# El enemigo ‘duerme’ en casa: hackers se ocultan hasta 5 meses en un servidor para atacar

- *Sophos encontró en una investigación que los atacantes se alojan de manera oculta para buscar herramientas en línea, muchas de ellas benignas, que luego les ayuden a implementar otras etapas de la amenaza.*

**CIUDAD DE MÉXICO. 12 de abril de 2022.-** Sophos, líder mundial en ciberseguridad de última generación, publicó los hallazgos de una investigación que detalla cómo los atacantes violaron las puertas de acceso y pasaron hasta cinco meses dentro de un servidor gubernamental de Estados Unidos, previo a la implementación de un ataque de ransomware.

La investigación detalla la forma en la que los atacantes también instalaron un criptominero antes de robar datos e implementar el ransomware Lockbit. El artículo sugiere que varios atacantes de diversos niveles de experiencia se infiltraron en dicho servidor vulnerable, antes de que éste fuera contenido e investigado por el equipo de respuesta a incidentes de Sophos.

“*Este fue un ataque muy desordenado. Trabajando junto con el objetivo, los investigadores de Sophos pudieron construir una imagen que comenzó con lo que parecen ser atacantes novatos que irrumpieron en el servidor, hurgaron en la red y usaron el servidor comprometido para buscar en Google una combinación de versiones pirateadas y gratuitas de piratas informáticos y legítimos*”, dijo Andrew Brandt, investigador principal de seguridad de Sophos.

“*Alrededor de cuatro meses después, la naturaleza de la actividad de ataque cambió, en algunos casos tan drásticamente que sugiere que algunos atacantes con habilidades muy diferentes se habían unido. Estos atacantes intentaron desinstalar el software de seguridad. Eventualmente robaron datos y cifraron archivos en varias máquinas al implementar el ransomware Lockbit*”, añade.

- **¿Cómo se inmiscuyen?**

Los investigadores de Sophos descubrieron que el punto de acceso inicial para este ataque, que data de septiembre del 2021, fue un puerto abierto de protocolo de escritorio remoto (RDP). Luego usaron un navegador del servidor vulnerado para buscar en línea las herramientas que usarían, e intentaron instalarlas.

En algunos casos, la búsqueda de herramientas llevó a los atacantes a sitios de descarga dudosos que enviaban un adware al servidor vulnerado, en lugar de las herramientas que estaban buscando.

La investigación muestra que los comportamientos de los atacantes cambiaron significativamente a mediados de enero, con signos de actividad más hábil y enfocada. Estos atacantes intentaron eliminar el criptominero malicioso y desinstalar el software de seguridad,

aprovechando el hecho de que el objetivo había dejado inadvertidamente una función de protección desactivada después de completar el mantenimiento.

Luego, los atacantes recopilaron y extrajeron datos, para así implementar el ransomware Lockbit. El ataque de ransomware tuvo un éxito limitado y los entes maliciosos no pudieron cifrar los datos en algunas máquinas.

- **Las 'red flags': ¿cómo detectar actividad inusual?**

Las herramientas que los atacantes intentaron instalar con fines maliciosos incluyeron Advanced Port Scanner, FileZilla, LaZagne, mimikatz, NLBrute, Process Hacker, PuTTY, Remote Desktop Passview, RDP Brute Forcer, SniffPass y WinSCP. Los atacantes también instalaron herramientas comerciales de acceso remoto, incluidas ScreenConnect y AnyDesk.

*"Si un miembro del equipo de TI no las ha descargado para un propósito específico, la presencia de tales herramientas en las máquinas de tu red es una señal de alerta de un ataque en curso"*, dijo Brandt. "*La actividad de red inesperada o inusual, como una máquina que escanea la red, es otro indicador de este tipo. Las fallas repetidas de inicio de sesión de RDP en una máquina a la que solo se puede acceder dentro de la red son una señal de que alguien podría estar usando esa herramienta para moverse lateralmente".*

"*Un enfoque de defensa en profundidad sólido, proactivo, las 24 horas del día, los 7 días de la semana ayudará a evitar que un ataque de este tipo se arraigue y se desarrolle. El primer paso es tratar de evitar que los atacantes tengan acceso a una red implementando la autenticación de múltiples factores y configurando reglas de firewall para bloquear el acceso remoto a los puertos RDP en ausencia de una conexión VPN*", concluye el especialista.

###

**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/