BOLETÍN DE ALERTA

Boletín Nro.: 2024-14
Fecha de publicación: 06/09/2024
Tema: Aumento de infecciones por el ransomware Akira en la región

Descripción:

Akira es una variante de ransomware que se identificó por primera vez en el primer trimestre de 2023. Esta variante de malware ataca tanto a sistemas Windows como Linux. Las primeras versiones de la variante de ransomware Akira cifraban archivos con una extensión .akira; sin embargo, a partir de agosto de 2023, algunos ataques de Akira comenzaron cifrar archivos con una extensión .powerranges.

Técnicas de Acceso Inicial

Investigadores de ciberseguridad han observado que comúnmente los actores de amenazas de Akira obtienen acceso inicial a las organizaciones a través del servicio de red privada virtual (VPN) sin autenticación de múltiple factor activada (MFA), o principalmente utilizando vulnerabilidades conocidas de Cisco CVE-2020-3259 y CVE-2023-20269 y otros. Otros métodos de acceso inicial incluyen el uso de servicios externos como el Protocolo de Escritorio Remoto (RDP), el phishing dirigido o por medio de credenciales válidas exfiltradas.

Técnicas de Persistencia y Descubrimiento

Una vez obtenido el acceso inicial, los actores de amenazas de Akira:

- intentan abusar de las funciones de los controladores de dominio creando nuevas cuentas de dominio para establecer persistencia. En algunos casos, se identificó a actores de amenazas de Akira creando una cuenta administrativa llamada itadm.
- aprovechan técnicas de ataque post-explotación, como Kerberoasting, para extraer credenciales almacenadas en la memoria del proceso (LSASS).
- utilizan herramientas de extracción de credenciales como Mimikatz y LaZagne para facilitar la escalada de privilegios.
- herramientas como SoftPerfect y Advanced IP Scanner se utilizan a menudo con fines de descubrimiento de dispositivos de red (reconocimiento),
- los comandos net Windows se utilizan para identificar controladores de dominio y recopilar información sobre las relaciones de confianza del dominio.

Técnicas de Evasión de la Defensa

A medida que los actores de amenazas de Akira se preparan para el movimiento lateral, suelen desactivar el software de seguridad para evitar la detección. Se observo que utilizan PowerTool para terminar los procesos relacionados con el antivirus.

Técnicas de Exfiltación e Impacto

Los actores de amenazas de Akira aprovechan herramientas como FileZilla, WinRAR, WinSCP y RClone para exfiltrar datos.

Para establecer canales de comando y control, los actores de amenazas aprovechan herramientas fácilmente disponibles como AnyDesk, MobaXterm, RustDesk, Ngrok y Cloudflare Tunnel, lo que permite la exfiltración a través de diversos protocolos como el Protocolo de Transferencia de Archivos (FTP), el Protocolo de Transferencia de Archivos Seguro (SFTP) y servicios de almacenamiento en la nube como Mega para conectarse a servidores de exfiltración.

Los actores de amenazas de Akira utilizan un modelo de doble extorsión: cifran los sistemas después de exfiltrar los datos.

La nota de rescate de Akira proporciona a cada empresa un código único e instrucciones para ponerse en contacto con los actores de amenazas a través de una URL .onion. Generalmente, no dejan una demanda inicial de rescate o instrucciones de pago en las redes comprometidas, y no transmiten esta información hasta que son contactados por la víctima. Los pagos de rescate se realizan en Bitcoin a direcciones de billetera de criptomonedas proporcionadas por los actores de amenazas.

Para ejercer más presión, los actores de amenazas de Akira amenazan con publicar los datos exfiltrados en la red Tor.

Técnicas de Cifrado

Los actores de amenazas de Akira utilizan un sofisticado esquema de cifrado híbrido para bloquear los datos. Este enfoque de múltiples capas adapta los métodos de cifrado según el tipo y el tamaño del archivo, y es capaz de realizar un cifrado total o parcial. Los archivos cifrados se anexan con una extensión .akira o .powerranges.

