las órdenes y descubrió que de pronto su ordenador estaba incapacitado para comunicarse con la impresora por la red de área local de la oficina, Julia sugirió que aquello podría ser obra de Mitnick. Pero rápidamente descubrimos que el problema se había debido a un error y no a un saboteador.

Finalmente, poco después de las 7 de la tarde, tuvimos las órdenes listas. Como Levord no había avanzado en acortar la lista de direcciones, Bowler metió las cuatro órdenes en una carpeta y salimos para ver al juez Dixon.

Al salir al vestíbulo de la oficina de Bowler Julia vio un cuenco lleno de pequeños caramelos rojos en forma de corazón típicos del día de San Valentín. Tras revolver un poco encontró uno que ponía YES DEAR y me lo dio. La broma consistía en que yo a veces la fastidio diciéndole eso, pero yo estaba tan desasosegado que me limité a mirarlo distraídamente antes de metérmelo en la

boca. Los cuatro nos encaminamos a los ascensores, animados por las dos asistentes.

"¡A por ellos!", exclamó la de la ronca voz de fumador.

Resolvimos cubrir el trayecto hasta la casa del juez en la furgoneta especial de Bowler, para poder luego proseguir directamente hacia el Player's Club. Todavía esperaba llegar al complejo de apartamentos antes de las 8 y captar a Mitnick en el aire antes de su descanso para cenar, que generalmente duraba más o menos hasta las 11 de la noche La furgoneta, provista de persianas y cortinas en las ventanillas, me permitiría

permanecer fuera de la vista durante la vigilancia. Además sería más cómoda que el Geo, pues se trataba de un completo salón familiar móvil, con paneles de madera, gruesa tapicería, envoltorios de comida y juguetes de plástico por el suelo.

Con Levord siguiéndonos en su Crown Victoria, nos dirigimos a un acaudalado barrio al norte de Raleigh que resultó estar bastante próximo al emplazamiento de Mitnick. Julia y yo aguardamos en la furgoneta mientras Bowler y Levord entraban en la casa del juez, una vivienda de ladrillo, de tamaño mediano, con un pequeño porche

techado. Afuera había oscurecido bastante, con lo que nos fue fácil observar a través del ventanal sin cortinas del salón de la casa del juez a las personas que se movían en el interior.

Mientras esperábamos, decidí enviarle a Andrew el código de alerta que habíamos convenido de antemano, lo cual me dio cierto trabajo. Yo quería colocar el número 080663 entre sendos guiones para que resultara claro de una ojeada que este no era un número telefónico normal. En muchos busca numéricos, el guión se logra pulsando la tecla *, pero cuando introduje la

combinación *080663* seguida de la tecla # para enviarla, me dio una señal de error. Tras introducirla otra vez con igual resultado, introduje el número código sin los guiones, que fue transmitido sin problemas. Sólo me quedaba esperar que Andrew lo interpretaría correctamente.

Las cosas no iban como la seda en el interior de la casa del juez. El juez Dixon, según supimos después, estaba pidiendo diversos cambios en las órdenes, incluyendo una disposición autorizando un arresto después de las 10 de la noche, lo cual era legalmente necesario estipular, ya que las

detenciones han de efectuarse en general durante las horas normales de vigilia. Estaba claro que se iba a necesitar documentación adicional, de modo que Bowler hizo arreglos para que alguno de sus letrados la preparase y se reuniera con él en el lugar de la vigilancia. Casi a las 8:30 Bowler y Levord salieron de la casa.

Recorrimos varios kilómetros hasta el aparcamiento del centro comercial situado sobre Duraleigh Road frente al complejo de apartamentos, y Levord se desvió por una calle lateral hacia el extremo del Player's Club donde se iba a desarrollar la acción. A estas alturas

no teníamos idea de cuántos ni qué clase de refuerzos había reunido Levord, pero yo supuse que ya que esta parte de la función estaba totalmente en manos del FBI, ellos sabrían lo que hacían.

Bowler fue rodeando el pequeño aparcamiento del centro comercial mientras considerábamos el mejor lugar donde situar la furgoneta. Al final aparcó de forma que por el parabrisas viésemos la urbanización, aunque no del lado de Mitnick. Yo me senté al fondo, para no llamar la atención. Después de instalar mi monitor, encendí una diminuta linterna que me había prestado Julia para vigilar la pantalla mientras

empezaba a buscar las frecuencias, tanto de Cellular One como de Sprint. No había señales de Mitnick.

"Parece que está cenando", dije. Tal vez hubiera salido; incluso podría estar aquí, en la zona comercial. Miramos por los alrededores en torno a la furgoneta, pero no andaba nadie a pie por Duraleigh Road. Bowler y Julia resolvieron dar una vuelta caminando por la zona para ver si veían a alguien que pudiera ser Mitnick, aunque ninguno de los dos sabía exactamente qué aspecto tenía.

