Nro. Alerta:	AL-2024-017	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	06-ago-2024	**Ransomware AKIRA**	Pág.: **1** of **11**

I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: Ransomware AKIRA

Nivel de riesgo: Alto

II. ALERTA

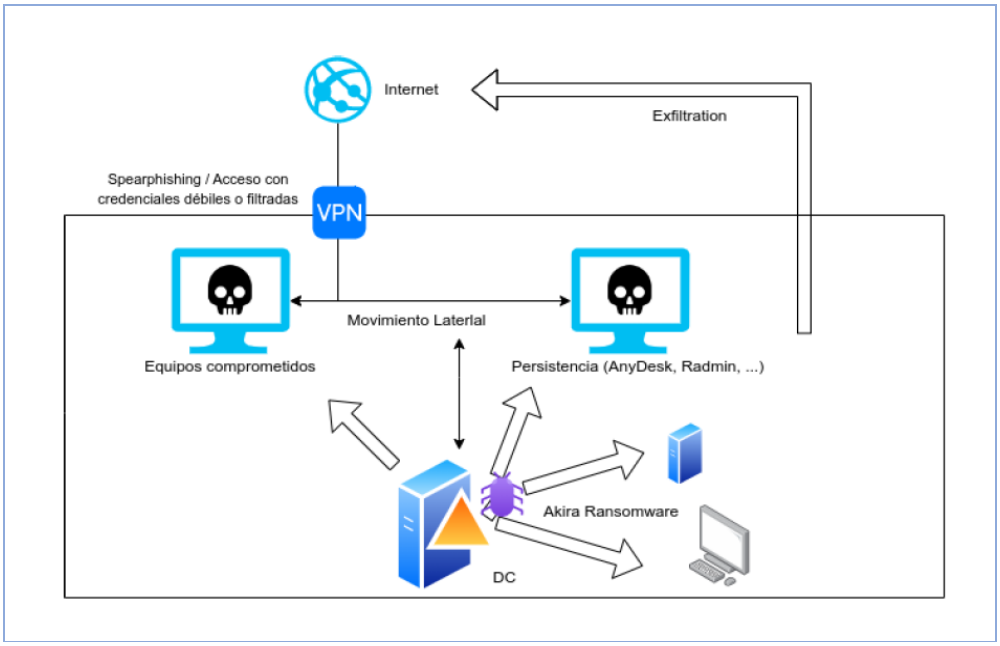

Figura 1.- ***Ransomware AKIRA***

III. INTRODUCCIÓN

El malware Akira de tipo ransomware fue identificado en marzo de 2023 y es operado por un grupo que ha estado activo desde entonces realizando diferentes campañas donde ha impactado a muchas víctimas, la mayoría de ellas localizadas en los Estados Unidos,

Europa y Australia; así también han sido afectadas por estos ataques algunas industrias que incluye educación, finanzas, bienes raíces, construcción, salud; Prestadores de Servicios de Telecomunicaciones, entre otras. En abril de 2023, tras un enfoque inicial en los sistemas Windows, los actores de amenazas de Akira implementaron una variante de Linux dirigida a las máquinas virtuales VMware ESXi. Al 1 de enero de 2024, el grupo de ransomware ha afectado a más de 250 organizaciones y ha obtenido aproximadamente 42 millones de dólares en ganancias por ransomware.

El grupo de ransomware tiene como estrategia la doble extorsión donde no solo cifran los datos, sino que también ex filtran información sensible, amenazando con venderla o filtrarla públicamente si no se cumple con el pago del rescate. Esta estrategia aumenta las posibilidades de pago de las víctimas y, para apoyarla técnicamente, el grupo cuenta con un sitio web de estilo retro en la red Tor, donde hacen públicos los datos robados si las víctimas no pagan el rescate demandado. Además, en dicho sitio web también ofrecen una función de chat para que las víctimas puedan comunicarse con ellos utilizando un ID único que incluyen para cada una en la nota de rescate.

