05/07/2012

EPR07/2012
www.enisa.europa.eu

La agencia de seguridad cibernética de la UE, ENISA; robos "High Roller" de bancos en línea revelan brechas de seguridad.

En respuesta al informe sobre "High Roller" en ciberataques, la agencia de seguridad cibernética de la UE, ENISA, informa de que muchos de los sistemas de banca en línea se basan peligrosamente en que los ordenadores sean seguros, pero en lugar de eso deberían sospechar que los ordenadores de sus clientes están infectados.

Los recientes ciberataques "High Roller" a las cuentas más ricas de los bancos y que han supuesto la pérdida de decenas de millones de dólares, han sido analizados en un informe recientemente publicado por McAfee y Guardian Analytics. El informe describe los detalles técnicos y el impacto de esta serie de ciberataques. El viejo dicho de que "*los criminales van donde está el dinero",* hoy se traduce en que *"los ladrones de bancos actúan en línea*", como ha declarado el Director Ejecutivo de ENISA, el Profesor Udo Helmbrecht. No debería ser una sorpresa que los grandes grupos del crimen organizado se dirijan a las páginas web de los bancos. Sin embargo, los ataques en línea llamaron mucho la atención debido a tres razones:

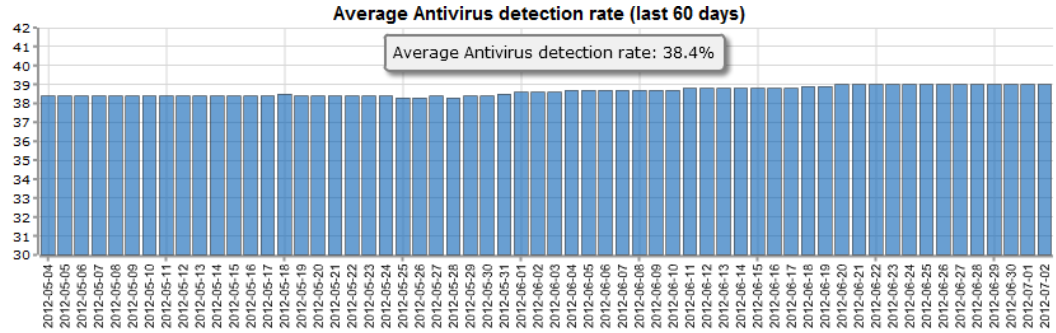
1. **Altamente Automatizados**: los atacantes redujeron al mínimo la intervención manual, basándose mayormente en la automatización. Además los ataques fueron rápidos y fáciles de pasar por alto por los usuarios.
2. **Sofisticados**: Las medidas de protección de los bancos, como la autenticación de dos factores y la detección del fraude, fueron burladas. Los usuarios no se dieron cuenta inmediatamente debido a que las transacciones fraudulentas se escondieron tras malware (insertando el código JavaScript en las páginas).
3. **Dirigidos**: Sólo los ordenadores de usuarios con saldos bancarios altos fueron atacados (por ejemplo, en torno a 5.000 ordenadores en Holanda).

Los ciberataques se hicieron en tres fases. Primero se identificaron los objetivos mediante el uso del reconocimiento en línea y el phishing. Las víctimas con acceso a cuentas bancarias con saldos elevados (de ahí el nombre de "High Rollers") fueron seleccionadas. En segundo lugar, el malware (SpyEye, Zeus e Ice 9) fue cargado en el ordenador de la víctima, personalizado de acuerdo a sus páginas web de banca en línea. El malware se activa cuando la víctima comienza una nueva sesión de banca en línea. SpyEye, Zeus e Ice 9 son los tipos de herramientas de malware más comunes y están diseñadas para este tipo de ataque. Más tarde, se realizaron transacciones fraudulentas automatizadas en nombre del usuario y escondiéndolas tras mensajes de aviso y espera. El malware transfiere las sumas de cuentas de ahorro a cuentas de cheques y entonces se envía a mulas en el extranjero que recogen el dinero en efectivo y lo envían de vuelta más adelante mediante una

transferencia de persona a persona (como Western Union). Un detallado análisis técnico y una serie de recomendaciones de McAfee y Guardian Analytics puede consultarse en línea.

Recomendaciones

1. **Dar por seguro que todos los ordenadores están infectados**: Los ataques usaron Zeus, que es un kit de virus "Házlo-Tú-Mismo" disponible por unos mil euros. Zeus ha estado al alcance de cualquiera desde 2007 y el grado de ser detectado es muy bajo[1]. Para un banco en la actual situación es más seguro asumir que los ordenadores de todos sus clientes están infectados y ,por lo tanto, que los bancos deben tomar las medidas de protección necesarias para enfrentarse a ello.



Estadísticas de Zeus: sólo alrededor del 40% de Zeus malware es detectado.