Para hacer frente al helado aire nocturno de febrero, Bowler llevaba un

sombrero de fieltro y una trinchera, y al salir de la furgoneta se volvió hacia mí y me preguntó, con timidez: "¿Le parece que tengo demasiado aspecto de agente de paisano?". Evidentemente estaba disfrutando con aquella inesperada aventura.

Con las cortinas laterales cerradas para no ser visto, no podía ver qué hacían Julia y Bowler, pero a los quince minutos ambos regresaron de su vuelta de reconocimiento. Mientras les escuchaba, Bowler me dejó ponerme su sombrero para que no me sintiese ajeno a su diversión. Él y Julia habían pasado por delante de un restaurante chino de

comida para llevar, una pizzería a domicilio y un bar, mirando a través de los respectivos escaparates; entraron en una tienda a comprar Gatorade, palomitas y pilas para la linterna de Julia.

"No vi a nadie que se pareciese a Mitnick", dijo Julia con humor, "pero te aseguro que en el aparcamiento había varios personajes sospechosos". Camino de las tiendas habían visto a dos hombres sentados a oscuras en el asiento delantero de un coche evidentemente oficial, de frente al Player's Club.

Julia había decidido entrar en el chino a comprarnos algo más de comida,

y mientras aguardaba el pedido notó que uno de los que atendían en el mostrador se volvía hacia un compañero y le decía: "Me parece que algo está pasando; esos tipos llevan ahí muchísimo rato". Uno de los empleados de la pizzería también se había asomado varias veces a la puerta para ver qué podía estar ocurriendo en el aparcamiento.

Durante las siguientes dos horas no hubo más que silencio en el escáner, y no pude ahuyentar el pensamiento de que Kevin podría haber huido, una situación que resultaba cada vez más verosímil, dado lo escasamente sutil que era lo

poco que podíamos ver de la operación de vigilancia.

"La otra noche lo vimos hablar de *Los fisgones;* puede que haya ido al cine", dijo en cierto momento Julia, en un intento por levantarme el ánimo.

En un rincón del aparcamiento, al lado de la gasolinera, había un grupo de teléfonos públicos que yo alcanzaba a ver mirando a través de las cortinas laterales. Para ser un día de semana en pleno invierno, el número de llamadas que se estaban efectuando desde ellos resultaba llamativo. Varias veces sonó el busca —Markoff desde el Sheraton, ansioso por noticias— y Julia salió del

coche para ir hasta el teléfono público a llamarle. Entonces, cerca de las 11, hubo una llamada de Andrew desde la Netcom.

"Esto no va a gustarte" me advirtió Julia cuando volvió de hablar con él. Andrew se había dado cuenta de que había vuelto a meter la pata. Tres horas antes, cuando me había costado varios intentos transmitirle el mensaje de "alerta", Andrew había interpretado la ráfaga de señales como señal de que Kevin ya había sido detenido. Como pruebas, se había puesto a hacer copias de seguridad de los archivos que Mitnick había escondido en diversos

lugares de Internet y luego había empezado a borrar las propias versiones del intruso.

Había también una noticia buena: Andrew había analizado el borrado del archivo de cuenta de la Well realizado ese mismo día por Mitnick determinando que era consecuencia de un simple error tipográfico, no un acto de sabotaje. Pero la noticia mala era devastadora: nuestra vigilancia había sido irremisiblemente comprometida.

Y había ocurrido hacía varias horas. De nuevo Andrew había pospuesto la llamada, temiendo mi cólera. Aquello era increíble. Yo había estado

presionando duramente al FBI, y si ahora todo se derrumbaba y Mitnick huía, ellos iban a poder venir a decirme: "Su gente lo echó a perder".

Pero no había tiempo para lamentarse del error: mi monitor indicaba que Kevin Mitnick acababa de fichar para el turno de la noche. Y si no había advertido antes de la cena que sus escondrijos habían sido destruidos —y su presencia actual indicaba que podía no haberse enterado aún—, estaba por descubrirlo.

No había sido yo el único en enterarse de que Kevin había vuelto. Repentinamente, el coche de Levord y

varios otros vehículos atravesaron velozmente el aparcamiento y desaparecieron detrás de una bolera situada al final del centro comercial. Era una breve reunión final de coordinación de las agencias federal y la policía local, y Bowler se acercó con la furgoneta a la media docena de agentes de paisano que se habían reunido. Le entregó las órdenes enmendadas a Levord, y yo le advertí al grupo que Mitnick podía haber sido puesto accidentalmente sobre aviso, de modo que la prisa era más crucial que nunca. Alguien mencionó que los agentes de Quantico tenían ahora un "radiofaro" al

que apuntar y podían usar un monitor manual de potencia de señales para el trabajo de acercamiento, de modo que no debía llevarles mucho tiempo encontrarle. La reunión duró menos de un minuto, y los otros se fueron a ocupar sus respectivos puestos alrededor y sobre el extremo del Player's Club.

