EL CRIMEN ORGANIZADO SE TRASLADA AL ROBO DE DATOS

Crecen a una cifra récord los robos de numeración de tarjetas de crédito y otros tipos de datos sensitivos en las redes de compañías.

Usted mantiene los programas maliciosos alejados de su PC y es suficientemente conocedor para evitar los ataques de phishing. Tiene la precaución de navegar por sitios de confianza y sabe cómo realizar transacciones bancarias en línea. Por lo tanto, sus datos financieros deberían estar relativamente seguros, ¿verdad?

Se equivoca. La cifra récord que alcanzan los robos de números de tarjeta de crédito y de otros datos digitales valiosos de instituciones financieras parece burlarse de estas medidas para protegernos; y muchos de los atracos son perpetrados por grupos de criminales organizados. Y los individuos no pueden impedir que los piratas saqueen electrónicamente las redes de un banco o de un procesador de tarjetas de crédito, ya que estos penetran en la red de la compañía por un agujero olvidado, pero fácil de aprovechar, con el fin de desatar programas maliciosos que se encargan de robar la numeración de tarjeta de crédito y números de identificación personal (PIN) a los cajeros automáticos.

“No me preocupan tanto los interceptores de pulsaciones de teclas, sino los robos de datos”, explica Joe Stewart, quien investiga los programas maliciosos para el proveedor de seguridad de negocio SecureWorks. “Opero bajo la suposición de que los criminales ya tienen mis números de tarjeta de crédito, de las tarjetas de débito y los PIN, pero que no han llegado a usarlas porque tienen tanta cantidad de datos en los que trabajar”.

LOS ROBOS SUBEN COMO LA ESPUMA

Según el informe Data Breach Investigations Report 2009 de Verizon Business (find.pcworld.com/62872), los ladrones se apoderaron de 285 millones de registros en 2008, más de lo que Verizon Business había encontrado en los cuatro años anteriores combinados. La compañía basó su informe en investigaciones públicas y otras privadas de los principales robos reportados en compañías importantes, para lo cual se enfocaron en aquellos ataques donde los delincuentes tuvieron éxito y se hicieron de las numeraciones de tarjeta de crédito u otros datos. Los hallazgos coinciden con informes de mayor alcance del Identity Theft Resource Center (idtheftcenter.org), el cual reporta que número total de allanamientos de datos, que varía desde portátiles extraviadas hasta robos masivos de datos, saltó a un 47 por ciento en 2008 con 656 allanamientos reportados, una cifra superior a los 446 de 2007.

Los responsables de la mayoría de los robos son los ladrones en busca de ganancias: “El 91 por ciento de todos los registros robados en 2008 se atribuye a la actividad delictiva organizada”, indica el informe. Peter Tippett, autor principal del informe y

vicepresidente de innovación y tecnología de Verizon Business, dice que el estudio tomó en cuenta las direcciones IP usadas en los robos, además de los arrestos efectuados y los que se harán como resultado de investigaciones. La compañía coordinó frecuentemente sus investigaciones con agencias policiales como el FBI y Scotland Yard.

De los 90 allanamientos estudiados como fundamento del informe, 68 procedían de una dirección IP y un lugar particular, y Europa del Este fue la fuente más común. “Tenemos muchas evidencias de que la actividad delictiva en Europa del Este es obra del crimen organizado”, dice Tippet. La fuente más común en segundo lugar fue Asia Oriental, seguida por América del Norte.

Hoy, los ladrones de datos en línea de no se limitan simplemente a ejecutar rastreos automáticos para aprovecharse de cualquier agujero que encuentran en las redes. Lo más probable es que primero seleccionan un blanco específico cuyos datos puedan ser convertidos en dinero efectivo, y después planifican cómo entrar, dice Tippett. Con frecuencia encuentran un punto fácil para entrar, por ejemplo, una conexión de acceso a la Internet que emplea una contraseña predeterminada.

Incluso en los pocos casos donde los piratas se enfocaron en un agujero específico de software, no atacaron nuevas fallas potencialmente desconocidas por los profesionales de TI. De los seis casos en los cuales Verizon Business reportó un ataque centrado en el software, cinco aprovecharon vulnerabilidades que ya tenían correcciones disponibles por más de un año; la solución para el sexto existía desde hacía seis meses.

Una vez dentro, los malhechores por lo general insertaban programas maliciosos para evadir el software de seguridad, en lugares que les ayudaban a profundizar más en la red, o en ubicaciones que permitían robar y enviar datos una vez que llegaban al blanco de sus ataques.

Un allanamiento exitoso puede persistir por meses y recopilar muchos más datos que una simple numeración de tarjetas de crédito. “Ahora el billete gordo está en robar los PIN junto con las cuentas de crédito y de débito”, según el informe. “Estos ataques basados en los PIN golpean al consumidor mucho más fuerte...porque este tipo de fraude típicamente involucra retirar el efectivo directamente de la cuenta del consumidor”.

¿Qué esperanza hay para los consumidores?

Muchas compañías tienen sistemas de vigilancia de fraudes para detectar, por ejemplo, los intentos de usar el número de una tarjeta de crédito robada. Estos sistemas frecuentemente encuentran las primeras pistas de un allanamiento de datos, dice Tippett. Pero la detección del fraude tiene lugar sólo después de ocurrido el robo; y las personas no pueden hacer mucho para proteger sus datos antes de ese momento.

Aún así, usted puede mitigar el daño potencial de un allanamiento. Detectar tempranamente el robo de identidad puede hacer la gran diferencia a la hora de

recuperarse de un ataque; y hay servicios como Mint.com o Rudder (rudder.com) que pueden consolidar las transacciones de múltiples cuentas de cheques de ahorro y de tarjetas de crédito en un solo lugar donde usted puede detectar anomalías. La mayoría de las cuentas financieras en línea le permiten recibir una alerta por correo electrónico o SMS para diversos cargos o transacciones. Vea find.pcworld.com/62879 para más información sobre estas alertas y servicios.

Por Erik Larkin

PC WORLD