2. **Dispositivos seguros de banca en línea**: Muchos de los sistemas de banca en línea, algunos con códigos de transacción de una sola vez, calculadoras o lectores de tarjetas inteligentes, basan su trabajo en la creencia de que los ordenadores de los consumidores no están infectados. Dado el estado actual de la seguridad de los ordenadores, esta creencia resulta peligrosa. **Por el contrario, los bancos deben asumir que los ordenadores están infectados, y por ello tomar las medidas necesarias para proteger a los consumidores de transacciones fraudulentas.** Por ejemplo, un sistema básico de autenticación de dos factores no previene los ataques sobre las transacciones de tipo "man-in-the-middle" o "man-in-the-browser"[2]. Por lo tanto, es **importante cruzar las verificaciones** de los valores y destinos de ciertas transacciones con el usuario, a través de un canal seguro o de un **dispositivo seguro** (por ejemplo un mensaje de texto, una llamada telefónica, un lector de

[1] *La tasa de detección de Zeus binarios es de un 38.4%. En otras palabras, incluso si se aplican programas de antivirus actualizados, hay muchas posibilidades de estar infectado.*

[2] *Incluso si el usuario tiene que teclear un código nuevo y secreto cada vez para autentificar una transacción al servidor, el atacante puede interceptor el código y reemplazarlo en el servidor para ejecutar una transacción fraudulenta.*

tarjetas independiente con pantalla). Incluso los smartphones podrían ser utilizados en esto, dotando a los smartphones de una seguridad que resista los ataques.

3. **Una cooperación estrecha es necesaria para acabar con los centros mundiales de comandos:** Los ciberataques son llevados a cabo usando servidores de comandos y control dinámicos localizados en todo el mundo, usando por ejemplo botnets de flujo rápido (fast flux botnets)[3] y proveedores de hosting a prueba de balas[4]. Los criminales usan estos trucos para hacer que la aplicación de la ley y los procesos de notificación y desmontaje sean más complicados. **Por lo tanto, una cooperación global fuerte, tanto en términos de prevención como de responsabilidad, es necesaria**. ENISA trabaja fomentando vínculos más estrechos y un mayor intercambio de información entre los equipos nacionales de respuesta a emergencias informáticas (CERTs en sus siglas en inglés), los agentes del orden y los países de la UE para mejorar la respuesta a incidencias a través de fronteras.

La prevención de ciberataques es importante, pero también es necesario estar preparado cuando los ataques suceden. ENISA ha estado trabajando con los diferentes Estados miembros de la UE para garantizar que los CERTs de todos los países funcionan correctamente para manejar las incidencias en seguridad cibernética. ENISA organiza ejercicios de seguridad cibernética a gran escala internacional (por ejemplo, Europa Cyber 2010, Cyber del Atlántico 2011 o la próxima Europa Cyber 2012) para incrementar la colaboración internacional en incidencias de seguridad a gran escala. ENISA está trabajando además con Estados miembros para mejorar la notificación de incidencias y asegurar mayor transparencia sobre las causas, la frecuencia y el impacto de incidencias pasadas. Actualmente, consumidores, negocios y responsables políticos se ven obligados a hacer cálculos aproximados. La CE anunció recientemente una futura estrategia de seguridad en Internet, frente a la posibilidad de ampliar el Artículo 13 bis (obligatoriedad de notificación de incidencias y medidas de seguridad obligatorias) más allá del sector de las simples comunicaciones electrónicas.

Mirando al futuro, la seguridad del navegador y la seguridad de los teléfonos inteligentes (smartphones) jugarán un papel cada vez más importante a medida que más y más transacciones se realicen a través de los smartphones o tablets. La rápida adopción de los smartphones ofrece una importante oportunidad para mejorar la seguridad de punto final (por

[3] *El Flujo rápido (Fast Flux) es una técnica donde el nombre de un dominio señala una larga y rápida combinación de campios de un conjunto de direcciones IP (por ejemplo, en ordenadores).*

[4] *"Proveedores de hosting a prueba de balas" (o Bulletproof hosting providers" en inglés) es un término que se refiera a un proveedor sin condiciones para revisar el material cargado. Los criminales cibernéticos utilizan hosting a prueba de balaspara albergar servidores de mando y control, los sitios de infección por malware, sitios de phising y demás.*

ejemplo mediante el uso de tiendas de aplicaciones aprobadas o de smartphones como segundos factores) pero no deberíamos dar por sentada la seguridad del smartphone[5].

Para entrevistas: Ulf Bergstrom, Portavoz de ENISA, press@enisa.europa.eu, Teléfono móvil: + 30 6948 460 143, o cert-relations@enisa.europa.eu

Traducción. La versión original en inglés es el documento auténtico.
www.enisa.europa.eu

[5] *Tenga en cuenta que mientras vemos que muchos fabricantes de teléfonos inteligentes han tomado la oportunidad demejorar la seguridad de los ordenadores, debemos advertir de que ya ha habido casos en los que los criminales han infectado tanto el ordenador como el smartphone de la víctima para eludir los sistemas de autentificación de dos factores basados en mensajes de texto usando Zitmo.*