KASPERSKY lab

Ciberamenazas a las instituciones financieras para 2019:

PANORAMA Y PREDICCIONES

CONTENIDO

INTRODUCCIÓN. ACONTECIMIENTOS CLAVES EN 2018

El año pasado fue muy activo en cuanto a las amenazas digitales que enfrentaron las instituciones financieras: los grupos de ciberdelincuencia usaron nuevas técnicas de infiltración y la geografía de los ataques se extendió.

A pesar de todo esto, comenzaremos la revisión con una tendencia positiva: en 2018, las fuerzas policiales arrestaron a varios miembros del reconocido grupo de ciberdelincuencia responsable de Carbanak/Cobalt y Fin7, entre otros. Estos grupos han participado en ataques a docenas, si no cientos, de empresas e instituciones financieras en todo el mundo. Desafortunadamente, el arresto de los miembros del grupo, entre los que se encontraba el líder de Carbanak, no logró detener por completo sus actividades. De hecho, fue el inicio del proceso de división de los grupos en unidades más pequeñas.

El actor más activo durante 2018 fue Lazarus. Este grupo está ampliando su arsenal de herramientas de forma gradual y está en la búsqueda de objetivos nuevos. Su área actual de interés incluye bancos, compañías de tecnología financiera, cambio de criptomonedas, terminales PoS y cajeros automáticos. En términos geográficos, hemos registrado intentos de infección en docenas de países, principalmente en Asia, África y América Latina.

Hacia finales del año pasado, notamos que debido a la falta de madurez de sus sistemas de seguridad, el riesgo para las nuevas compañías de tecnología financiera y de cambios de criptomonedas eran mucho mayores. Estos tipos de compañías fueron el objetivo más frecuente. El ataque más creativo durante 2018, desde nuestro punto de vista, fue AppleJeus, que apuntó a los corredores de criptomonedas. En este caso, los ciberdelincuentes crearon un software especial con apariencia y funciones legítimas. No obstante, el programa también cargaba una actualización mal intencionada que resultó ser una puerta trasera. Este es un tipo nuevo de ataque, que infecta a sus objetivos través de la cadena de suministro.

Para continuar con el tema de los ataques a las cadenas de suministro, vale mencionar al grupo MageCart que este año, con la infección de las páginas de pago de los sitios web (entre ellos, los sitios de grandes empresas como British Airways), accedió a una enorme cantidad de datos de pago con tarjeta.

Este ataque fue aun más efectivo porque los delincuentes eligieron un objetivo interesante: Magento, una de las plataformas más populares para las tiendas en línea. Aprovechando las vulnerabilidades de Magento, los delincuentes pudieron infectar docenas de sitios con una técnica que, probablemente, otros grupos adoptarán.

También debemos mencionar el desarrollo de familias de malware para cajeros automáticos. En 2018, los especialistas de Kaspersky Lab descubrieron seis familias nuevas, lo que significa que, en la actualidad, hay más de 20 de ellas. Algunas familias de malware para cajeros automáticos también han evolucionado, por ejemplo, el malware Plotus, originado en América Latina, se actualizó a una versión más reciente, Peralda, ganando así nueva funcionalidad. El mayor daño asociado con los ataques a los cajeros automáticos fue provocado por las infecciones a las redes internas de las entidades bancarias, como FASTCash y ATMJackPot, que permitió a los atacantes acceder a miles de cajeros automáticos.

En 2018 también se vieron ataques a organizaciones que usan sistemas bancarios. En primer lugar, nuestro análisis conductual basado en el aprendizaje mecánico detectó diversas olas de actividad mal intencionada en relación con la propagación del troyano bancario Buhtrap, este año, ya que los atacantes insertaron su código en foros y sitios de noticias populares. En segundo lugar, detectamos ataques a los departamentos financieros de las compañías industriales, donde pagos de cientos de miles de dólares no levantarían muchas sospechas. En las etapas finales de este tipo de ataques, los atacantes suelen instalar herramientas de administración remotas en las computadoras infectadas, como RMS, TeamViewer y VNC.

Antes de dar nuestros pronósticos para 2019, veamos cuán exactas fueron las predicciones para 2018.

- **Ataques mediante tecnologías subyacentes de la cadena de bloques de los sistemas financieros implementados por las mismas instituciones financieras:** esto no sucedió en el campo financiero, pero sí se observó en el sector de casinos en línea.
- **Más ataques a las cadenas de suministro en el mundo financiero:** sí

- **Ataques a las redes sociales masivas (entre otros, cuentas de Twitter, páginas de Facebook, canales de Telegram) incluyendo accesos ilegales y manipulación para obtener ganancias financieras a través del mercado de cambio de criptomonedas o la bolsa:** sí
- **Automatización de malware en cajeros automáticos –** sí. Por ejemplo, existen programas mal intencionados que dan dinero inmediato a los atacantes.
- **Más ataques a las plataformas de cambio de criptomonedas:** sí
- **Un pico en el fraude a las tarjetas tradicionales debido a la gran vulneración de datos que se produjo el año anterior:** no
- **Más ataques patrocinados por naciones/estados contra organizaciones financieras:** sí
- **Inclusión de tecnologías financieras y usuarios móviles a los ataques: una caída en la cantidad de troyanos bancarios tradicionales en Internet orientados a las computadoras. Los usuarios nóveles de banca móvil son el nuevo objetivo principal de los ciberdelincuentes:** sí. En particular, algunos troyanos bancarios dejaron de atacar a los usuarios de banca móvil mediante computadoras, mientras que la cantidad de troyanos que atacó a los usuarios de dispositivos móviles aumentó más del doble durante el año pasado.

