



Alerta Internacional de Cibertaque

Risk Advisory | Noticias Relevantes

El **12 de agosto** el **FBI** advierte a los bancos sobre un posible cibertaque global hacía los cajeros automáticos, un fraude conocido como **"ATM Cashout"** en el cual los atacantes utilizan tarjetas clonadas en los cajeros alrededor del mundo para extraer **millones de dólares** en cuestión de horas, así mismo el FBI indica que esto provocará operaciones ilimitadas que comprometerán a instituciones financieras o procesadores de tarjetas con este malware, en el cual accederán a las cuentas e información de los cuenta-habientes de dichas instituciones, así como podrán obtener acceso a las redes habilitando un robo de fondos a los cajeros a gran escala.

El **13 de agosto** **COSMO Co-Cooperative Bank** un banco de la India, fue uno de las instituciones que sufrieron dicho ataque, donde varias fuentes confirman que la alerta del FBI estaba relacionada con una violación a dicho banco, según múltiples fuentes de noticias, los ladrones que usaron tarjetas clonadas ejecutaron unas 12,000 transacciones y robaron aproximadamente **\$ 13.5 millones** de cuentas Cosmos a través de 25 cajeros automáticos ubicados en Canadá, Hong Kong e India.

Los ciberdelincuentes suelen crear copias fraudulentas de tarjetas legítimas mediante el envío de datos de tarjetas robadas a los conspiradores que imprimen los datos en tarjetas de banda magnética reutilizables, como las

tarjetas de regalo compradas en tiendas minoristas”, advirtió el FBI. “En un momento predeterminado, los co-conspiradores retiran los fondos de la cuenta de los cajeros automáticos que usan estas tarjetas”.

Todas las operaciones virtuales de **ATM cashout** son realizadas los fines de semana, por lo regular justo después de que las instituciones financieras cierran el día sábado. El mes pasado, **KrebsOnSecurity** publicó una historia sobre una aparente operación ilimitada utilizada para extraer un total de **\$ 2.4 millones** de cuentas en el Banco Nacional de **Blacksburg** en dos retiros separados de cajeros automáticos entre mayo de 2016 y enero de 2017.

Los ciberdelincuentes de los bancos de Blacksburg volvieron a atacar el sábado 7 de enero y hasta el lunes 9 de enero 2018 logrando retirar casi **\$ 2 millones** en otra operación ilimitada de retiro de efectivo en cajeros automáticos.

El FBI está exhortando a los bancos a que revisen cómo manejan la seguridad, como la implementación de requisitos sólidos de contraseña y la autenticación de dos factores mediante un token físico o digital cuando sea posible para los administradores locales y las funciones críticas del negocio.

Entre otras recomendaciones del FBI se encuentran:

- La implementación de una lista blanca de aplicaciones para bloquear la ejecución de malware.
- Monitoreo para la presencia de protocolos de red remotos y herramientas administrativas utilizadas para pivotar de nuevo en la red y realizar la post-explotación de una red, como Powershell, cobalt strike y TeamViewer.
- Monitoreo para tráfico encriptado (SSL o TLS) viajando sobre puertos no estándar, así como monitorear el tráfico de red a las regiones en las que no esperaríamos ver conexiones salientes de la institución financiera.

Lo anterior nos lleva a la pregunta ¿Estamos preparados para este tipo de ataques? ¿Contamos con las herramientas necesarias?

Referencia:

<https://krebsonsecurity.com/2018/08/fbi-warns-of-unlimited-atm-cashout-blitz/>

<https://www.news18.com/news/tech/hackers-dupe-cosmos-co-operative-bank-of-rs-94-cro-re-1844475.html>

Contactos

Emilio Sandoval
Socio Risk Advisory
esandoval@deloitte.com

Ingrid Fuentes
Gerente Risk Advisory
iefuentes@deloitte.com

Deloitte se refiere a una o más de las firmas miembro de Deloitte Touche Tohmatsu Limited (“DTTL”), su red global de firmas miembro, y sus entidades relacionadas. DTTL (también denominada “Deloitte Global”) y cada una de sus firmas miembro son entidades legalmente separadas e independientes. DTTL no presta servicios a clientes. Por favor, consulte www.deloitte.com/about para una descripción más detallada.

Deloitte es un proveedor líder mundial de servicios de auditoría y aseguramiento, consultoría, asesoría financiera, gestión de riesgos, impuestos y servicios relacionados. Nuestra red de firmas miembro en más de 150 países y territorios atiende a cuatro de cada cinco compañías del Fortune Global 500®. Conozca cómo las aproximadamente 264,00 personas de Deloitte generan un impacto que trasciende en www.deloitte.com.

Este documento sólo contiene información general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro, ni ninguna de sus afiliadas (en conjunto, la “red Deloitte”), presta asesoría o servicios profesionales por medio de esta publicación. Antes de tomar cualquier decisión o medida que pueda afectar sus finanzas o negocio, debe consultar a un asesor profesional calificado. Ninguna entidad de la red Deloitte será responsable por cualquier pérdida que pueda sufrir cualquier persona que confíe en este documento.