Bowler volvió lentamente con la furgoneta a nuestro sitio en el aparcamiento y yo reanudé mi tarea, captando las idas y venidas de Mitnick a lo largo de aproximadamente una hora. Por lo general, al concluir una llamada de información, volvía a marcar inmediatamente. Pero en un momento

dado no le oí volver al aire, de modo que empecé a comprobar los vectores adyacentes del emplazamiento de la célula de Cellular One, para ver si su señal había sido rebotada a otro sector. Y entonces advertí algo extraño.

Aunque Kevin estaba al sur de la célula, yo ahora estaba captando una portadora desde el norte. Desde que estaba en Raleigh, era la primera vez que veía colocar dentro de esta célula otra llamada de otra parte que no fuese la vecindad de Mitnick. Debido a la irregular fiabilidad de las conexiones celulares y al coste relativamente alto del servicio a menos que sea robado, no

es corriente utilizar la radio celular para transmitir informaciones.

Les comuniqué mi descubrimiento a Bowler y a Julia, y nos pusimos a conversar en voz baja. ¿Se había mudado Mitnick? ¿Tenía un socio? ¿O se había movilizado después de ser alertado por la prematura limpieza de Andrew?

Después de captar el MIN de este nuevo usuario, le dije a Bowler: "Vamos hasta los teléfonos públicos". Eran las 12:40 a.m. Él situó la furgoneta lo más cerca que pudo de los teléfonos, con el vehículo entre el complejo de apartamentos y yo para que me deslizara

fuera y poder llamar al técnico de Cellular One.

"Gary", dije cuando Gary Whitman cogió el teléfono. "¿Está observando?".

Estaba efectivamente vigilando el emplazamiento de Cellular One, de modo que le leí el nuevo MIN y le pedí que me avisara cada vez que nuestro misterioso llamador pusiera una nueva llamada y se mudara a una nueva frecuencia. Lo podía hacer por mi busca pasándome los nuevos números de canal.

Una vez más, Bowler volvió a nuestro lugar en el aparcamiento y casi inmediatamente recibí la primera serie

por el busca, lo que me permitió hacer un rápido barrido entre el sector de Mitnick y el del hombre misterioso, confirmando que en efecto teníamos dos usuarios separados utilizando la misma célula. Estuve cuarenta y cinco minutos vigilando a los dos.

Entonces, casi exactamente a la 1:30, el portador de Mitnick se paró. Inmediatamente vimos pasar velozmente la furgoneta rural de Quantico, primero por Duraleigh Road y al poco rato a toda velocidad en dirección opuesta. El vehículo llevaba ahora la antena direccional que la noche anterior había estado en la furgoneta de Fred Backhaus.

El segundo usuario seguía aún en el aire, y era evidente que los agentes de Quantico también lo habían ubicado.

Otros vehículos se estaban moviendo ahora hacia el Player's Club, incluyendo el de nuestros vecinos del aparcamiento. "Ha ocurrido algo", dijo Bowler. "Vamos a echar una ojeada".

Lentamente, sacó la furgoneta del aparcamiento y se metió en la calle lateral más próxima a los apartamentos, para detenerse detrás de unos arbustos, desde donde veíamos directamente el aparcamiento. Bajamos de la furgoneta. Ahora veíamos que la zona estaba bien cubierta. Había por lo menos cuatro

coches oficiales y una docena de agentes de paisano.

Yo quería ir a decirles a los agentes lo que sabía sobre las nuevas señales procedentes del norte, pero Bowler vino a colocarse a mi lado y dijo: "No, no, no. En este momento no puede hacer nada. Además, todavía no sabemos si tienen a Mitnick. Él podría verle".

"Pero yo tengo el MIN", objeté. "Cellular One me está enviando los números de canal".

"¿Por qué no manda a Julia con un papelito?", sugirió él.

Julia fue. Ellos de entrada se molestaron, pero cuando se dieron

cuenta de que les llevaba una valiosa información, recibieron el MIN y mi busca y una vez más la furgoneta del equipo de Quantico salió rugiendo, esta vez hacia el norte. Julia regresó, y nos instalamos en la furgoneta a escuchar el suave siseo del modem del misterioso usuario.

A los diez minutos entró Levord.

"Estamos dentro", dijo. "Tenemos a Mitnick. Pero vamos a tener que llamar al juez para que autorice el registro de una dirección nueva".

