Cibercrimen, un ‘huésped’ duradero: incrementa 36% su permanencia en sistemas infectados

- *El aumento se debe a la explotación de las vulnerabilidades de ProxyLogon y ProxyShell, además de los agentes de acceso inicial.*
- *A pesar de una caída en el uso del protocolo de escritorio remoto para el acceso externo, los atacantes aumentaron el uso de la herramienta para el movimiento lateral interno.*

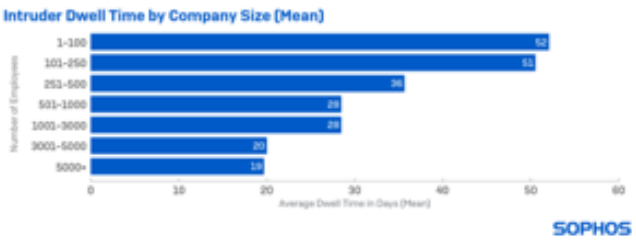
Sophos, líder mundial en ciberseguridad de última generación, publicó el informe “Libro de Estrategias del Adversario Activo 2022" (Active Adversary Playbook), que detalla los comportamientos de los atacantes que el equipo de respuesta rápida de Sophos detectó en 2021.

Los hallazgos muestran un aumento del 36% en el tiempo de permanencia en los sistemas vulnerados, con un tiempo promedio de 15 días; cifra superior a los 11 días promedio registrados durante 2020.

El informe también revela el impacto de las vulnerabilidades de ProxyShell en Microsoft Exchange, que Sophos cree que algunos agentes de acceso inicial (IAB por sus siglas en inglés) aprovecharon para vulnerar las redes y luego vender ese acceso a otros atacantes .

“El mundo del cibercrimen se ha vuelto increíblemente diverso y especializado. Los IAB han desarrollado estrategias para vulnerar a un objetivo realizando un reconocimiento exploratorio o instalando una puerta trasera, y luego vendiendo la llave de acceso a grupos de ransomware para gestionar sus propios ataques”, dijo John Shier, asesor senior de seguridad de Sophos.

“En este panorama de amenazas cibernéticas cada vez más dinámico y basado en especialidades, puede ser difícil para las organizaciones mantenerse al día con las herramientas y enfoques en constante cambio que utilizan los atacantes. Es vital que los defensores entiendan qué buscar en cada etapa de la cadena de ataque, para que puedan detectar y neutralizar los ataques lo más rápido posible”, añade.



La investigación de Sophos también muestra que el tiempo de permanencia de los intrusos fue mayor en los entornos de las organizaciones más pequeñas. Los atacantes permanecieron

durante aproximadamente 51 días en organizaciones con hasta 250 empleados, mientras que normalmente pasaron 20 días en organizaciones con 3000 a 5000 empleados.

"Los atacantes consideran que las organizaciones más grandes son más valiosas, por lo que están más motivados para entrar, obtener lo que quieren y salir. Las organizaciones más pequeñas tienen menos 'valor' percibido, por lo que los atacantes pueden darse el lujo de estar al acecho en la red en segundo plano durante un período más largo. También es posible que estos atacantes tuvieran menos experiencia y necesitarán más tiempo para averiguar qué hacer una vez que estuvieran dentro de la red", señala Shier.

"Por último, debemos destacar que las organizaciones más pequeñas suelen tener menos visibilidad a lo largo de la cadena de ataque para detectar y expulsar a los atacantes, lo que prolonga su presencia. Con las oportunidades de las vulnerabilidades ProxyLogon y ProxyShell sin parches, estamos viendo más evidencia de múltiples atacantes en un solo objetivo. Cuando esto sucede, los atacantes procuran moverse más rápido para vencer a otros entes maliciosos que les pudieran representar una competencia", indica.

Los hallazgos clave adicionales en estudio son:

- **El tiempo medio de permanencia es mayor en aquellos ataques 'sigilosos' que no son propiamente un ataque de ransomware a gran escala.** Mientras que el tiempo promedio en organizaciones vulneradas por el ransomware fue de 11 días; en aquellas vulneradas sin verse afectadas por un ataque de grandes dimensiones (23% de todos los incidentes), fue de 34 días.

- **El Protocolo de escritorio remoto (RDP) ya no se utiliza para el acceso a los sistemas, sino para el movimiento lateral interno.** En 2020, los atacantes usaron RDP para actividades externas en el 32% de los casos analizados, pero esto disminuyó al 13% en 2021. Si bien este cambio es positivo, contrasta con el porcentaje de uso lateral interno, dentro de los sistemas afectados, que fue de 82% frente al 69% del año previo.