Al igual que la mayoría de ransomware, Akira utiliza criptografía simétrica y asimétrica para cifrar los ficheros en los equipos de sus víctimas. En concreto, cuando se ejecuta Akira calcula una clave de cifrado y vector de inicialización aleatorios para el algoritmo Chacha20. Estos valores son cifrados con RSA a través de una clave pública que se encuentra embebida en el propio código y que los actores cambian por cada víctima. A diferencia de Conti, en el que se basa su código, y de la mayoría de ransomware, Akira calcula una única clave de cifrado que es utilizada para cifrar todos los ficheros. Por tanto, si se averigua esta clave, se podrían llegar a descifrar.

IV. VECTOR DE ATAQUE:

El FBI y los investigadores de ciberseguridad han observado que los actores de amenazas de Akira obtienen acceso inicial a las organizaciones a través de un servicio de red privada virtual (VPN) sin autenticación multifactor (MFA) configurada, principalmente utilizando vulnerabilidades conocidas de Cisco [T1190] CVE-2020-3259 y CVE-2023-20269.[2],[3]; los métodos adicionales de acceso inicial incluyen el uso de servicios externos como el

Protocolo de escritorio remoto (RDP) [T1133], phishing selectivo [T1566.001] [T1566.002] y el abuso de credenciales válidas [T1078].

Una vez que se obtiene el acceso inicial, los actores de amenazas de Akira intentan abusar de las funciones de los controladores de dominio mediante la creación de nuevas cuentas de dominio [T1136.002] para establecer la persistencia. En algunos casos, el FBI identificó a los actores de amenazas de Akira creando una cuenta administrativa llamada *itadm.*

Según informes del FBI y de fuentes abiertas, los actores de amenazas de Akira aprovechan las técnicas de ataque posteriores a la explotación, como Kerberoasting, para extraer credenciales almacenadas en la memoria de proceso del Servicio de subsistema de autoridad de seguridad local (LSASS) [T1003.001].

Los actores de amenazas de Akira también utilizan herramientas de extracción de credenciales [T1003] como Mimikatz y LaZagne para ayudar en la escalada de privilegios.

Herramientas como SoftPerfect y Advanced IP Scanner se utilizan a menudo para fines de descubrimiento (reconocimiento) de dispositivos de red [T1016] y los comandos net de Windows se utilizan para identificar controladores de dominio [T1018] y recopilar información sobre relaciones de confianza de dominio [T1482].

V. IMPACTO:

Los actores de amenazas de Akira utilizan herramientas como FileZilla, WinRAR [T1560.001], WinSCP y RClone para exfiltrar datos [T1048]. Para establecer canales de comando y control, los actores de amenazas utilizan herramientas disponibles como AnyDesk, MobaXterm, RustDesk, Ngrok y Cloudflare Tunnel, lo que permite la exfiltración a través de varios protocolos como el Protocolo de transferencia de archivos (FTP), el Protocolo de transferencia segura de archivos (SFTP) y servicios de almacenamiento en la nube como Mega [T1537] para conectarse a servidores de exfiltración.

Los actores de amenazas de Akira utilizan un modelo de doble extorsión [T1657] y cifran los sistemas [T1486] después de exfiltrar datos. La nota de rescate de Akira proporciona a cada empresa un código único e instrucciones para contactar a los actores de amenazas a través de una URL .onion.

Los actores de amenazas de Akira no dejan una demanda de rescate inicial ni instrucciones de pago en las redes comprometidas y no transmiten esta información hasta que la víctima se pone en contacto con ellos. Los pagos de rescate se realizan en Bitcoin a las direcciones de billetera de criptomonedas proporcionadas por los actores de amenazas. Para ejercer más presión, los actores de amenazas de Akira amenazan con publicar datos exfiltrados en la red Tor y, en algunos casos, han llamado a las empresas víctimas, según informes del FBI.

