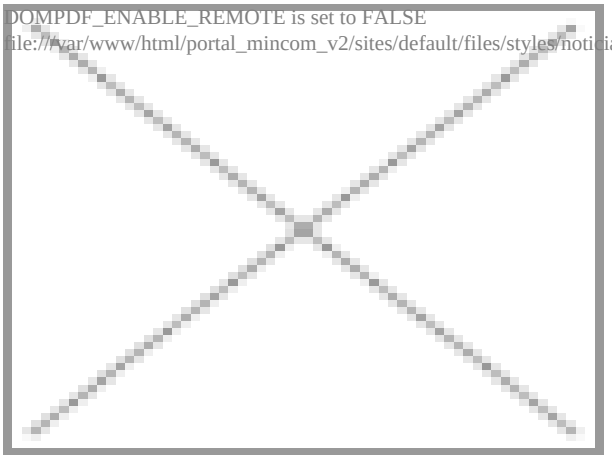
Ministerio de Comunicaciones
Published on *Ministerio de Comunicaciones* (https://www.mincom.gob.cu)



Fuente:
TIC Beat

El mito de la operativa de seguridad infranqueable sobre el sistema de pagos interbancarios se desmonta, aunque el problema no es de SWIFT, sino de la forma en la que se custodian las credenciales de los clientes.

Muchos podrían pensar que, para un ciberdelincuente, es mucho más efectivo hackear las cuentas de muchos pequeños usuarios de un banco y hacerse “minitransferencias” para no hacer saltar las alarmas. Sin embargo, el fraude bancario mayorista también tiene su público.

No sólo porque el importe de sus robos ascienda a cifras mucho más elevadas, sino porque planta cara al sistema financiero internacional tal y como lo conocemos.

Hace unas semanas, una banda de ciberdelincuentes perpetró uno de los mayores robos de la historia: lograron ejecutar con éxito una táctica de intrusión en los equipos informáticos del Banco Central de Bangladesh. Gracias a ello, pudieron hacerse con las credenciales que les permitieron impersonarse con el banco en el mercado mayorista de capitales.

Una vez hecho, bombardearon el Banco de la Reserva Federal de Nueva York con más de 40 órdenes de transferencia de fondos desde la cuenta del banco a diferentes entidades de Filipinas y Sri Lanka.

Una de las claves de este tipo de actos es no levantar sospechas, pero la quinta orden de transferencia hizo saltar las alarmas de los responsables debido a que los delincuentes deletrearon una palabra en inglés de forma errónea. Igualmente, otro de los motivos que hicieron sospechar a las autoridades era el breve espacio de tiempo entre una y otra transacción.

Al final, los ciberdelincuentes robaron un total de 80 millones de dólares y consiguieron quedarse con el botín. Se aprovecharon de la laxa legislación que existe en los casinos de Filipinas, ya que ésta les exime de tener que identificar el origen de los fondos de sus clientes.

Pero lo más importante de todo es que, el resto de las órdenes que se impidieron, ascendían a la "módica" cifra de 800 millones de dólares.

La banda que perpetró este ataque es conocida como Lazurus, y está especializada en ejecutar transacciones fraudulentas sobre la red SWIFT, obteniendo un peligroso nivel de acceso.

El modus operandi es sencillo: infectan un ordenador de algún empleado de la compañía que quieren perpetrar y, a partir de ahí, van escalando privilegios de acceso en la red corporativa hasta que consiguen el acceso a SWIFT.

Pero, ¿Qué es la red SWIFT? Se trata de una red de transferencias financieras mayoristas que, hasta hace unos años, utilizaban exclusivamente las entidades financieras para ordenar y ejecutar transferencias inmediatas y seguras. Los estándares de protección, así como su compleja burocracia y la arquitectura que le da soporte, están entre los mejores considerados del mundo dentro del sector.

Las entidades financieras a nivel mundial estaban bastante seguras de su impenetrabilidad, hasta que hace unos años la red SWIFT decidió diversificar su negocio e integró también a grandes compañías no financieras con necesidades de mover grandes cantidades. Por eso, este falso mito de la seguridad financiera perfecta se ha ido desvaneciendo.

A pesar de ello, hemos de decir que el problema no es de la red SWIFT, sino de la forma en la que se custodian las credenciales de los usuarios.

Una de las bandas especialistas en realizar este tipo de ataques es la anteriormente citada, Lazarus. La policía sospecha que podría estar relacionada con el opaco régimen de Corea del Norte, y que podría estar sirviendo a sus intereses más allá del robo financiero.

Y es que, debido a la similitud del modus operandi, así como a la utilización de algunas líneas de código que coinciden en distintos ataques, algunos atribuyen a esta banda la autoría de diversos ataques perpetrados contra los gobiernos de EEUU y Corea del Sur. Adicionalmente, también se les involucra en el escándalo de Sony Pictures y la película La Entrevista.

Disponible en: http://www.ticbeat.com/seguridad/el-sistema-de-pagos-interbancario-swift-nuevo-objetivo-de-hackers/ [1]

Links
[1] http://www.ticbeat.com/seguridad/el-sistema-de-pagos-interbancario-swift-nuevo-objetivo-de-hackers/