UNIVERSIDAD SIMÓN BOLÍVAR

Departamento de Computación y Tecnología de la Información

CI3715 – Ingeniería de Software

INFORME

Integrantes:

Arleyn Goncalves 10-10290

Francisco Sucre 10-10717

Sartenejas, 14 de Junio de 2015

Introducción

Estamos viviendo en una época de grandes cambios en la historia de la humanidad, estamos viviendo la era de la comunicación, de la globalización y mas importante aun, de la movilidad. Hoy en día casi todas las personas tienen dispositivos tecnológicos que les permiten comunicarse con los demás en cualquier momento o lugar del mundo, que les permiten acceder a una mundo de información casi infinito por medio de la conexión al Internet, uno de los mas grandes inventos del hombre que ha logrado crear redes de comunicación en todo el mundo, un invento que definitivamente marco nuestra era digital. El Internet es una herramienta poderosa que hace al mundo girar hoy en día, en necesario para trabajar en casi cualquier empresa y es lo que permite que existan y se organicen compañías o movimientos de escala mundial ¿es un invento maravilloso no? Pero hay que preguntarnos ¿Y esta herramienta tan poderosa tiene algún efecto negativo? ¿ Tiene algún peligro? Pues en las manos equivocadas, si.

Al igual que se han creado Cyber comunidades y hasta empresas que funcionan puramente mediante Internet, también ha surgido un nuevo tipo de crimen, el crimen informático. Imaginen por un segundo que están frente a su computadora, en sus ropas “cómodas” un jueves por la noche, tienes a tu disposición una webcam pero no la estas usando por el momento, y pocos días después, te llega un mensaje diciendo que pagues una “cuota de rescate” o se publicara un contenido sensible de ti, eso es un ejemplo del poder que puede dar el Internet y la informática en las manos equivocadas. Al igual que el crimen se han mudado a este mundo, la ley también ha tenido que adaptarse, creando así la “informática forense” y escuadrones especializados en perseguir a criminales informáticos. En el programa CSI Cyber podemos un perfecto ejemplo de estos criminales, de sus capacidades y de las personas que los persiguen.

1. Resumen

El siguiente capítulo a resumir es el noveno de la primera temporada de CSI Cyber titulado como L0m1s.

En este capítulo la locura comienza cuando nueve aviones que partieron desde el mismo aeropuerto se enfrentan a un ataque coordinado bloqueando la señal Wi -Fi durante sus vuelo. Simón, el jefe del departamento hizo una controversial llamada a tierra a todos los aviones en cuestión lo antes posible.

La mayor parte del equipo se dirigió a Miami, que era donde parecía originarse el problema. Sin embargo, los nueve aviones terminaron aterrizando en diferentes ciudades. Con el tiempo, los teléfonos que parecían haber causado el ataque se determinaron, y los principales sospechosos fueron detenidos y cuestionados.

Todos los pasajeros afectados tenían sus tarjetas de crédito en mal estado de forma, llevando al equipo a llegar a la conclusión de que todo era un atraco para robar a los pasajeros. El robo se realizo mientras los pasajeros utilizaron estaciones de carga en el aeropuerto invadiendo los dispositivos de las personas y robando la información personal almacenada en sus dispositivos celulares.

Krumitz (Especialista Técnico) determina que los sospechosos en cuestión, cuyos teléfonos bloquearon la conexión Wi-Fi de los aviones, eran también víctimas, no los creadores del problema, ya que el software malicioso se había cargado en sus teléfonos sin que ellos supieran. Posteriormente L0m1s (El hacker) optó por chantajear a varias personas con la exposición de cierta información sensible si no pagaban una cuota de rescate considerable.

Poco después, se descubrió que algunos de los pasajeros habían pagado el dinero del rescate con el fin de mantener sus secretos ocultos, pero la información se publicó de todos modos. Entonces Krumitz emerge, alegando que él sabe que "L0M1S" es una de las personas inicialmente detenidas en el primer lugar, Willa una joven de 16 años. Avery (Agente especial a cargo) recibe una orden para ella y su tableta, Willa confiesa y sus razones fueron que ella lo hizo porque “estaba aburrida y porque ella podía.”

Al final Willa (L0m1s) fue liberada ya que era menor de edad y Avery le reclama a Krumitz que cometió acciones contra la ley, ya que él pagó el chantaje por medio de un mensaje que contenía un virus troyano tomando el control del portátil de Willa y obteniendo una foto digital de ella sin una orden judicial.

2. Cyber delitos cometidos

- **Sabotaje informático**, se hackeó el router de los nueve aviones, para sobrecargar el dispositivo y denegar el servicio.
- **Robo de tarjeta de créditos**, debido al robo de datos de los teléfonos celulares.
- **Fraude informático,** chantaje por la información obtenida de los teléfonos celulares.
- **Invasión a la privacidad**, obtener información privada sin el consentimiento del propietario.
- **Revelar información**, publicar información privada sin el consentimiento del propietario.
- **Sabotaje informático,** enviar mensaje con un virus troyano para tomar el control de una portátil.
- **Sextorsión,** amenaza de enviar o publicar contenido sexual de una persona.

3. Tipificar cada delito según la Ley contra los Delitos Informáticos de la legislación venezolana

- El sabotaje informativo realizado para hackear el router de los nueve aviones para denegar el servicio del WIFI, se relaciona con el **Artículo 7. Sabotaje o daño a sistemas** de la Ley contra Delitos Informáticos de la legislación que nos indica que: el que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información, en este caso el router de los aviones; será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

- La invasión a la privacidad y sectorsión que se mostraron en el episodio, se relaciona con el **Artículo 14. Espionaje informático** de la Ley contra Delitos Informáticos de la legislación que nos indica que: El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, en este caso los dispositivos celulares de los pasajeros, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

  La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro, en este caso se obtuvieron beneficios monetarios debido al chantaje.