Los actores que operan Akira cuentan con un sitio en la red TOR para enumerar las organizaciones presuntamente afectadas por su ransomware y ofrecer enlaces de descarga de los datos recopilados por ellos en caso de no pagar el rescate demandado. El sitio tiene un aspecto retro y para navegar por él es necesario especificar comandos como si de una terminal se tratase. Si se indica el comando “leaks” se puede acceder a la descarga de los ficheros de las compañías que aparentemente no han pagado el rescate demandado. Por otra parte, con el comando “news” se obtiene un listado de todas las compañías a las que habrían comprometido hasta el momento. Con el comando “contact” se puede enviar un mensaje a los actores.

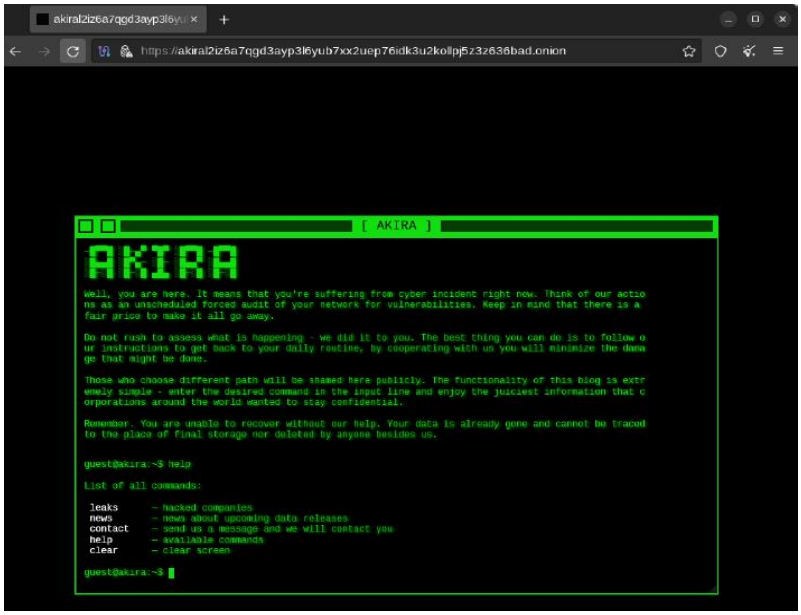

Figura 2.- ***Ransomware AKIRA - Sitio oficial de publicación de leaks de los actores de Akira en la red TOR***
(hxxps://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion)

VI. INDICADORES DE COMPROMISO

Descargo de responsabilidad: Se recomienda investigar o verificar estos indicadores antes de tomar medidas, como bloquearlos.

Archivos maliciosos asociados con Akira Ransomware

Nombre del archivo	Hash (SHA-256)	Descripción
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Akira ransomware encryptor
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Remote desktop application
Gcapi.dll	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	DLL file that assists with the execution of AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Ngrok tool for persistence
Config.yml	Varies by use	Ngrok configuration file
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Exfiltration tool
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Network file transfer program
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Network file transfer program
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f750ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	Akira_v2 ransomware
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fcdfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f079f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c	Akira “Megazord” ransomware

Nombre del archivo	Hash (SHA-256)	Descripción
	9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Plaintext credential leaking tool
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	PowerShell script for obtaining and decrypting accounts from Veeam servers
PowershellKerberos TicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Kerberos ticket dumping tool from LSA cache
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	OpenSSH Backdoor
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Network scanner that scans IP addresses and ports

Nombre del archivo	Hash (MD5)	Descripción
winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c	Network file transfer program

Descargo de responsabilidad: si bien los actores de amenazas de Akira pueden cambiar la fecha y la hora, un análisis de terceros confiable confirmó que estas muestras se crearon el 28 de diciembre de 2023.

