Así opera REvil, el ransomware bajo servicio más frecuente en la actualidad.

- ***El 37% de las compañías a nivel mundial se vieron afectadas por ransomware en el último año, de acuerdo con Sophos.***

CIUDAD DE MÉXICO. 15 de junio de 2021.- El ransomware es, hoy en día, la amenaza más grande en cuestión de crimen cibernético para las compañías. De acuerdo con Sophos, líder mundial en ciberseguridad de última generación, el 37% de las empresas a nivel mundial se han visto afectadas por ransomware en el último año.

Los ejemplos son variados: en las últimas semanas han surgido casos como el hackeo a la compañía Electronic Arts, una de las principales desarrolladoras de videojuegos del mundo. La firma indicó que cibercriminales habrían obtenido alrededor de 780 gigantes de datos de la empresa, tales como el código fuente del motor que alimenta a títulos como FIFA, Madden y Battlefield, entre los más populares.

La amenaza es tal que el Departamento de Justicia de Estados Unidos indicó recientemente que las investigaciones sobre ransomware se llevarían a cabo con protocolos similares a los que se utilizan en casos sobre terrorismo, elevando el nivel de prioridad para ese tipo de acontecimientos.

Ante ese panorama, los ciberdelincuentes están migrando su método de ataque a la utilización de un **ransomware 'bajo servicio' (*ransomware as a service* RaaS)**, que les permite obtener la capacidad de concentrarse en el robo y la implementación del ataque y no en el desarrollo del virus.

Uno de los **RaaS** más frecuentes es **Sodinokibi o REvil:** un ransomware muy convencional cuyas rutinas, configuración y comportamiento lo vuelven uno de los más utilizados y efectivos para los criminales. Sophos detectó que este ransomware realiza, antes de ingresar a los sistemas vulnerados, una serie de intentos de inicio de sesión en plataformas de acceso remoto o VPNs. Generalmente buscan acceder mediante cuentas legítimas que no requieren del uso de autenticación multifactor.

Una investigación reciente reveló, que una empresa vulnerada recibió alrededor de 35,000 intentos de sesión fallidos en un periodo de 5 minutos en un protocolo de acceso remoto (RDP), originados en 349 direcciones IP.

REvil se presenta como un archivo ejecutable y encriptado que, cuando se ejecuta por primera vez, enumera una lista de procesos y elimina los archivos temporales y copias de seguridad instalados en la máquina. Luego intenta deshabilitar los servicios de ciberseguridad, como las herramientas de Sophos, aunque se ha detectado que dichos intentos no concluyen con éxito.

Una vez incrustado, REvil aparece como un archivo de imagen en formato .bmp codificado, que el ransomware posteriormente establece como la imagen de escritorio en la computadora afectada. La imagen dice: todos sus archivos están encriptados. Posteriormente, indica al usuario el nombre de una 'Nota de Rescate' y la carpeta en la que ésta se ubica. Cuando el usuario va a la nota, encuentra las instrucciones y el monto a pagar por el rescate de la información.

Otra peculiaridad de este ataque es que utiliza la criptomoneda Monero como su método de pago. Esto se debe a que esta divisa digital tiene características de privacidad adicionales que el Bitcoin no tiene, por lo que se vuelve menos probable que las compañías consigan una recuperación del rescate pagado.

Sophos recomienda, ante este tipo de amenazas, procurar la creación constante de copias de seguridad fuera de línea así como fomentar una cultura de actualizaciones e instalación de parches frecuente dentro de la industria, además de medidas básicas como el uso de administradores de contraseñas, autenticación multifactor, y escaneo a la red de la empresa para vigilar la seguridad en puertos RDP, VPN, entre otros usados frecuentemente.

La ciberseguridad es una tarea sin final. Nunca se alcanza un nivel de protección con riesgo 'cero' y, por el contrario, las amenazas están en constante evolución y mejoran su nivel de sofisticación, por lo que las medidas de ciberseguridad deben cambiar y anticiparse a nuevos ataques, antes de que sea demasiado tarde.

###

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/