RSA®

The Security Division of EMC

White paper

Defensa contra el enemigo: la lógica detrás de la creciente amenaza del crimeware

El método más popular usado para cometer fraudes financieros en los canales en línea es la apropiación de identidad. Esto ocurre cuando un estafador se adueña de una identidad o cuenta existente a fin de robar los fondos de la cuenta. La comisión de fraudes por medio de tácticas de robo de identidad tradicionales, como la creación de una nueva identidad y el incumplimiento de la devolución de un préstamo, aún existe, pero no prevalece, ya que los canales en línea ofrecen numerosas ventajas a los estafadores. Son muchas las razones por las que continúa el aumento de los delitos en los canales en línea, entre ellas:

- Accesibilidad universal: Internet permite a los estafadores operar a escala global, dándole relativamente poca importancia a la ubicación geográfica, el idioma y la nacionalidad.
- Escalabilidad: las alternativas para la apropiación de identidad son costosas en cuanto a recursos y niveles de sofisticación.
- Facilidad de operación: apropiarse de una identidad existente y personificar a un usuario genuino es una tarea sencilla.
- Anonimato: Internet permite total anonimato y dificulta el seguimiento de la verdadera identidad de un estafador.

La apropiación de identidad en el mundo en línea se lleva a cabo, tradicionalmente, por medio de tácticas de "ingeniería social", por lo general, un engaño que logra que los consumidores revelen sin darse cuenta sus credenciales personales (como nombre de usuario y contraseña). Phishing, el acto de simular ser una entidad u organización legítima (generalmente mediante correo electrónico) y dirigir a los consumidores a un sitio Web fraudulento para obtener su información personal, es el mejor ejemplo de este enfoque y el de uso más común entre los estafadores.

Hacking, que consiste en "ingresar ilegalmente" o aprovechar vulnerabilidades en un sitio de Internet para obtener acceso no autorizado, se ha idealizado en la cultura popular, pero muy pocas veces se usa como técnica para cometer delitos financieros. Hacking se suele usar como herramienta para montar la infraestructura para otro tipo de estafas (como hosting para ataques de phishing o como método para diseminar software malicioso), o para penetrar en sitios Web relativamente pequeños y desprotegidos a fin de volver a usar credenciales en sus bases de datos en sitios financieros de mayor tamaño.

Dado que las organizaciones han aprendido a administrar de manera eficaz los riesgos conocidos y que los estafadores desean mejorar su rendimiento, ha surgido un nuevo método de apropiación de identidad y cuentas: el crimeware o los troyanos financieros.

Crimeware: la amenaza de próxima generación

Crimeware es un programa malicioso que se descarga en la PC del usuario sin que este se dé cuenta, ya sea al engañar a la víctima para que lo ejecute o al aprovechar los puntos débiles de su sistema operativo, navegador u otro software instalado en la PC. Si bien existen distintas clases de software malicioso en el mundo en línea, crimeware, en este white paper, se puede definir como cualquier programa de software malicioso que cumple, al menos, uno de los siguientes criterios:

1. Robo de credenciales en línea, datos personales o cualquier otro tipo de información necesaria para la apropiación de identidad, con la intención de usar la identidad de terceros para robar fondos.

2. Ejecución de transacciones no autorizadas en línea para robar fondos: esto incluye troyanos que "secuestran" operaciones bancarias en línea u otras sesiones seguras de usuarios infectados y llevan a cabo transacciones fraudulentas después de que el usuario cierra la sesión.

Crimeware también implica acciones secundarias. Por lo general, el crimeware desactiva los sistemas protectores de la PC del usuario, como un software antivirus o un firewall personal, o usa el equipo infectado como plataforma para realizar actividades fraudulentas. Por ejemplo, algunos crimeware usan la PC infectada del usuario para enviar correos electrónicos no deseados o como un sitio host para los ataques de phishing (como parte de una red de software robotizada).

El crimeware se puede dividir en dos categorías. La primera categoría de troyanos incluye registradores de digitación, programas capturadores de pantallas y troyanos para pharming, como Torpig, Briz, Haxdoor y Gozi/Banksniff. La segunda categoría, menos común y publicitada que las demás, incluye troyanos para ataques del sistema e-gold y algunas variantes del troyano Metaphisher.