Le tendí a Bowler mi teléfono móvil para que pudiera despertar al juez Dixon y pedirle la orden de registro de la casa

de Mitnick. A continuación le envié a Andrew por mi busca el código "adelante". Por fin era hora de que se pusiera a alertar a la Well y al resto de nuestra lista. Esperaba que todavía estuviera despierto.

Mientras Bowler hablaba con el juez, Levord nos describió a Julia y a mí cómo él y varios agentes más habían golpeado a la puerta del apartamento y aguardado cinco minutos enteros a que se abriese. Cuando finalmente se abrió, el hombre que apareció se negó a admitir que era Kevin Mitnick.

Ellos entraron igual, y Mitnick corrió a guardar unos papeles en un

maletín, un acto sin sentido, dadas las circunstancias. Dijo que estaba al teléfono hablando con su abogado, pero cuando Levord cogió el auricular, la línea estaba muerta. El delincuente informático más famoso de América se puso a vomitar en el suelo del salón de su casa.

"Todavía no le hemos interrogado", dijo Levord. "Nos preocupa su condición física. Encontramos frascos de medicinas. Está bajo alguna clase de tratamiento".

Ahora no había peligro en salir de la furgoneta. El equipo de Quantico había vuelto, y me dirigí adonde se

encontraban, junto a su furgoneta rural. El aire frío y húmedo de la noche había terminado dando paso a una ligera lluvia. Los agentes tenían el aspecto de unos fatigados atletas veteranos después de una gran victoria: alegres, pero demasiado cansados para celebrarlo. Habían seguido captando crecientes ecos de radio con la antena direccional, de modo que se pusieron a recorrer el complejo rastreando a Kevin con el medidor de potencia de las señales, y la señal celular cada vez más intensa les llevó hasta la misma puerta principal de Mitnick.

Pregunté por la otra señal de datos.

Me dijeron que la habían seguido durante un rato pero no habían podido situarla. Al igual que otros hilos de la investigación, permanecería siendo un misterio.

Esa noche no vi a Mitnick en ningún momento. Pasaría aún no menos de otra hora antes de que fuera provisionalmente enviado a una celda en la cárcel del condado de Wake en el centro de la ciudad. Mucho antes de eso, Levord Burns obtuvo del juez, vía Bowler, una orden de registro, y puso a sus agentes a reunir pruebas.

Levord vino nuevamente a la furgoneta a informar de tales avances.

Le pregunté si podía echar una ojeada al apartamento, para ver cómo mi oponente había pasado sus días y sus noches, pero Levord no me lo permitió.

"Hemos hecho un montón de fotografías del interior del apartamento, pero son pruebas para el juicio y nadie más puede verlas hasta que esté terminado", declaró. Pero en cambio nos mostró el coche de Mitnick, un viejo Plymouth Horizon azul claro.

El talante de Levord había mejorado visiblemente, a pesar de la constante llovizna fría que nos estaba calando a todos, y dio la vuelta hasta el costado de la furgoneta para estrecharme la mano.

“Enhorabuena”, dije. “Hemos conseguido hacer esto sin matarnos el uno al otro”.

Él no respondió, pero por primera vez desde que le conocí, el agente especial Burns me dedicó una sonrisa.

17. ¡Usted es Tsutomu!

A la mañana siguiente me despertó una llamada de Markoff.

“La comparecencia de Kevin en el tribunal es a las diez en punto”, dijo.

Miré el reloj y vi que ya eran más de las nueve. “Nos encontraremos en el vestíbulo en cuanto nos hayamos vestido”, le dije, mientras sacudía suavemente a Julia para despertarla, antes de descorrer las cortinas de la habitación del hotel y contemplar la

húmeda mañana gris de Raleigh.

Markoff nos condujo al centro bajo una leve lluvia, y como me sentía un tanto aislado desde la ruptura de mi terminal RadioMail, decidí usar el teléfono móvil para revisar mi buzón de voz en San Diego. Increíble. Había un nuevo mensaje con aquel fingido acento asiático, y había sido enviado poco antes de las 7 de la mañana, hora de la costa Oeste, ocho horas completas después de la detención de Mitnick, pero mucho antes de que su captura hubiese sido anunciada por los medios de comunicación.

El mensaje era largo e inconexo, sin

nada de la arrogancia ni las baladronadas que habíamos oído antes, sino pronunciado de forma tan agitada y rápida que en ocasiones el acento desaparecía por completo. Después de escucharlo, lo pasé dos veces más, primero poniéndole el auricular en la oreja a Julia y después a Markoff:

> Hola, soy yo otra vez, Tsutomu, hijo mío. Sólo quería decirte… muy importante, muy importante. Todas esas llamadas telefónicas que recibiste con… mmm… haciendo referencia a películas de Kung Fu… nada que ver en absoluto con

cuestiones informáticas. Sólo una… mmm… interesante pequeña llamada.