- **Las combinaciones de herramientas en los ataques son cada vez más comunes, por lo que son una buena señal de advertencia.** Por ejemplo, las investigaciones de incidentes encontraron que en 2021 PowerShell y los scripts maliciosos que no son de PowerShell se utilizaron en el 64 % de los casos; PowerShell y Cobalt Strike combinados en el 56 % de los casos; y PowerShell y PsExec se encontraron en el 51%. La detección de tales correlaciones puede servir como advertencia temprana de un ataque inminente.

- **Filtración de datos, la constante.** El cincuenta por ciento de los incidentes de ransomware involucraron la filtración de datos confirmada y la brecha media entre el robo de datos y la implementación del ransomware fue de 4.28 días. El 73% de los

incidentes a los que respondió Sophos en 2021 involucraron ransomware. De estos incidentes de ransomware, el 50% también involucró la exfiltración de datos.

- **Conti fue el grupo de ransomware más prolífico de 2021, representando el 18 % de los incidentes en general**. El ransomware REvil representó uno de cada 10 incidentes, mientras que otras familias de ransomware predominantes incluyeron DarkSide, el RaaS detrás del notorio ataque a Colonial Pipeline en Estados Unidos. Se identificaron 41 adversarios de ransomware diferentes en los 144 incidentes incluidos en el análisis. De estos, alrededor de 28 eran grupos nuevos y vistos por primera vez durante 2021. Dieciocho grupos de ransomware vistos en incidentes en 2020 desaparecieron de la lista en 2021

"*Las señales de alerta que los defensores deben tener en cuenta incluyen la detección de una herramienta legítima, una combinación de herramientas o una actividad en un lugar inesperado o en un momento poco común",* dijo Shier. "*Vale la pena señalar que también puede haber momentos de poca o ninguna actividad, pero eso no significa que no se haya violado una organización. Por ejemplo, es probable que haya muchas más infracciones de ProxyLogon o ProxyShell que actualmente se desconocen, en las que se han implantado puertas traseras en objetivos para el acceso persistente y ahora permanecen en silencio hasta que se usa o vende ese acceso",* añade.

"Los defensores deben estar alerta ante cualquier señal sospechosa e investigar de inmediato. Necesitan parchear errores críticos, especialmente aquellos en software ampliamente utilizado y, como prioridad, fortalecer la seguridad de los servicios de acceso remoto. Hasta que se

cierren los puntos de entrada expuestos y se elimine por completo todo lo que los atacantes han hecho para establecer y retener el acceso, casi cualquiera puede entrar tras ellos, y probablemente lo hará", sentenció el especialista.

El "Libro de Estrategias del Adversario Activo 2022" (Active Adversary Playbook) se basa en 144 incidentes detectados en 2021, dirigidos a organizaciones de todos los tamaños, en una amplia gama de sectores industriales y ubicadas en Estados Unidos, Canadá, el Reino Unido, Alemania, Italia, España, Francia, Suiza, Bélgica, Países Bajos, Austria, Emiratos Árabes Unidos, Arabia Saudita, Filipinas, Bahamas, Angola y Japón. Los sectores más representados son Manufactura (17%); Retail (14%); Salud (13%); TI (9%); Construcción (8%) y Educación (6%).

El objetivo de este informe es ayudar a los equipos de seguridad a comprender cómo se comportan y qué hacen los adversarios durante los ataques, así como recomendaciones para detectar y defenderse de actividades maliciosas en la red. Para obtener más información sobre los comportamientos, las herramientas y las técnicas de los atacantes, consulte el "Libro de Estrategias del Adversario Activo 2022" (Active Adversary Playbook), en Sophos News.

Recursos adicionales

- Read the latest security news and views on Sophos' award-winning news website Naked Security and on Sophos News.
- Lee sobre el panorama de amenazas en evolución y cómo las organizaciones experimentan los ataques en el Estado del ransomware 2022 y el Informe de amenazas de Sophos 2022.
- Conoce la investigación de Sophos sobre una amplia gama de grupos de ransomware individuales en el Sophos Ransomware Threat Intelligence Center.
- Obtén más información sobre cómo Sophos Rapid Response Service contiene, neutraliza e investiga los ataques las 24 horas del día, los 7 días de la semana.
- Conozca los cuatro consejos principales para responder a un incidente de seguridad de Sophos Rapid Response y Managed Threat Response Team.
- Lee las últimas noticias y opiniones sobre seguridad en el galardonado sitio web de noticias de Sophos Naked Security y en Sophos News.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de

ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/