Incremento y propagación del crimeware

Para comprender el predominio del crimeware y su impacto, es necesario considerar la razón de su surgimiento desde la perspectiva de un estafador. Los delitos en línea tienden a ocurrir donde la funcionalidad propicia el comportamiento fraudulento. Los blancos de preferencia para fraudes en línea incluyen los sitios que permiten:

- Transferir fondos que son prácticamente instantáneos (las transacciones que llevan mucho tiempo se pueden considerar fraudulentas, cancelar o usar para montar una operación policial encubierta).
- Realizar lavado de dinero.
- Emular el comportamiento de un usuario real.

La evolución del crimeware es el resultado de la necesidad de dar respuesta a los dos desafíos principales que enfrenta la comunidad de estafadores con respecto a esta funcionalidad:

- Escalabilidad: “obtener mayor ganancia por menos”.
- Adaptación: superar las nuevas medidas de seguridad que las instituciones o gobiernos han implementado para combatir el fraude en línea.

En términos de escalabilidad, existen ciertos mercados y geografías donde la funcionalidad que propicia el fraude ha madurado y los métodos tradicionales para perpetrar delitos financieros no aprovechan todo el potencial del mercado para este tipo de acciones ilícitas. Por consiguiente, el crimeware se desarrolló como una forma de comprometer más credenciales de manera eficaz (frente a los métodos tradicionales de ataque), aunque esto implique una mayor inversión en infraestructura y costos operacionales. Es probable que el crimeware en sí coexista con más métodos tradicionales de fraude en línea, como phishing, reproducción de credenciales y ataques de diccionario.

Con respecto a la adaptación, gracias a la implementación de medidas, como la autenticación sólida, y a una mayor conciencia del cliente, los métodos tradicionales de ataque en línea para que el usuario dé a conocer voluntariamente sus credenciales personales han perdido eficacia y se han vuelto inútiles. En cambio, los estafadores se ven obligados a creer que el crimeware reemplazará las formas tradicionales de fraude.

Enfoque en troyanos: Torpig

Torpig: también llamado “Anserin” o “Sinowal” es una de las familias de troyanos más maliciosas (una serie de códigos maliciosos que se introducen en la computadora del usuario a fin de obtener datos personales, principalmente, por medio de credenciales bancarias en línea). Después de que el usuario se registra en un sitio, Torpig sobrescribe la página genuina (sin dejar de conservar la barra de direcciones y el SSL válido) con el mismo aspecto que el sitio original. La mayoría de los usuarios desconoce que Torpig incluso está en su computadora, ya que es muy difícil de detectar.

Torpig también recupera todos los nombres de usuario y las contraseñas guardadas en Internet Explorer, Outlook, Eudora, etc. La razón de tener credenciales, como direcciones de correo electrónico y contraseñas, es que algunas instituciones financieras envían correos electrónicos de confirmación de transacciones específicas completadas. Al tener la dirección de correo electrónico y la contraseña del usuario real, los estafadores pueden iniciar sesión en la cuenta de correo electrónico y eliminar el correo electrónico, por lo que el usuario real no se da cuenta de la transacción fraudulenta que acaba de ocurrir.

Torpig es extremadamente peligroso y se encuentra en constante evolución. Torpig no se puede eliminar de un sistema en funcionamiento dado que siempre se está ejecutando en un sistema de un usuario infectado. Además, se actualiza varias veces al día por medio del mothership, un servidor de control y comando que opera desde una ubicación desconocida mediante el uso de un canal de comunicación criptográfica, lo que dificulta aun más mitigar este tipo de crimeware.

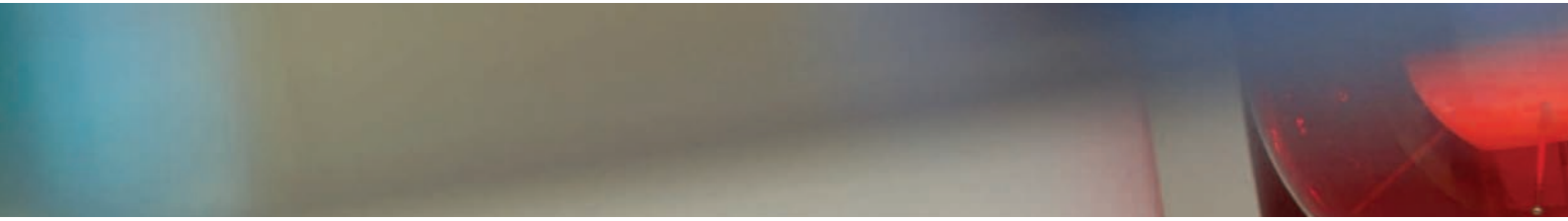
Cuantificación de la amenaza del crimeware

El predominio de troyanos y crimeware financiero aumenta a un ritmo alarmante:

- En 2006, SOPHOS detectó más de 41.000 amenazas nuevas de malware.
  - El 41% contaba con características de spyware.
  - El 42% eran descargadores diseñados para desactivar la seguridad antes de descargar el crimeware.
- Un reciente análisis de RSA de una única variante de Gozi/BankSniff arrojó un total de 30.000 usuarios infectados en un mes.
- Los costos del crimeware en el entorno de los estafadores también van en baja, lo cual indica una maduración del mercado para el código malicioso.