Ahora veo que esto se está volviendo demasiado grande, demasiado grande. Quiero decirte, hijo mío, que éstas no tienen absolutamente nada que ver con actividades informáticas. Sólo burlarse de las películas de Kung Fu. Eso es. Eso es.

Y haciendo referencia a… mmm… tratando de hacer una referencia a poner las películas de Kung Fu en… en una referencia informática. Eso es. Nada que ver

con ningún Mitnick, con ataques, esas cosas, nada. Te digo que era sólo una llamada interesante eso… es. Todo coincidencia. Esto se está volviendo demasiado grande, y nada malo ha hecho nadie que dejara mensajes en tu buzón de voz. Sólo para que sepas. ¿Vale? Se está volviendo demasiado grande."

Estábamos asombrados. "De modo que volvemos a las andadas", dije. Me pregunté en voz alta dónde se escondería el amigo de Mitnick. Tenía curiosidad por saber si se habría ocultado aquí en Raleigh. ¿A quién habría llamado

Mitnick en los minutos que trascurrieron antes de que les abriera la puerta a los del FBI? ¿Era éste el dueño del segundo teléfono móvil que había estado efectuando las llamadas de datos que el equipo de Quantico había estado persiguiendo?

Continuábamos hablando de este segundo misterio cuando entramos en el edificio federal. Se trataba simplemente de una vista preliminar, y la noticia de la detención de Mitnick no se había divulgado aún. Entramos en una pequeña sala de tribunal vacía y nos sentamos en la última de las tres cortas hileras de asientos que habían sido reservadas

para el público. Era igual a todas las salas de tribunal del país, un recinto austero, sin ventanas y con el cielo raso muy alto.

Al poco rato Mitnick fue introducido en la sala desde una puerta al frente del recinto y a la derecha del estrado del juez por un fornido aguacil. Kevin no tenía aspecto de enfermo, pero tampoco se parecía en nada al obeso "hacker del lado oscuro" con gafas que una vez había aterrorizado a Los Ángeles. El que veíamos era un joven alto, ni grueso ni delgado, que usaba gafas de aro metálico y llevaba el cabello castaño suelto y largo hasta los hombros. Vestía

un chándal gris oscuro, estaba esposado y con las piernas encadenadas.

Se detuvo un momento al reconocernos. Pareció perplejo, y abrió mucho los ojos.

"¡Usted es Tsutomu!" exclamó en tono de sorpresa, y a continuación miró al reportero que estaba a mi lado. "Y usted es Markoff".

Los dos asentimos con la cabeza.

Tanto para Mitnick como para mí había quedado claro que aquello ya no era un juego. Yo había considerado la caza y captura como deporte, pero ahora era evidente que era absolutamente real y tenía consecuencias reales.

Después de varias semanas de seguir la pista de aquel hombre, de ver el daño causado por él, de ir comprendiendo que en la invasión de la intimidad de los demás y en el atropello de la propiedad intelectual de otros no era sólo inflexible y tenaz, sino además mezquino y vengativo, de una cosa estaba seguro sobre Kevin Mitnick: él no era en modo alguno el héroe de una película sobre cierto maltratado hacker informático cuyo único delito fuera la curiosidad. No había nada de heroico en leer el correo de otras personas y en robarles el software.

Lo condujeron a la mesa de los

acusados y el juez Dixon entró en la sala. La vista terminó en menos de diez minutos. Todavía no le habían designado un defensor de oficio, así que Mitnick estuvo solo en aquella mesa, con el alguacil a su espalda. Yo tenía curiosidad por ver si continuaría con su comedia, pero cuando le preguntaron su nombre se identificó como Kevin David Mitnick. El espíritu de lucha lo había abandonado, y su cansancio era visible.

Mientras el juez le leía los cargos —fraude en telecomunicaciones, y fraude informático, cada uno penable hasta con quince años o más—, fue evidente que Mitnick empezaba a comprender lo que

le esperaba. Aquel juego tenía penalizaciones reales. Con voz suave requirió permiso del tribunal para comunicarse con su abogado de California. El juez señaló que fueran cuales fuesen sus cuentas legales pendientes, el Tribunal del Distrito Este de Carolina del Norte se ocuparía de él primero. La audiencia preliminar fue fijada para dos días después, el viernes por la mañana.

Todo el asunto duró menos de diez minutos. Después que el juez se retiró, Markoff se encaminó a la reja que separa la galería para el público del resto del recinto. Julia y yo lo seguimos.

