Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°261	Fecha: 01-11-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ransomware Akira activo en América Latina		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Akira se está convirtiendo rápidamente en una de las familias de ransomware de más rápido crecimiento gracias a su uso de tácticas de doble extorsión, un modelo de distribución de ransomware como servicio (RaaS) y opciones de pago únicas. Poco a poco, se ha hecho una lista de víctimas al infiltrarse en redes corporativas de todo el mundo, cifra archivos y luego exige rescates de millones de dólares.

El ransomware Akira surgió en marzo de 2023 y originalmente se dirigía a empresas con sede en EE.UU. y Canadá, pero actualmente está muy activo en América Latina.

Se propaga a través de correos electrónicos de phishing, malvertising y vulnerabilidades de software. Una vez que infecta el sistema, cifra los archivos con una clave única, haciéndolos inaccesibles.

Akira tiene diversas capacidades como la persistencia en el sistema infectado, la evasión de la defensa, la recolección de información del sistema y la comunicación con un servidor de control y comando.

El 12 de septiembre de 2023, el Centro de Coordinación de Ciberseguridad del Sector Salud (HC3) del Departamento de Salud y Servicios Humanos de EE.UU. publicó un boletín de seguridad alertando a la industria de la salud sobre los ataques de Akira.

2. DETALLES:

Según su código, es completamente diferente de la familia de ransomware Akira que estuvo activa en 2017, aunque ambos agregan archivos cifrados con la misma extensión .akira.

Según el análisis de TrendMicro, Akira parece estar basado en el ransomware Conti: comparte rutinas similares como la ofuscación de cadenas y el cifrado de archivos, y evita las mismas extensiones de archivos que Conti. Se cree que la principal motivación de los operadores de Akira para dirigirse a las organizaciones es de naturaleza financiera.

El grupo Akira RaaS realiza tácticas de doble extorsión y roba datos críticos de las víctimas antes de cifrar dispositivos y archivos. Curiosamente, según los informes, los operadores de Akira brindan a las víctimas la opción de pagar por el descifrado de archivos o la eliminación de datos; no obligan a las víctimas a pagar por ambos. Según otros informes, las demandas de rescate por Akira suelen oscilar entre 200.000 dólares y más de 4 millones de dólares.

En junio de 2023, apenas tres meses después de que se descubriera, Akira amplió su lista de sistemas objetivo para incluir máquinas Linux. El analista de malware rivitna compartió en X que los actores del ransomware Akira utilizaron un cifrador de Linux y apuntaron a máquinas virtuales VMware ESXi.

Mientras tanto, en agosto, el investigador SecurityAura informó que Akira estaba apuntando a cuentas VPN de Cisco que no tenían autenticación multifactor (MFA). Cisco publicó un aviso de seguridad el 6 de septiembre de 2023, indicando que los operadores de ransomware Akira explotaron CVE-2023-20269, una vulnerabilidad de día cero en la función VPN de acceso remoto de dos de sus productos: el software Cisco Adaptive Security Appliance (ASA) y Software Cisco Firepower Thread Defense (FTD).

Cisco informó que los actores maliciosos que explotan CVE-2023-20269 pueden identificar credenciales válidas de las que se podría abusar para establecer sesiones VPN de acceso remoto no autorizadas y, para las víctimas que ejecutan la versión 9.16 del software Cisco ASA o anterior, establecer una sesión VPN SSL sin cliente.

Akira comúnmente se infiltra en sistemas Windows y Linux específicos a través de servicios VPN, especialmente donde los usuarios no han habilitado la autenticación multifactor. Para obtener acceso a los dispositivos de las víctimas, los atacantes utilizan credenciales comprometidas.

Una vez que un sistema está infectado con Akira, el malware intenta eliminar carpetas de respaldo que podrían usarse para restaurar datos perdidos. Para ello ejecuta el siguiente comando de PowerShell:

powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject".

Luego, el ransomware cifra los archivos con determinadas extensiones y les añade la extensión ".akira" a cada uno de ellos. Mientras cifra, omite los archivos que se encuentren en las carpetas Recycle Bin, System Volume Information, Boot, ProgramData y Windows. También evitará cifrar los archivos del sistema Windows con las extensiones .exe, .lnk, .dll, .msi y .sys.

Akira Ransomware también usa la API de Windows Restart Manager para cerrar procesos o apagar servicios de Windows que puedan estar manteniendo un archivo abierto y evitar el cifrado.

Cada carpeta del ordenador contendrá una nota de rescate llamada akira_readme.txt que incluye información sobre lo que les ha pasado a los archivos de la víctima y enlaces al sitio de filtración de datos y al sitio de negociación de Akira.

"En cuanto a sus datos, si no llegamos a un acuerdo, intentaremos vender la información personal/secretos comerciales/bases de datos/códigos fuente – en general, todo lo que tenga un valor en el mercado negro – a varios actores de amenazas a la vez. Entonces todo esto se publicará en nuestro blog", amenaza la nota de rescate de Akira.

Cada víctima de Akira tiene una contraseña de negociación única que se ingresa en el sitio del actor de amenazas en la web oscura.

3. RECOMENDACIONES:

- Hacer uso del doble factor de autentificación.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.
- En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2023/10/ransomware-akira-activo-en-america.html • hxxps://cyberwarmag.com/akira-ransomware-amenaza/