Para comprender cómo este análisis se traduce en un impacto real, se deben considerar varios criterios.

Ubicación geográfica: existen ciertas regiones geográficas que son casi exclusivamente afectadas por los troyanos financieros. Por ejemplo, en Alemania, más del 90% de los fraudes bancarios en línea es el resultado directo de la actividad de los troyanos. Lo mismo se puede decir para Benelux, Suiza, y otras ubicaciones geográficas. En estas áreas, las leyes y reglamentaciones exigen autenticación sólida al iniciar sesión para usar los servicios del sistema bancario en línea, lo cual hace que ataques fraudulentos simples, como phishing, reproducción de credenciales de bases de datos robadas o averiguaciones mediante el método fuerza bruta pierdan eficacia. En los países donde los tokens de contraseñas de un solo uso son comunes, se usan modalidades más sofisticadas de crimeware, como troyanos de secuestro de sesiones y sus variantes relacionadas. En los Estados Unidos, con la Guía FFIEC, que requiere que las instituciones financieras empleen autenticación sólida al iniciar sesión, es probable que los troyanos sucedan al phishing y se conviertan en la principal clase de fraude bancario en línea del futuro.



Impacto de un único ataque: para comprender el impacto de los troyanos, se debe comparar un ataque de phishing con uno de un troyano. Un ataque de phishing, por lo general, dura entre 5 horas o menos (si es Cliente del servicio antiphishing de RSA® FraudAction℠), que es un promedio de 105 horas en la industria[1]. RSA analizó recientemente los logs de un troyano llamado Gozi/Banksniff que estuvo activo durante cinco meses antes de que se lo detuviera. La mayoría de los principales proveedores de antivirus no logró detectar al troyano durante ese período; además, el troyano comprometió un promedio de 30.000 computadoras nuevas por mes (en comparación con las varias decenas de credenciales que un ataque de phishing podría producir).

Consecuencias: para las instituciones financieras, es mucho más difícil administrar el riesgo relacionado con los troyanos. Esto sucede por las siguientes razones:

- No tienen control sobre las PCs de los usuarios y no pueden exigir parches ni protección antivirus.
- A diferencia de un ataque de phishing que no se puede ocultar (se notificará con el tiempo) o de un ataque por fuerza bruta (alguna persona revisará los logs y los identificará finalmente), los troyanos pueden permanecer sin ser detectados durante meses, y así causar inconcebibles pérdidas por fraude en las instituciones financieras y la pérdida general de la confianza del consumidor en los canales en línea.
- El crimeware afecta a las instituciones financieras, aunque no de manera directa. No obstante, dichas instituciones son financieramente responsables por las pérdidas relacionadas con los ataques.

Otra manera de determinar el daño potencial del crimeware es analizar si los consumidores son propensos a ser víctimas de este tipo de ataques.

Todo usuario en línea está expuesto a descargar crimeware en su computadora. Si bien el crimeware se ha extendido tradicionalmente por medio de enlaces en correos electrónicos o archivos adjuntos, está surgiendo una tendencia más atemorizante: la diseminación de troyanos mediante sitios en línea legítimos. Esto ocurre cuando un estafador ataca un sitio legítimo e infecta a los usuarios con un troyano al solicitarles la descarga de un programa, o bien al aprovechar una debilidad en Microsoft Windows o Internet Explorer, lo cual infecta la computadora del usuario de manera silenciosa. Un buen ejemplo fue el uso del sitio Web oficial de Miami Dolphins para diseminar un registrador de digitación (crimeware que roba información ingresada por medio del navegador) durante el Super Bowl. Además, el fenómeno en constante crecimiento de Web 2.0 exacerba el potencial para que millones de usuarios se infecten sin percibirlo por medio de crimeware, ya que el contenido se comparte y se distribuye sin costo alguno por medio de la Web (por ejemplo, mediante YouTube y MySpace). Según un reciente estudio de investigación de consumidores llevado a cabo por RSA, casi la mitad de los usuarios en línea de todo el mundo están cada vez más preocupados por los troyanos y el crimeware, y se espera que esta cifra aumente considerablemente en los próximos meses.

