**Cibercrimen amenaza al retail mediante el Internet de las Cosas y los *Infostealers:* Netskope Threat Labs**

Bogotá, Colombia. 03 de abril abril de 2024 - Netskope Threat Labs publicó su informe de investigación más reciente, centrado en las amenazas en la nube para el retail, el cual revela que las botnets de Internet de las Cosas (IoT), los troyanos de acceso remoto y los *infostealers* fueron las principales formas mediante las que se desplegó el malware en contra del sector minorista en el último año.

* Los principales hallazgos del reporte son:

**Los *infostealers,* el malware que acecha al retail:** Se trata de una familia de malware muy común para el sector minorista, mediante la cual los atacantes intentan robar datos valiosos como detalles de pagos de organizaciones y clientes. Los *infostealers* también alimentan el ecosistema de ciberdelincuencia más amplio, con atacantes vendiendo credenciales robadas y detalles financieros personales.

**Botnets y troyanos apuntando a dispositivos de red**: La familia de botnets Mirai apuntan con mayor frecuencia a dispositivos de red expuestos que ejecutan Linux, como *routers*, cámaras y otros dispositivos IoT en el entorno minorista. Los dispositivos IoT a menudo se pasan por alto como un riesgo de seguridad, pero pueden ser efectivos proporcionando información visual o sensorial que puede asistir en el cibercrimen, o incluso ser abusados para lanzar ataques DDoS contra otros objetivos.

De manera similar, los troyanos de acceso remoto (RAT) fueron populares ya que permiten el acceso a navegadores y cámaras de videovigilancia, enviando información a atacantes o recibiendo comandos. Desde la filtración del código fuente del malware Mirai, el número de variantes de este malware ha aumentado considerablemente y representa un riesgo para el sector minorista con múltiples puntos finales vulnerables.

**Suite de Microsoft, cada vez más un objetivo**: En el informe del año pasado, las aplicaciones de Google eran mucho más populares en el sector minorista que en otras industrias, pero durante el último año, los investigadores han visto un resurgimiento de la popularidad de Microsoft. Esto es particularmente evidente para el almacenamiento, con la brecha entre OneDrive y Google Drive ampliándose durante el último año, con el porcentaje promedio de usuarios pasando de 43% a 51% para OneDrive y cayendo de 34% a 23% para Google Drive.

Vemos tendencias similares con Outlook (21%) suplantando a Gmail (13%) como la aplicación de correo electrónico más popular. Microsoft OneDrive sigue siendo la aplicación en la nube más popular para la entrega de malware en todos los sectores, incluido el minorista. Los atacantes gravitan hacia tácticas que capitalizan la confianza y familiaridad de los usuarios con OneDrive, aumentando la probabilidad de que hagan clic en los enlaces y descarguen el malware. En el sector minorista, los ataques a través de Outlook son más exitosos que en otros sectores: el minorista ve el doble de descargas de malware a través de Outlook (10%) que el promedio de otras industrias (5%).

**Popularidad de WhatsApp en el sector minorista:** La aplicación fue tres veces más popular en el sector minorista (14%) que en otras industrias (5.8%) tanto para uso promedio como para descargas. Sin embargo, WhatsApp no fue incluido entre las aplicaciones actuales más populares para descargas de malware.

Esto puede cambiar a medida que los actores de amenazas comiencen a ver su popularidad justificando el caso económico para dirigir más ataques a través de la aplicación. Aplicaciones de redes sociales como X (12%), Facebook (10%) e Instagram (1.5% para subidas) fueron todas más populares en el sector minorista que el promedio de otras industrias.

Para profundizar más sobre los hallazgos del reporte, el jefe de Inteligencia Cibernética en Netskope, Paolo Passeri, comentó:

*"Es sorprendente que el sector minorista todavía se encuentre específicamente amenazado con botnets cómo Mirai mientras los atacantes buscan comprometer dispositivos IoT vulnerables o mal configurados en ubicaciones minoristas y abusar de ellos para amplificar dramáticamente el efecto de un ataque de denegación de servicio distribuido (DDoS)”.*

*“Mirai no es una amenaza particularmente reciente, y el hecho de que los atacantes continúen usándolo desde su descubrimiento en 2016 para apuntar a dispositivos IoT muestra que demasiadas organizaciones continúan pasando por alto el peligro que implican estos dispositivos conectados a internet. Esto plantea un riesgo significativo no solo para los objetivos de los ataques lanzados desde el botnet de IoT, sino también para la organización cuyos dispositivos IoT son esclavizados en el botnet, ya que su explotación puede llevar fácilmente a interrupciones que impacten el funcionamiento del negocio”.*

*"Esta vulnerabilidad, junto con el uso de infostealers y malware de acceso remoto para extraer credenciales y datos financieros de clientes, hace que el sector minorista sea un objetivo potencialmente lucrativo”.*

*"Me interesó particularmente ver que infostealers como Qakbot están entre las principales amenazas para los minoristas, a pesar de que esta operación fue derribada por el FBI a finales de agosto de 2023. Su infraestructura ha sido rápidamente reequipada por los atacantes para distribuir cargas útiles de malware adicionales, proporcionando oportunidades adicionales para los atacantes. El hecho de que continúen siendo entre los principales métodos que los atacantes usan para apuntar a organizaciones minoristas muestra que los líderes de seguridad todavía tienen mucho que hacer para fortalecer su infraestructura y puntos finales. Afortunadamente, seguir las mejores prácticas fundamentales de higiene cibernética como inspeccionar el tráfico web y en la nube, además de bloquear el tráfico malicioso y aislar puntos finales o dominios comprometidos reducirá el riesgo de ser víctima de estos atacantes.*"

Netskope Threat Labs recomienda a las empresas en el sector minorista revisar su postura de seguridad en la nube y considerar la adopción de una solución Secure Access Service Edge (SASE) para garantizar una visibilidad completa y control de su uso de aplicaciones en la nube y prevenir la exfiltración de datos.

Para leer el reporte completo visita [este enlace.](https://www.netskope.com/resources/threat-labs-reports/threat-labs-report-retail-2024)

**Acerca de Netskope**
Netskope es la compañía líder mundial en SASE que ayuda a las organizaciones a aplicar los principios de confianza cero (zero trust) y las innovaciones de IA/ML para proteger los datos y defenderse de las ciberamenazas. Rápida y fácil de usar, la plataforma Netskope proporciona acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos en cualquier lugar. Netskope ayuda a los clientes a reducir riesgos, acelerar el rendimiento y obtener una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas. Miles de clientes confían en Netskope y en su potente red NewEdge para hacer frente a las amenazas cambiantes, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red, y los nuevos requisitos normativos. Para saber cómo Netskope ayuda a los clientes a estar preparados en su viaje SASE, visite <https://www.netskope.com/es/>