DarkVishnya, la nueva oleada de robos cibernéticos en Europa

Durante 2017 y 2018, investigadores de Kaspersky Lab participaron en una respuesta a incidentes de varios **robos cibernéticos** a organizaciones financieras en Europa del Este. Los analistas descubrieron que, en cada caso, el acceso a la red corporativa se realizó a través de un dispositivo desconocido, controlado por ciberdelincuentes, escondido en los edificios de las empresas y conectado a la red.

Hasta el momento, se han **atacado al menos a ocho bancos** de la región, con pérdidas estimadas en decenas de millones de euros.

"Durante el último año y medio, observamos en los bancos un tipo de ataque completamente nuevo, bastante sofisticado y complejo en términos de detección. El punto de entrada a la red del banco permaneció desconocido durante mucho tiempo, ya que podía situarse en cualquier oficina y en cualquier región. Estos dispositivos desconocidos, introducidos secretamente por terceros y ocultos, no se podían descubrir remotamente. Además, **el grupo especificado por detrás de este APT utilizó aplicaciones legítimas, lo que complicó aún más la respuesta al incidente**", dijo Sergey Golovanov, analista de seguridad de Kaspersky Lab.

Esta técnica no es novedad en América Latina, ya que desde 2014 la región se enfrenta a **Prilex, amenaza que comenzó atacando cajeros automáticos y luego evolucionó para robar tarjetas de crédito** protegidas por contraseña y chip vía sistemas de punto de venta (POV).

Según Fabio Assolini, analista senior de seguridad de Kaspersky Lab en América Latina, el malware brasileño utiliza un blackbox y un módem 3G para realizar los ataques a los cajeros automáticos.

"Los **ataques de blackbox se han vuelto cada vez más comunes contra grandes y medianas empresas**, explotando fallas en la seguridad física y puntos de redes expuestos que permiten realizar un ataque que compromete el entorno digital de la empresa al puro estilo de *Mr. Robot*. Su detección es difícil, mas no imposible. Las empresas tienen que invertir en inventario de hardware y control de dispositivos conectados a la red, a fin de disminuir el 'shadow IT', además de adoptar otras buenas prácticas de seguridad", explica el analista.

Operación

Los ciberdelincuentes utilizaron tres tipos de dispositivos: una laptop, una Raspberry Pi (computadora de una sola placa del tamaño de una tarjeta de crédito) o una Bash Bunny (herramienta especialmente diseñada para automatizar y realizar ataques por USB), equipados con GPRS, módem 3G o LTE, que les permitió acceder de forma remota a la red corporativa de la entidad bancaria.

Una vez establecida la conexión, los cibercriminales intentaron tener acceso a los servidores web para hacerse con los datos que necesitaban para ejecutar RDP (protocolo de escritorio remoto) en

una computadora y luego hacerse de dinero o datos.

Este **método de ataque *fileless* incluyó el uso de kits de herramientas de ejecución remota como Impacket, winexesvc.exe o psexec.exe.** En la etapa final, los hackers utilizaron software de control remoto para mantener el acceso al equipo infectado.

Para protegerse contra este tipo de robo digital poco frecuente, se aconseja a las instituciones financieras que presten especial atención a la supervisión de dispositivos conectados y al acceso a la red corporativa. Otra recomendación es aumentar el control de acceso a la red corporativa para facilitar la detección de actividades sospechosas, e identificar y eliminar completamente las fallas de seguridad, incluidos aquellos que implican configuraciones de red inadecuadas.