PREDICCIONES PARA 2019

- **Surgimiento de nuevos grupos debido a la fragmentación de Cobalt/ Carbanak y Fin7: nuevos grupos, nuevas geografías**

El arresto de los líderes y los miembros independientes de los principales grupos de ciberdelincuencia no ha logrado detener los ataques a instituciones financieras. Es posible que el próximo año veamos la fragmentación de estos grupos y la creación de nuevos grupos por miembros antiguos, lo que llevará a la intensificación de los ataques y la expansión del área geográfica de las víctimas potenciales.

Al mismo tiempo, los grupos locales ampliarán sus actividades, lo que aumentará la calidad y la escala. Parece razonable asumir que algunos miembros de los grupos regionales se pondrán en contacto con los miembros antiguos del grupo Fin7 o Cobalt para facilitar el acceso a los objetivos regionales y ganar nuevas herramientas para perpetrar sus ataques.

- **Primeros ataques a través del robo y el uso de datos biométricos**

Diversas instituciones financieras están implementando sistemas biométricos para la identificación y la autenticación de usuarios, pero ya se han producido importantes filtraciones de datos biométricos. Estos dos hechos sientan las bases de los primeros ataques POC (Prueba de concepto) a los servicios financieros usando datos biométricos filtrados.

- **El surgimiento de nuevos grupos locales que atacan a instituciones financieras en la región indo-paquistaní, el sudeste de Asia y el centro de Europa**

La actividad de los ciberdelincuentes en estas regiones está en crecimiento permanente: los factores que contribuyen a esto son la falta de madurez de las soluciones de protección que aplica el sector financiero y la rápida propagación de los distintos medios de pago electrónico entre la población y las empresas de estas regiones. En la actualidad, se han dado todos los requisitos previos para el surgimiento de un nuevo centro de amenazas financieras en Asia, además de los tres centros ya existentes en América Latina, la península de Corea y la antigua Unión Soviética..

- **Continuación de ataques contra la cadena de suministro: ataques contra pequeñas empresas que prestan sus servicios a instituciones financieras en todo el mundo**

Esta tendencia seguirá vigente en 2019. Los ataques contra proveedores de software resultaron efectivos y permitieron a los atacantes obtener acceso a diversos objetivos importantes. Los primeros afectados serán las pequeñas empresas (que prestan servicios financieros especializados para los actores más grandes), como los proveedores de sistemas de transferencia de dinero, los bancos y las casas de cambio.

- **La ciberdelincuencia tradicional se enfocará en objetivos más sencillos y en evadir las soluciones antifraude: los ataques contra sistemas de pagos en línea reemplazarán a los ataques contra terminales PoS.**

El próximo año, en lo que respecta a las amenazas a usuarios y tiendas comunes, el riesgo será mucho mayor para quienes usen tarjetas sin chip o no tengan autorización de dos factores para transacciones. Los ciberdelincuentes se han enfocado en algunos objetivos simples, más fáciles de monetizar. Sin embargo, esto no significa que no usen otras técnicas complejas. Por ejemplo, para evadir los sistemas antifraude, copian todos los parámetros de sistema de la computadora y el navegador. Por otro lado, este comportamiento ciberdelincuencial implicará una disminución de los ataques contra terminales PoS y su preferencia por los ataques contra plataformas de pago en línea.

- **Los sistemas de ciberseguridad de las instituciones financieras serán evadidos con dispositivos físicos conectados a la red interna**

Debido a la falta de seguridad física y de control sobre los dispositivos conectados en muchas redes, los ciberdelincuentes explotarán de forma activa las situaciones en las que se pueda instalar una computadora o un minitablero configurado específicamente para robar datos de la red y transferir la información con módems 4G/LTE.

Los ataques de este tipo darán a los grupos de ciberdelincuentes una oportunidad para acceder a distintos datos, como información sobre los clientes y la infraestructura de red de las instituciones financieras.

- **Ataques contra la banca móvil para usuarios empresariales**

Las aplicaciones móviles para empresas son cada vez más populares, lo que podría llevar a los primeros ataques contra sus usuarios. Existen herramientas más que suficientes para esto y las posibles pérdidas que sufrirían las empresas son mucho mayores que las pérdidas que sufren las víctimas individuales. Los vectores de ataque más probables son los ataques en el nivel de API de la Web y a través de la cadena de suministro.

- **Campañas de ingeniería social avanzada dirigidas a operadores, secretarios y otros empleados internos a cargo del cableado: ocasionarán filtraciones de datos**

La ingeniería social es popular en algunas regiones, como América Latina. Los ciberdelincuentes apuntan a personas específicas en empresas e instituciones financieras para que les transfieran grandes sumas de dinero. Debido a la gran cantidad de fugas de datos en años anteriores, este tipo de ataque es cada vez más efectivo. Los delincuentes pueden usar la información interna robada sobre la organización atacada para que sus mensajes parezcan absolutamente legítimos. La idea principal sigue siendo la misma: hacer que los objetivos crean que la solicitud financiera proviene de socios o directores empresariales. Estas técnicas no usan malware, pero ponen de relieve el modo en que la ingeniería social obtiene resultados y aumentarán su poder en 2019. Esto incluye ataques como el fraude "SIM Swap".