Para inhibir aún más la recuperación del sistema, el encriptador de Akira (w.exe) utiliza comandos de PowerShell para eliminar las copias en sombra de volumen (VSS) en los sistemas Windows. Además, aparece una nota de rescate llamada fn.txt tanto en el directorio raíz (C:) como en el directorio de inicio de cada usuario (C:\Users).

Indicadores de Compromiso

Archivos maliciosos asociados al ransomware akira:

w.exe

Win.exe

AnyDesk.exe

Gcapi.dll

Sysmon.exe

Rclone.exe

Winscp.rnd

WinSCP-6.1.2- Setup.exe

Akira_v2

Megazord

VeeamHax.exe

Veeam-GetCreds.ps1

PowershellKer beros TicketDumper

sshd.exe

ipscan-3.9.1- setup.exe

winrar-x64- 623.exe

Medidas Preventivas y Mitigación

El CERT-PY recomienda a las organizaciones aplicar las siguientes mitigaciones para limitar el uso potencial de las técnicas comunes de descubrimiento de sistemas y redes, y para reducir el riesgo de compromiso por parte del ransomware Akira:

- Habilitar la autenticación de multiple factor (MFA) para todos los servicios en la medida de lo posible, especialmente para el correo web, la VPN y las cuentas que accedan a sistemas críticos.
- Priorizar la remediación de vulnerabilidades conocidas explotadas activamente.
- Aplicar parches y actualizar regularmente el software, las aplicaciones, sistemas operativos, firmware a su última versión, y realizar evaluaciones de vulnerabilidad periódicas.
- Auditar cuentas de usuarios con privilegios administrativos y configurar controles de acceso según el principio de privilegio mínimo.
- Deshabilitar puertos no utilizados
- **Mantener copias de seguridad de los datos fuera de línea y probar periódicamente las copias de seguridad y restauración**
- Asegurar que todos los datos de la copia de seguridad estén cifrados y sean inmutables

- Implementar un plan de recuperación para mantener y retener múltiples copias de archivos confidenciales en una ubicación físicamente separada, segmentada y segura (por ejemplo, disco duro, dispositivo de almacenamiento, la nube, etc)
- Requerir que todas las cuentas tengan inicios de sesión con contraseñas robustas
- Segmentar las redes para evitar la propagación de ransomware
- Identificar, detectar e investigar actividad anormal y posible recorrido del ransomware indicado con una herramienta de monitoreo de redes.
- Filtrar el tráfico de red evitando que orígenes desconocidos o que no sean de confianza accedan de forma remota a servicios de sistemas internos
- Revisar los controladores de dominio, servidores, estaciones de trabajo y directorios activos en busca de nuevos y/o cuentas no reconocidas

Validar controles de Seguridad

Los CIS Controls proporcionan un conjunto mínimo de prácticas y protecciones contra las amenazas más comunes e impactantes. Para ello, el CERT-PY cuenta con varios servicios de ciberseguridad sin costo, a disposición de Organismos y Entidades del Estado, que pueden ser consultados y aprovechados para aumentar los niveles de madurez en ciberseguridad.

El CERT-PY ofrece además el servicio de gestión de incidentes ciberneticos para apoyar a Organismos Públicos y Privados en la atención de incidentes, reportando los casos a abuse@cert.gov.py con la mayor cantidad de detalles. El CERT-PY mantiene la confidencialidad de las Organizaciones que reportan sus casos. Podría realizar alertas a la comunidad de forma anonimizada, con enfoque en la amenaza que pone en riesgo al ecosistema nacional.

Hasta la fecha no se han identificado sistemas de gobierno afectados por el malware. El CERT-PY continua con el monitoreo permanente de las amenazas.

Información adicional:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
- https://attack.mitre.org/versions/v14/matrices/enterprise/
- https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR_MITIC_01-21.pdf
- https://www.cert.gov.py/actualizaciones-de-seguridad-para-cisco-abordan-multiples-vulnerabilidades-de-alto-riesgo/
- https://community.cisco.com/t5/vpn/cve-id-2023-20269-to-mitigate-this-vulnerability/td-p/4924383