Kevin se puso de pie y giró para mirarnos de frente.

Se irguió y se dirigió a mí. “Tsutomu, respeto su capacidad profesional”, dijo.

Yo le devolví la mirada e hice un movimiento de cabeza. No parecía haber mucho que decir. En nuestro enfrentamiento, él había perdido claramente.

Curiosamente, viéndolo marchar hacia su celda no me sentí ni bien ni mal, apenas vagamente satisfecho. La solución no era para mí plenamente inobjetable, y no porque compartiese la objeción de algunos que consideraban a

Mitnick un inocente explorador del cyberespacio, sin siquiera el incentivo del provecho propio del empleado que delinque, sino porque él parecía en muchos aspectos un caso especial. Era la sexta vez que lo arrestaban. Sabía, ciertamente, lo que se jugaba, y yo no había captado la menor prueba de un propósito moral más elevado en sus actividades, o al menos una inocente curiosidad.

El alguacil empezaba a llevárselo cuando Markoff dijo, "Kevin, espero que las cosas marchen bien para ti".

Mitnick pareció no haberle oído de entrada, pero luego se detuvo un instante

y se volvió hacia nosotros. Después de hacer una leve señal de asentimiento con la cabeza, volvió a girarse y se lo llevaron.

Nosotros tres nos encaminamos al ascensor. Esta vez, Mitnick estaba más comprometido que nunca. Era reincidente en por lo menos dos delitos federales, y encima había violado la libertad condicional. Más de media docena de distritos federales y varios estados esperaban para formular cargos contra él.

Ninguno de nosotros podía imaginar la psicología de su obsesión. ¿Se tenía él mismo por el inocente *voyeur* que su

amigo Eric Corley creía que era? ¿O estaba envuelto en su propia leyenda, viviendo una visión, inspirada en Robert Redford, de ser el último héroe americano fugitivo? ¿Era algún nuevo tipo de cyberadicto, como lo había considerado un juez federal en 1988? Yo había leído en alguna parte que los jugadores y los falsificadores de cheques exhiben un comportamiento similar: aun cuando se dan cuenta de que tarde o temprano perderán o serán cogidos, experimentan un irresistible deseo de seguir actuando hasta que fallen. Tal vez en algún recóndito lugar de su ser, Mitnick había sido hasta tal

punto seducido por el juego, que aceptaba la misma fatal certidumbre de que tarde o temprano sería apresado. No había modo de saberlo.

Después regresamos al Sheraton. Markoff se fue a preparar su reportaje para el *New York Times* del jueves, en tanto que Julia y yo pasamos en la habitación del hotel el resto del día, en buena parte telefoneando a Andrew, a la gente de la Well y la Netcom, y a otros administradores de sistemas alrededor de Internet cuyas redes podrían haber sido comprometidas por Mitnick. Esa noche, a eso de las 9, Markoff, Julia y yo volvimos a la central de Sprint y

esperamos hasta que Murph y Joe pudieron salir a cenar. Cuando acabaron su turno era tarde, y estuvimos un buen rato dando vueltas antes de encontrar un sitio donde comer.

Cuando al día siguiente me desperté, descubrí que el verdadero caos había empezado. El arresto de Kevin Mitnick era la gran noticia, y el diluvio periodístico había empezado con ganas. Esa mañana descubrí asimismo un último mensaje del interlocutor misterioso. Lo había dejado en el buzón de voz de mi despacho a las 7:23 de la tarde, hora de San Diego, la noche anterior, con una voz llena de urgencia:

Tsutomu, amigo mío. Sólo quiero decir… quiero reiterar que es una gran broma. Es grande, se burla de las películas de Kung Fu, no tiene nada que ver con violación de ordenadores, Mitnick, nada! Díselo a ellos, no hagas que vengan a por mí. No, no salgas volando a venir a por mí. No valgo la pena… sólo me burlo de las películas de Kung Fu. Eso es todo. Gracias.

El juego había terminado de veras.

Epílogo

En julio de 1995, Kevin Mitnick aceptó declararse culpable de una acusación de fraude en telefonía celular y, sin juicio, fue sentenciado a ocho meses de cárcel. Como consecuencia de su detención en Raleigh, los fiscales federales le habían adjudicado veintitrés cargos de fraude telefónico e informático, pero todos ellos menos uno fueron retirados como parte del acuerdo mencionado.

No obstante, los problemas legales de Mitnick no han concluido. Actualmente está preso en Los Ángeles esperando nuevos cargos, incluidos violaciones de libertad condicional, manipulación de los ordenadores del Departamento de Vehículos a Motor del Estado de California y acusaciones de fraude telefónico e informático que pueden presentar contra él más de media docena de distritos federales. A menos que consiga un nuevo acuerdo, tiene un juicio fijado para finales de noviembre, y es probable que pase más tiempo en prisión.