Actividades de fondo: evolución de la tecnología del crimeware

- En la actualidad, la mayoría de los troyanos están basados en rootkit y, de a poco, se tiende a que todos sean así desde su creación.
- Los principales "proveedores" de troyanos monitorean detalladamente las más importantes compañías de antivirus para comprobar si su software es detectable. Si se detecta su crimeware, emiten una actualización "en cuestión de horas" a un costo muy bajo.
- La mayoría de los troyanos se diseñan para evadir la tecnología especial de captación "Visual Key", como teclados virtuales, teclados JavaScript y teclados basados en FLASH.
- Troyanos específicos pueden eliminar cookies, memoria caché y contraseñas con vencimiento automático de Internet Explorer, Firefox y Opera para obligar a los usuarios a que vuelvan a escribir sus credenciales personales.
- Algunos troyanos tienen la capacidad de hacer pharming local al usar el sistema API, en vez de modificar el archivo host.

1 Fuente: Anti-Phishing Working Group (APWG)

Enfoque en troyanos: Gozi/Banksniff

El troyano Gozi/BankSniff se detectó por primera vez en el 2005 y desde entonces atenta contra los clientes de las instituciones financieras y otros sitios Web, y los infecta para robar credenciales de usuarios. Gozi/BankSniff recolecta nombres de usuario y contraseñas de determinados sitios Web, incluidos los de bancos, comerciantes en línea y proveedores de servicios de correo electrónico, como Google y Yahoo! El crimeware espera a que el usuario de la computadora infectada acceda al sitio objetivo y lleve a cabo el inicio de sesión con el registro de las teclas pulsadas; de ese modo, recopila los datos de los usuarios y los envía a servidores "paralelos".

Si bien Gozi/BankSniff no es una amenaza nueva, muchos productos antivirus no pueden detectarlo, ya que cambia constantemente por medio de un proceso rápido de mutación. Asimismo, los comunicados de crimeware con el servidor paralelo y sus canales de control se pueden encriptar. El acceso remoto de control de los troyanos está protegido con contraseña, y los controladores de troyanos usan una contraseña diferente para cada computadora infectada.

En enero de 2007, RSA identificó el principal servidor paralelo de troyanos y obtuvo logs de información robada por el troyano que se recopiló durante un mes. El tamaño del archivo de log indicó que se había recopilado una gran cantidad de información en comparación con otro crimeware que RSA había detectado anteriormente. Otros hallazgos interesantes a partir del análisis de RSA son los siguientes:

- Los logs indican que los troyanos recopilaron información del navegador, direcciones IP, contraseñas y nombres de usuario de entre 50.000 y 70.000 computadoras infectadas durante un mes. La cantidad total de datos de cuentas robados durante ese período fue de 9.993.
- Los datos de ubicación geográfica IP de las víctimas indican que la base de infección de los troyanos se extendió. Durante ese mes, el troyano recopiló información de computadoras de usuarios de 160 países, principalmente en Turquía, India, Estados Unidos, Brasil, el Reino Unido y Alemania.
- El análisis de los logs indica que los dueños de los troyanos organizan los datos que recopilan en una base de datos SQL bien estructurada. La información se puede recuperar de esta base de datos en función de la dirección IP, sitio de destino y otras características de los datos.

Estrategias actuales de mitigación

El método estándar para combatir software malicioso se focaliza en las herramientas de software que se ejecutan en los equipos de las víctimas potenciales o dentro del área de acción de la organización. Esta estrategia es, por lo general, inadecuada para combatir el crimeware financiero por las siguientes razones:

1. Falta de protección directa: si bien las instituciones financieras pueden ser víctimas de ataques financieros de troyanos, no se pueden proteger directamente contra estos ataques mediante la instalación de software, ya que el software malicioso reside en las computadoras de los clientes y no dentro de su propia infraestructura. Generalmente, las instituciones financieras no pueden controlar ni imponer a los clientes el uso de software antivirus apropiado, ni tampoco garantizar que los parches y firmas estén actualizados. Si bien muchas instituciones financieras desarrollan programas y campañas a fin de educar a sus clientes acerca de cómo evitar infecciones de crimeware, en varios casos, esta estrategia no resulta demasiado exitosa.

