El programa ya habría atacado en Colombia y México.

LLAMADO ATMJADI:

NUEVO *MALWARE* TIENE EN LA MIRA A CAJEROS AUTOMÁTICOS DE AMÉRICA LATINA

Una nueva muestra de *malware* especializado en ataques a cajeros automáticos (ATM) fue advertida por la empresa de ciberseguridad Kaspersky. De acuerdo a la compañía, la actividad de este programa ya ha sido detectada en Colombia y México, por lo que su destino sería el mercado latinoamericano. Bautizado como ATMJaDi, su objetivo es vaciar los cajeros automáticos infectados, es decir, que expulse todo el dinero que posee en su interior.

"El hecho que el *malware* cuente con el mensaje en español y portugués es una gran alerta para los bancos de la región", dice Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para América Latina de Kaspersky.

Además, según la empresa, el hecho de que los ataques de este *malware* se centren en un subconjunto específico de ATM sugiere que posiblemente este haya sido creado por *insiders* con acceso al código fuente de un banco en particular y, por ende, a la red donde están conectados los cajeros automáticos.

APP

Keeper

Gestor de contraseñas y almacén digital de estas. La *app* genera, almacena y rellena automáticamente claves fuertes, a la vez que protege al usuario en todos sus dispositivos y guarda de forma segura los documentos privados. La función Auditoría ayuda a identificar qué cuentas requieren de una actualización de contraseñas, mientras la función Acceso de Emergencia permite elegir hasta cinco personas de confianza que pueden acceder a la cuenta en caso que el usuario no pueda.

Glos@rio

Firma

Cuando se habla de la firma de un virus o de un *malware*, se refiere a una serie de datos que lo identifican y permiten su detección por parte de un antivirus. Lamentablemente, como explica Kaspersky en su blog, actualmente las firmas no son suficientes para reconocer un archivo malicioso, ya que muchas de las amenazas nuevas utilizan cada vez formas más sofisticadas de ocultar su presencia y accionar.

VISITA A LAS OFICINAS DE CIBERSEGURIDAD DE DELOITTE CHILE:

Cómo se infiltra la *deep web* en un centro de ciberinteligencia

Deloitte, más conocida por sus labores de auditoría, opera desde hace dos años un centro de seguridad digital en sus oficinas de Las Condes, que trabaja en conjunto con centros homólogos en Canadá.

RAMÓN RIVERA NOTARIO

Trabajan a la par con otros tres centros de ciberseguridad en Canadá, y para comunicarse en vivo con ellos tienen la que denominan *"war room"* ("sala de guerra"), que cuenta con un muro repleto de pantallas. Pantallas que también abundan en el salón contiguo, donde realizan su labor todos los días los cerca de 25 analistas del Centro de Ciberinteligencia (CIC) de Deloitte en Chile.

Nicolás Corrado, socio líder de Ciberseguridad de Deloitte, explica que llevan dos años operando con este CIC en Chile, que depende de Deloitte Canadá y es el único de la empresa en Sudamérica. "Globalmente se evaluó entre Argentina, México y Chile, y terminó elegido Chile", señala Corrado, y añade que en conjunto con los centros de Canadá sirven a cerca de 70 clientes en América, con un total de alrededor de 200 empleados.

Nicolás Corrado explica que el CIC chileno, junto con los canadienses, trabaja con clientes como Air Canada, para la cual realiza pruebas de hackeo de sus aviones.

Sus labores se definen en cuatro pilares, según explica el ejecutivo: En el primero, denominado "Estrategia", asesoran a los clientes para definir su estrategia de ciberseguridad, incluyendo evaluar su nivel de defensa. El segundo es "Seguridad", que fija controles para proteger infraestructuras, gestionar vulnerabilidades, y proteger la privacidad de la información, entre otros.

Los dos últimos pilares que define la empresa son "Alerta", que monitorea, detecta, advierte y gestiona potenciales amenazas a los clientes, y "Resiliencia", pilar que se encarga de la respuesta a un incidente o emergencia.

