# Esto es lo que debes saber para combatir y prevenir un ataque de ransomware como el de Kaseya

**CIUDAD DE MÉXICO. 6 de julio de 2021.-** El pasado 2 de julio, un grupo de cibercriminales afiliados al ransomware REvil lanzaron un ataque de criptoextorsión en contra del servicio de administración remota de Kaseya. Los atacantes lanzaron un paquete de supuesta actualización del software que resultó ser apócrifo, dirigido a clientes, proveedores de servicios administrados y usuarios empresariales de dicho software.

Como ese caso, en los últimos meses se han presentado un sinfín de ataques bajo **REvil, un ransomware como servicio (RaaS)** operado por un grupo de cibercriminales "suscritos" que pagan por su utilización para la propagación de amenazas.

De acuerdo con el equipo de Sophos Rapid Response, y luego de varias investigaciones, esto es lo que debes saber para enfrentar y prevenir la latente posibilidad de ser víctima de un ataque de ransomware REvil:

- **Contención y neutralización**

Lo primero que debes saber es si el ataque aún está en curso o no, para luego determinar qué dispositivos están afectados y saber si la mejor idea es aislarlos o simplemente desconectar todas las redes. Además, se debe evaluar el daño en cuanto a qué sistemas operativos se vieron afectados, la calidad de la información comprometida, las copias de seguridad existentes y las máquinas vulneradas.

- **Determina desde cuándo ingresaron a tu red**

Lo más probable es que los atacantes estén en la red desde hace algunos días o incluso semanas. REvil ransomware es operado por adversarios humanos que han alquilado el malware a los desarrolladores, agregando sus propias herramientas y objetivos, lo cual toma tiempo para preparar ataques que causen una afectación significativa, lo que además les permite cobrar los rescates multimillonarios.

- **Encuentra tu vulnerabilidad**

Los posibles métodos de acceso inicial para REvil ransomware no se limitan a exploits vulnerables, ya que pueden ingresar mediante tácticas como el phishing, ataques de fuerza bruta contra servicios como VPNs, protocolos de escritorio remoto expuesto (RDP) y herramientas de administración remota Virtual Network Computing (VNC), e incluso algunos sistemas de administración basados en la nube.

- **¿A qué información tienen acceso?**

Debes saber que los atacantes tendrán acceso seguro a las cuentas de administrador de dominio, así como a otras cuentas de usuario. Los atacantes suelen comprometer varias cuentas durante un ataque. Su objetivo principal es obtener acceso a cuentas de administrador de dominio que se pueden utilizar para iniciar el ransomware.

- **Habrán escaneado tu red**

Ellos saben cuántos servidores y puntos finales tienes y dónde guardas tus copias de seguridad, datos y aplicaciones críticas para el negocio. Una de las primeras cosas que harán los atacantes cuando accedan a una red es identificar qué acceso tienen en la máquina local. El siguiente paso es averiguar qué máquinas remotas existen y si pueden acceder a ellas. Los atacantes utilizan escáneres de red legítimos como "Advanced Port Scanner" y "Angry IP Scanner" debido a su eficacia y al hecho de que es poco probable que se bloqueen.

- **Detecta y bloquea puertas traseras**

Es probable que los atacantes hayan instalado puertas traseras que les permitan entrar y salir de tu red. Habrán configurado carpetas y directorios para recopilar y almacenar información robada, además de canales para mover información fuera de la red. Las puertas traseras vienen en una variedad de formas. Algunos simplemente se comunican con la dirección IP de los atacantes, lo que les permite enviar y recibir comandos a la máquina.

Cabe destacar que muchas puertas traseras se clasifican como aplicaciones legítimas. Por ejemplo, los atacantes pueden utilizar herramientas de administración remota como RDP para mantener el acceso. Incluso si el RDP está deshabilitado de forma predeterminada, es muy fácil para un atacante con acceso de administrador a la máquina volver a habilitarlo.

- **¿Por qué crear copias de seguridad offline?**

Primero, los atacantes intentarán cifrar, eliminar, restablecer o desinstalar tus copias de seguridad. A menos que esas copias se almacenen sin conexión, están al alcance de los atacantes. Una "copia de seguridad" que está en línea y disponible todo el tiempo es solo una segunda copia de los archivos que serán encriptados.

- **El lanzamiento del ransomware no es el final**

Usando los diversos mecanismos de acceso que configuraron durante la etapa de preparación, los atacantes a menudo continuarán monitoreando la situación mediante métodos como un correo electrónico, para conocer la respuesta de la empresa. El atacante también puede esperar hasta que tu compañía se recupere para luego lanzar un segundo ataque y enfatizar realmente que puede seguir haciéndolo hasta recibir un pago.

Lidiar con un ciberataque es una experiencia estresante. Es por eso que muchas empresas creen que eliminar la amenaza y dar la vuelta a la hoja significa el final del problema, pero la verdad es que se trata de una labor continua, que no concluye y que, por el contrario, siempre evoluciona. Es importante que cada compañía se tome el tiempo para identificar cómo entraron los atacantes, aprender de los errores y realizar mejoras en su seguridad. Si no lo hacen, corren el riesgo de que otros adversarios, o incluso el mismo, ataquen de nuevo en el futuro.

**Sobre Sophos**

Sophos es la empresa líder mundial en ciberseguridad de última generación, que 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 para la detección 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, redes y endpoints contra ransomware, malware, exploits, phishing y una amplia gama de ciberataques. Sophos proporciona una plataforma única de gestión integral basada en la nube llamada Sophos Central, el eje 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 distribuidores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Para más información, ingresa a www.sophos.com.

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