2. Conciencia de los ataques: a pesar de que un ataque de phishing es visible y, en consecuencia, más fácil de detectar, les resulta difícil a las instituciones financieras determinar si son el blanco de crimeware. La mayoría de los troyanos son pasivos y no evidencian interacción con el usuario final, lo cual reduce la posibilidad de que un Cliente notifique actividades inusuales. Además, una institución financiera no suele poder detectar un ataque a partir de la información que se encuentra en sus propios servidores, y los proveedores de antivirus muy pocas veces publicitan cuáles son las instituciones atacadas por determinado malware (normalmente brindan información sobre el funcionamiento de malware y su eliminación). El resultado: los troyanos suelen ser la causa "misteriosa" o "silenciosa" de pérdidas por fraude no atribuidas.

3. Soluciones ineficaces: la mayoría de las soluciones antivirus son poco eficaces para proteger a los consumidores contra este tipo de troyanos, incluso cuando tienen un software antivirus instalado. ¿Por qué?

- Poco alcance: los troyanos financieros están menos diseminados que las redes de software robotizadas, spyware y otros tipos de software malicioso, lo que hace más difícil su detección. En consecuencia, los proveedores de antivirus suelen otorgar a los troyanos una baja prioridad.
- Impacto insuficiente: los proveedores de antivirus prefieren lanzar actualizaciones para malware que tiene un alto impacto en el equipo del consumidor. Dado que estos tipos de troyanos son pasivos, es probable que se les otorgue una baja prioridad de actualización.
- Urgencia: a diferencia de las redes de software robotizadas o spyware, estos tipos de troyanos actúan muy rápidamente. En el tiempo en que una compañía de antivirus demora en lanzar una actualización, se puede hacer mucho daño.

Moderación de la amenaza del crimeware

No existe una solución precisa para moderar la amenaza que representa el crimeware. Las instituciones financieras deben aplicar un enfoque por niveles que permita combinar una variedad de soluciones diseñadas para combatir la amenaza del crimeware a distintas escalas.

1. El primer punto de defensa posible yace dentro de la funcionalidad de las aplicaciones propias de la institución. Por ejemplo, la división de las transferencias de pagos en dos categorías: la primera categoría permitiría una transferencia inmediata a los beneficiarios existentes y la segunda categoría requeriría un retraso de 24 horas en la transferencia de fondos a los nuevos beneficiarios. Al implementar tales medidas, los ataques de intermediarios o “secuestro de sesiones” en tiempo real serían casi imposibles dado que es muy poco probable que el destino fraudulento de una transferencia de dinero sea uno al que el usuario legítimo haya transferido fondos anteriormente.

2. Las instituciones financieras deben emplear un servicio de suspensión e inteligencia de phishing y troyanos, como RSA® FraudAction℠, que brinda información y análisis de las nuevas variantes de crimeware que existen y la capacidad de accionar contra software malicioso si está afectando la base de clientes de una institución.

3. La implementación de una solución que brinda autenticación sólida al iniciar sesión, como RSA® Adaptive Authentication for Web, podría hacer que la mayor parte del crimeware para la recopilación de información resulte irrelevante o ineficaz.

4. Al usar la solución de monitoreo de fraudes back-end en tiempo real, como RSA® Transaction Monitoring, las instituciones financieras podrían hacer un seguimiento de las transacciones fraudulentas que resultan de la apropiación de cuentas y localizarlas, además de reducir en gran medida la capacidad de operación de los troyanos intermediarios o de secuestro de sesiones.

Información adicional

Anti-Fraud Command Center (AFCC) de RSA opera 24x7 para detener ataques de troyanos, phishing y pharming. Hasta la fecha, el AFCC detuvo más de 40.000 ataques en más de 130 países.
Para obtener más información, visite argentina.rsa.com.

Acerca de RSA

RSA, la División de Seguridad de EMC, cuenta con personal especializado en seguridad centrada en la información, lo que permite proteger la información a través de todo su ciclo de vida. RSA permite a los clientes asegurar de manera rentable los activos de información críticos y las identidades en línea (en el lugar y la etapa en que se encuentren) y administrar la información y los eventos de seguridad para aliviar la carga que impone el cumplimiento de normas. RSA ofrece soluciones líderes en la industria de verificación de identidad y control de acceso, encriptación y administración de claves, administración del cumplimiento de normas e información de seguridad, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, visite argentina.rsa.com y argentina.emc.com.

RSA y RSA Security son marcas comerciales registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. Todos los otros productos o servicios mencionados son marcas comerciales de sus respectivos dueños. ©2006-2007 RSA Security Inc. Todos los derechos reservados.

CRIME WP 0607

The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com