70 CLIENTES trabajan con el CIC de Deloitte en Chile, en conjunto con los de Canadá.

Cacería e infiltración

El *threat hunting* o cacería es una de las acciones de ciberinteligencia que realizan en el CIC. Énida Casanova lleva a cabo este procedimiento, que puede detectar ataques en curso o vulnerabilidades basado en comportamientos sospechosos.

"Creamos alertas específicas, modelando o emulando el comportamiento de cierto tipo de amenazas", explica la analista. Así, los expertos reciben un aviso cuando se detecta un comportamiento potencialmente peligroso, como la conexión a sitios web maliciosos y la descarga no solicitada de archivos.

Parte de la información que se utiliza en la cacería proviene del monitoreo que realiza la propia firma tanto de las redes sociales como de la *deep web* (porciones de internet no indexadas por motores de búsqueda) y *dark web* (sitios a los que solo se puede acceder con autorizaciones específicas). Eso sí, explica Cristián Gorena, gerente de ciberseguridad, no basta con observar, por lo que recurren a la infiltración.

"Tenemos analistas especializados que van creando *fake personas*, personajes digitales falsos. Por ejemplo, si queremos ver qué está pasando en la banca, generamos el perfil de Facebook de una persona de 30 a 40 años que odia la banca, que sigue a grupos que odian la banca, y así podemos entrar a círculos donde puede estar el adversario de nuestro cliente", indica el experto.

Más difícil es la infiltración en la *deep web*. "Necesitas acceso a los lugares donde están los atacantes, foros rusos que son con invitación", expone Gorena. Y añade: "Tenemos que crear una persona con cierta reputación. Ellos te desafían, debes demostrar qué has hecho, tus credenciales, qué puedes aportar al grupo. Lograr una posición en ellos tiene mucho valor, por eso protegemos nuestras fuentes. Cuando alertamos a nuestros clientes de lo que encontramos, no podemos revelar cuándo o quién lo dijo".

Parte del monitoreo involucra recopilar grandes cantidades de información, la que filtran según lo que se esté buscando como, por ejemplo, rangos de tarjetas de crédito de algún cliente, para saber si su información ha sido robada. Además, explica Corrado, realizan monitoreo de usuarios VIP y de posibles intentos de levantar sitios web falsos pero parecidos a los reales de un cliente, para realizar *phishing*.

Preocupaciones de seguridad de los consumidores en Chile

Fuente: Índice de Seguridad de Unisys 2019

SEGÚN LOS ENCUESTADOS EN EL ÍNDICE DE SEGURIDAD DE UNISYS 2019:

81% de chilenos dice haber vivido o conocer alguien que sufrió una amenaza digital

RAMÓN RIVERA NOTARIO

En 2019, Chile fue incluido por primera vez en el Índice de Seguridad que realiza a nivel mundial la firma de tecnologías de la información Unisys, que encuesta entre 1.000 y 1.500 personas en cada uno de los 13 países del estudio.

Los resultados ubicaron a Chile como el cuarto país con mayor nivel de preocupación de seguridad, solo superado por México, Colombia y Filipinas. Esto se explicaría, señaló durante la presentación del estudio Eduardo Almeida, vicepresidente y gerente general para Latinoamérica de Unisys, por un mayor temor de los chilenos frente a su seguridad digital, debido a vivir en una sociedad con un mayor grado de desarrollo tecnológico. De hecho, en el informe se señala que el 81% de los chilenos ha vivido o conoce a alguien que ha experimentado al menos un tipo de amenaza o advertencia cibernética.

El mayor nivel de preocupación de los cuatro ítems en que se organiza el estudio, se reflejó en Seguridad Financiera, con 229 puntos; seguido del de Seguridad Personal, Seguridad de Internet y en último lugar la Seguridad Nacional. Así, las principales preocupaciones estuvieron en torno al fraude, hackeos, *phishing* y robo de identidad (ver infografía).