  El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado; en este caso en particular se observa como se difundió información privada de una senadora de los Estados Unidos sobre su vida personal y de una ciudadana de la cual publicaron fotos privadas en una página pornográfica.

- En el caso de robo de tarjeta de créditos, se relaciona con el **Artículo 14. Fraude** de la Ley contra Delitos Informáticos de la legislación que nos indica que: El que, a través del uso indebido de tecnologías de información valiéndose de cualquier manipulación en sistemas o cualquier de sus componentes o en la data o información en ellos contenidas (en este caso de los celulares), consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno (obtener los datos suficientes para robar las tarjetas de créditos), será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

También del **Artículo 15. Obtención indebida de bienes o servicios,** que indica que: El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contra prestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Este caso se puede señalar en el capítulo por la compra de aparatos tecnológicos que se realizaron con el dinero robado de las tarjetas de crédito.

- En el caso de obtención de información privada, se relaciona con el **Artículo 20. Violación de la privacidad de la data o información de carácter personal.** El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Esto se refleja en el robo de información de los pasajeros del avión por medio de sus dispositivos celulares.

- En el caso de sextorsion y revelar información, se relaciona con el **Artículo 22. Revelación indebida de data o información de carácter personal.** El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Se manifiesta en el capítulo cuando se difundió información privada de la senadora y la ciudadana.

  Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

- En el caso de sextorsion, se relaciona con el **Artículo 23. Difusión o exhibición de material pornográfico.** El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas 7 advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. En el caso que se difundieron en una pagina pornográfica las fotos de la ciudadana de los estados unidos no se tomaron precauciones para restringir el acceso a niños, niñas y adolescentes.

4. Actividades de la unidad del FBI que pueden considerarse delitos informático.

En este capítulo uno de los participantes de la unidad del FBI cometió un delito informático al enviar un mensaje con un virus troyano al hacker pagando la multa, pudiendo tomar el control de su portátil y sacar una foto con su cámara web. Esta acción realizada se considera ilegal ya que incumple con los siguientes artículos

Articulo 6. Acceso indebido: al acceder sin permiso y sin una orden judicial a una portátil.
Artículo 11. Espionaje informático: al acceder al portátil y tomar una foto con la cámara web.

Debido a esta acción, se aplicarían el **Articulo 29. Penas Accesorias:** La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica

5. Análisis éticos de los problemas y soluciones presentados.

Los problemas generados por la criminal durante el programa son bastante graves, incluso si su plan era solamente robar las tarjetas de las personas, al sabotear las conexiones de los aviones pudo causar peores consecuencias, sin sus sistemas de conexión, los aviones pudieron haber perdido su capacidad para aterrizar correctamente o para coordinar sus vuelos, este tipo de acciones pudo haber causado un accidente con cientos de muertes. En cuanto al crimen del robo y de la extorsión, tienen menos potencial destructivo en la sociedad pero el robo o el chantaje nunca son acciones tomadas con una persona integra y ética, la criminal uso su conocimiento superior en el área informática para pisotear y aprovecharse de otras personas, para tomar lo que es ajeno, en general no hay duda de que las acciones tomadas por la criminal fueron poco éticas.

En el tema de Krumitz, hay una cierta ambigüedad, algunas personas podrían decir que tomo las acciones necesarias para atrapar a la criminal y que produjo resultados, lo cual aunque es cierto, nos hace preguntarnos, si Krumitz es una persona dispuesta a romper la ley para lograr sus resultados ¿Que nos asegura que un dia no vaya hacer para un beneficio personal? ¿Que nos asegura que un dia tome acciones parecidas a la de la criminal? Nada nos lo asegura y es por eso que puede ser peligroso combatir “fuego con fuego” cuando se trata de criminales, las acciones de Krumitz fueron fuera de la ley y eso no debería quedarse sin castigo, ya que ese tipo de acciones no deberían ser incentivadas.

Conclusión

Al ver este episodio de CSI Cyber pudimos ver varios ejemplos de la nueva oleada de crímenes que se enfrenta nuestra sociedad, en esta digital la tecnología esta al servicio de todos incluso de las personas que no tienen un código de ética que se adecue a las leyes de la sociedad y utilizan sus conocimientos para obtener beneficios, sean individuales o colectivos (Ciberterrorismo), rompiendo las leyes y pisoteando a otras personas.

Como mencionamos anteriormente, el Internet es una herramienta muy poderosa y por eso es necesario que la ley regule las acciones que se pueden tomar con ella, y que se entrenen especialistas como los del equipo del programa para detectar y atrapar a estos criminales. Crímenes como estos ocurren a menor escala todos los días, desde pequeños “hacks” que entran a tu computadora dentro del programa que te bajaste hasta hackeos de cuentas e incluso cuando bajas un programa o una canción ilegalmente, casi todos somos culpables de algún crimen informático aunque no seamos conscientes de ello. En Venezuela particularmente las leyes informáticas aunque no se apliquen son fuertes, pero esto también se debe a que es un aspecto totalmente distinto de la ley y no se sabe totalmente como manejarlo ¿debería un “buhonero” cumplir los mismos años de reo que un violador? ¿ Deberían tener alguna prisión especial ? ¿ Como evitamos este tipo de crímenes sin caer en problemas de invasión de privacidad ? (como en este programa y como el escándalo de gobierno norteamericano), estos son temas que son aun no se han desarrollado del todo y que con los años deben ir adaptándose a medida que aprendemos a lidiar con las amenazas de este nuevo mundo.