Hoy en día, al repasar los sucesos

del año anterior, sigo preocupado. Aun después de su arresto en febrero, la leyenda de Mitnick continúa creciendo. Durante muchos meses tras la detención hubo acaloradas discusiones en Internet sobre su actividad. Algunas personas siguen argumentando que como Kevin Mitnick nunca le hizo físicamente daño a nadie, lo que hacía era inofensivo.

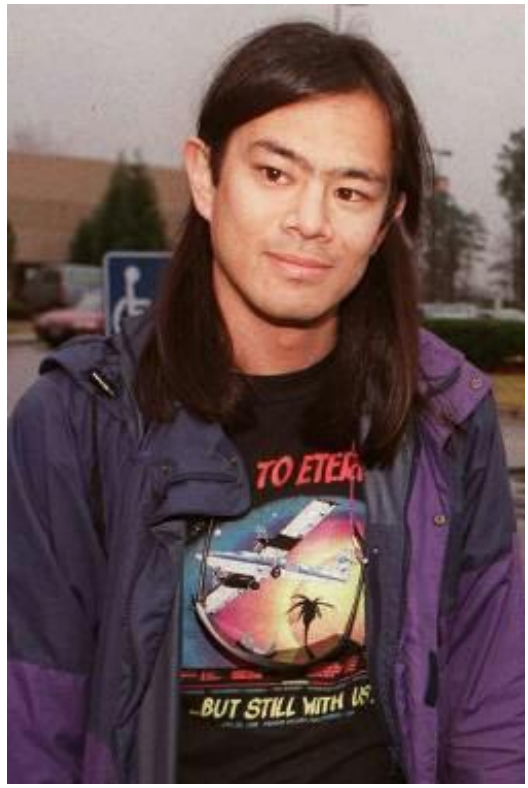
La cuestión es que ése es también el caso del hombre que ha tenido quince años y seis arrestos para averiguar lo que está bien y lo que está mal. A finales de la década de los ochenta, un juez federal hizo un esfuerzo especial para darle una segunda oportunidad.

Para mí, el verdadero delito de Kevin Mitnick es el haber violado el espíritu original de la ética del hacker. No está bien leer el correo de otras personas, y la creencia en que el software y otras tecnologías informáticas deben ser libremente compartidas, no es lo mismo que creer que está bien robarlas.

La red de ordenadores conocida como Internet empezó como un raro experimento de construcción de una comunidad de personas que compartían un conjunto de valores sobre la tecnología y el papel que los ordenadores podían desempeñar en el

desarrollo de este mundo. Esa comunidad se basaba fundamentalmente en un compartido sentido de la confianza. Hoy en día, los muros electrónicos que se levantan por todas partes en la Red son la prueba más evidente de la pérdida de esa confianza y de aquel sentido de comunidad. Es una pérdida que nos afecta a todos.

Octubre de 1995.



TSUTOMU SHIMOMURA. Es físico anaista y experto en seguridad de sistemas. Actualmente es miembro del Centro de Superordenadores de San Diego. Ha trabajado como investigador en el Departamento de Física de la Universidad de San Diego, en California y en el Laboratorio Nacional de Los

Álamos en Nuevo México.

JOHN MARKOFF. Sus conocimientos sobre tecnología han hecho de él uno de los más respetados periodistas en esta materia. Informa sobre Silicon Valley, para el *New York Times*. Ha escrito sobre ordenadores y tecnología para

Times desde 1989. Trabaja como reportero para el *San Francisco Examiner* y es coautor de *Cyberpunk: Outlaws and Hackers on the Computer Frontier* y *The High Cost of High-Tech: The Dark Side of the Chip*.

Notas

[1] Cyber = ciber, de cibernético; cop = poli y sleuth = detective *(N. del T.)* <<

[2] “¿Quién viene a comer?” o ¿Quién está por (a favor de) comer? (*N. del T.)*

<<

[3] El pequeño jardín o El jardincillo. *(N. del T.)* <<

[4] Fundación por el Software Libre y Liga por la Libertad de Programación. (*N. del T.)* <<

[5] Muro o muralla de fuego; también se lo conoce por Bola de Fuego. *(N. del T.)* <<

[6] WIRETAP: conectar subrepticiamente con una línea telefónica para interceptar mensajes u obtener información. *(N. del T.)* <<

[7] Background se refiere al trabajo que un ordenador operando en régimen de multiprogramación realiza como tarea de fondo en los intervalos libres entre otros trabajos, y al área de memoria que los almacena. *(N. del T.)* <<

