**Netskope Threat Labs: Los Infostealers apuntan a los datos del sector de la salud**

**6 de marzo de 2024** - [Netskope](https://www.netskope.com/) Threat Labs publicó su último [informe de investigación](https://www.netskope.com/resources/threat-labs-reports/netskope-threat-labs-report-healthcare-2024), revelando que los infostealers fueron la principal familia de malware y ransomware utilizada para atacar al sector de la salud. Durante 2023, el sector de la salud estuvo entre los [más afectados](https://www.hackmageddon.com/2023/03/02/the-biggest-data-breaches-of-2023/) por mega brechas, un tipo de ataque en el que se robaron más de un millón de registros.

El informe también examinó el continuo aumento en la adopción de aplicaciones en la nube en el sector de la salud, así como las tendencias de malware en el sector.

Principales hallazgos:

* **Objetivo clave de ataques de infostealers:** Los infostealers son una familia prominente de malware para el sector de la salud, ya que los atacantes intentan robar datos valiosos de organizaciones y pacientes para luego chantajear o exigir un rescate por esos datos.
  + Ransomware Clopp especialmente activo: El grupo de ransomware Clopp fue particularmente activo atacando a organizaciones de salud y seguros de salud, explotando la [vulnerabilidad CVE-2023-34362 en MOVEit.](https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html)
  + La atención médica estuvo entre los [sectores más afectados](https://www.hackmageddon.com/2023/03/02/the-biggest-data-breaches-of-2023/) durante el 2023 por mega brechas, un tipo de ataque en el que se robaron más de un millón de registros.
* **Descargas de malware aumentaron en 2023 pero se estabilizaron en H2:** El malware entregado a través de la nube terminó el año en aproximadamente el 40% de las descargas de malware en el sector de la salud, después de alcanzar un pico del 50% en junio que luego disminuyó en la segunda mitad del año. La atención médica mostró una ligera tendencia por debajo de otras industrias, pero el malware entregado a través de la nube en el sector creció considerablemente de un año a otro, aumentando desde tan solo el 30% hace un año.
  + Es destacable que el sector de la salud parecía tener el porcentaje más bajo de malware proveniente de la nube en los últimos 12 meses, clasificándose en sexto lugar con aproximadamente el 40% de las descargas totales de malware, detrás de las telecomunicaciones, servicios financieros, manufactura, comercio minorista, tecnología, gobierno estatal y local, y educación.
  + Las aplicaciones en la nube son cada vez más un objetivo para el malware, ya que brindan a los atacantes la capacidad de eludir los controles de seguridad habituales que dependen de herramientas como listas de bloqueo de dominios y monitoreo del tráfico web, y dichos ataques afectan a empresas que no aplican principios de confianza cero para inspeccionar de manera rutinaria el tráfico en la nube.
* **Resistiendo la tendencia de malware en Microsoft OneDrive:** Aunque Microsoft OneDrive siguió siendo la aplicación más popular en el sector de la salud, su uso fue significativamente menor que en otros sectores, lo que resultó en menos descargas de malware a través de OneDrive en comparación con otras industrias.
  + La prevalencia general de los ataques de malware originados en OneDrive refleja la fusión de tácticas adversarias (abusar de OneDrive para distribuir malware) y el comportamiento de la víctima (su probabilidad de hacer clic en los enlaces y descargar el malware), junto con la amplia popularidad de OneDrive.
* **Popularidad de Slack en el sector de la salud:** Slack fue la segunda aplicación más utilizada para cargar archivos (después de OneDrive) y la quinta para descargar, significativamente más alta que en otros sectores. Sin embargo, esta tendencia de uso no se correlacionó con la cantidad de descargas de malware desde la aplicación.Ni siquiera estaba entre las 10 fuentes principales.
  + Dado que Slack es una aplicación empresarial sólida, los atacantes necesitan emplear tácticas y contenido diferentes para dirigirse a usuarios que deben aceptar o compartir invitaciones a canales externos. Este proceso es más complejo en comparación con otras aplicaciones de mensajería para consumidores, como WhatsApp, que podrían utilizarse en un dispositivo corporativo. En cambio, los atacantes usarían Slack como un servidor de comando y control, ya que su API proporciona un mecanismo flexible para cargar (o exfiltrar) datos.

**Declaraciones de Paolo Passeri, Principal de Inteligencia Cibernética en Netskope:**

"Los infostealers están entre las principales amenazas para el sector de la salud, y esto se refleja en el hecho de que durante el 2023 muchas organizaciones de salud fueron blanco de mega brechas, y entre los principales objetivos de la masiva campaña Clop que explotó la vulnerabilidad CVE-2023-34362."

"Por supuesto, este modus operandi no sorprende debido a los tipos de datos personales gestionados por estas organizaciones, pero es particularmente efectivo porque los atacantes no necesariamente tienen que cifrar los datos en un ataque al estilo ransomware. En cambio, exfiltran la información robada y la utilizan para chantajear a la víctima (o a sus clientes/pacientes)."

"El malware y los infostealers no deberían ser la única preocupación para el sector de la salud; también deberían considerar la vulnerabilidad de su cadena de suministro y aplicar la misma estrategia de confianza cero que aplicarían en su propia organización a terceros en la cadena de suministro."

El informe se basa en datos de uso anonimizados recopilados sobre un subconjunto del sector de la salud de los más de 2,500 clientes de Netskope, todos los cuales otorgan autorización previa para analizar sus datos de esta manera.

Para acceder al informe completo, visite aquí o contacte a:

Renán Rodríguez

PR Executive another

Renan.rodriguez@another.co

Acerca de Netskope:

Netskope, líder global en SASE, ayuda a las organizaciones a aplicar los principios de confianza cero e innovaciones de IA/ML para proteger datos y defenderse contra amenazas cibernéticas. La plataforma Netskope, rápida y fácil de usar, proporciona acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos en cualquier lugar. Netskope ayuda a reducir el riesgo, acelerar el rendimiento y obtener una visibilidad sin igual en cualquier actividad de aplicaciones en la nube, web y privadas. Miles de clientes confían en Netskope y su potente red NewEdge para abordar amenazas en evolución, nuevos riesgos, cambios tecnológicos, organizativos y de red, y nuevos requisitos regulatorios. Descubra cómo Netskope ayuda a los clientes a estar listos para cualquier cosa en su viaje SASE, visite netskope.com.