[8] Algo así como “Paseo de la Biotécnica de San Diego”. *(N. del T.)* <<

[9] *Wizard:* mago, brujo, hechicero. *(N. del T.)* <<

[10] Resistor = resistencia, elemento que en un circuito eléctrico es utilizado para proporcionar resistencia contra el paso de la corriente. *(N. del T.)* <<

[11] “Estudiantes Radicalmente Enfáticos Interesados en la Tecnología de la Ciencia y Demás Estudios de Investigación”. *(N. del T.)* <<

[12] Una pieza de plástico liviano, con forma de plato, con el que se juega lanzándoselo entre sí los jugadores. *(N. del T.)* <<

[13] Stepper: un motor paso a paso (que rota en incrementos pequeños y fijos). *(N. del T.)* <<

[14] Termita: mezcla de polvo de aluminio y un óxido metálico que, al inflamarse, produce elevadísima temperatura. *(N. del T.)* <<

[15] *Remote procedure call ToolTalk database server daemon:* Demonio servidor de base de datos de llamada remota (aproximadamente). *(N. del T.)* <<

[16] Visualizador de montaje o “programa cotilla”. *(N. del T.)* <<

[17] IP-spoofing : procedimiento consistente en violar el protocolo de Internet (la convención relativa a la transmisión de información entre sistemas u ordenadores por la Red) adoptando una identidad falsa. *(N. del T.)* <<

[18] Online: conectado directamente a y/o controlado por un ordenador. *(N. del T.)* <<

[19] Burrito: una tortilla de harina que envuelve un relleno, sea de carne, de frijoles o de queso. *(N. del T.)* <<

[20] Una instalación con fuente de aguas termales y lugar de vacaciones en el antiguo emplazamiento de una misión religiosa en el condado de Sonoma. *(N. del T.)* <<

[21] Pretty Good Privacy: intimidad o privacidad aceptable o bastante buena. *(N. del T.)* <<

[22] *Tweedledum & Tweedledee*: cosas que difieren sólo o principalmente en el nombre. *(N. del T.)* <<

[23] CFP, sus siglas en inglés: Computers, Freedom and Privacy. *(N. del T.)* <<

[24] Dead Heads: el autor emplea más adelante la forma "Deadheads", en ambos casos con mayúscula inicial, lo que parecería indicar que alude a admiradores o devotos de un grupo de *rock* de San Francisco conocido por The Grateful Dead o simplemente The Dead, uno de cuyos letristas es citado más abajo como cofundador de la Well. La acepción primaria de *deadhead* es la de persona muy estúpida, inane o aburrida. Por otras razones, también le cabe la acepción de "gorrón".*(N. del T.)* <<

[25] *Fuck* es la más corriente de las palabrotas en inglés. *(N. del T.)* <<

[26] Aquí vas:-) Una visión de Dios. *(N. del T.)* <<

[27] “Oye john, Kevin es un buen nombre”. La palabra “john” es un vulgarismo con diversos significados injuriosos. *(N. del T.)* <<

[28] pw = password = contraseña; 4; four = for = para; nl: Netherlands = Holanda. *(N. del T.)* <<

[29] En este caso, redundancia implica la repetición de unidades a fin de proporcionar un elemento de seguridad para evitar fallos. *(N. del T.)* <<

[30] Interfaz Estándar para Pequeños Ordenadores. *(N. del T.)* <<

[31] Un bus es un camino para las señales entre los diferentes órganos de un microprocesador. El bus de control proporciona la necesaria sincronización y controla la información a través del sistema. *(N. del T.)* <<

[32] Occam's Razor: (por Guillermo de Occam, filósofo inglés del siglo XIII fundador del nominalismo). La regla establece que los entes no deben multiplicarse innecesariamente, lo cual se interpreta en el sentido que menciona el autor. *(N. del T.)* <<

[33] Buffer o memoria-tampón es un área de memoria que se utiliza para guardar una información de forma temporal. *(N. del T.)* <<

[34] Un *loop* es una forma curva o circular en un elemento lineal de cierta longitud (como, por ejemplo, si tomamos un trozo de hilo y cruzamos un extremo por encima del otro). *(N. del T.)* <<

[35] Reuben Lucius Goldberg ("Rube"), 1883-1970. Caricaturista americano. *(N. del T.)* <<

[36] Worm = gusano: un programa que se mueve por toda la red y deposita información en cada nodo (elemento de datos accesible por dos o más rutas) con fines de diagnóstico, o hace que los ordenadores ociosos compartan parcialmente la carga del procesamiento. *(N. del T.)* <<

[37] Celebración en EE. UU., el último lunes de mayo, en honor de los soldados muertos en guerra. *(N. del T.)* <<

[38] Nombres reales o verdaderos. *(N. del T.)* <<