Hash (SHA-256)
0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f

Hash (SHA-256)
a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2
643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64

Comandos asociados con Akira Ransomware

Persistencia y Descubrimiento
nltest /dclist: [T1018]
nltest /DOMAIN_TRUSTS [T1482]
net group “Domain admins” /dom [T1069.002]
net localgroup “Administrators” /dom [T1069.001]
tasklist [T1057]
rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full [T1003.001]
Credenciales de Acceso
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db" /d "C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<firefox_profile_id>.default-release\key4.db.tmp” **Nota:** Se utiliza para acceder a los datos de Firefox.
cmd.exe /Q /c esentutl.exe /y "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /d "C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data.tmp” **Nota:** Se utiliza para acceder a los datos de Google Chrome.
Impacto
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject" [T1490]

Para obtener ayuda con el mapeo de la actividad cibernética maliciosa al marco MITRE ATT&CK, consulte las Mejores prácticas de CISA y MITRE ATT&CK para el mapeo de MITRE ATT&CK y la herramienta *Decider* de CISA.

VII. RECOMENDACIONES:

Ante un ataque de ransomware, es fundamental actuar con rapidez y seguir un conjunto de pasos específicos para minimizar el daño y aumentar las posibilidades de recuperación.

Algunos pasos a seguir son:

- **Implementar un plan de recuperación** para mantener y conservar varias copias de datos y servidores confidenciales o de propiedad privada en una ubicación físicamente separada, segmentada y segura (por ejemplo, disco duro, dispositivo de almacenamiento, la nube).

- **Exigir que todas las cuentas con inicios de sesión con contraseña** (por ejemplo, cuentas de servicio, cuentas de administrador y cuentas de administrador de dominio) cumplan con los estándares del NIST. En particular, exigir a los empleados que utilicen contraseñas largas y considerar no exigir cambios de contraseña recurrentes, ya que esto puede debilitar la seguridad.

- **Exigir autenticación multifactor** para todos los servicios en la medida de lo posible, en particular para correo web, redes privadas virtuales y cuentas que acceden a sistemas críticos.

- **Mantener todos los sistemas operativos, software y firmware actualizados**. La aplicación oportuna de parches es uno de los pasos más eficientes y rentables que una organización puede tomar para minimizar su exposición a amenazas de ciberseguridad. Priorizar la aplicación de parches a las vulnerabilidades explotadas conocidas en los sistemas conectados a Internet.

- **Segmentar las redes para evitar la propagación de ransomware.** La segmentación de la red puede ayudar a prevenir la propagación de ransomware al controlar los flujos de tráfico entre varias subredes y el acceso a ellas, y al restringir el movimiento lateral del adversario.

- **Identificar, detectar e investigar la actividad anormal y el posible cruce del ransomware indicado con una herramienta de monitoreo de redes.** Para ayudar a detectar el ransomware, implemente una herramienta que registre e informe todo el tráfico de la red, incluida la actividad de movimiento lateral en una red. Las herramientas de detección y respuesta de endpoints (EDR) son particularmente útiles para detectar conexiones laterales, ya que tienen información sobre las conexiones de redes comunes y poco comunes para cada host.

- **Filtrar el tráfico de la red al evitar que orígenes desconocidos o no confiables accedan a servicios remotos en sistemas internos.** Esto evita que los actores de amenazas se conecten directamente a los servicios de acceso remoto que han establecido para la persistencia.

- **Instalar, actualizar** regularmente y habilitar la detección en tiempo real del software antivirus en todos los hosts.

- **Revisar los controladores de dominio**, servidores, estaciones de trabajo y directorios activos en busca de cuentas nuevas o no reconocidas.

- **Audite** las cuentas de usuario con privilegios administrativos y configure los controles de acceso según el principio de privilegio mínimo.

- **Desactive** los puertos no utilizados.

- **Considere agregar un banner de correo electrónico** a los correos electrónicos recibidos desde fuera de su organización.

- **Desactive los hipervínculos** en los correos electrónicos recibidos.

- **Implemente el acceso basado en el tiempo para las cuentas configuradas en el nivel de administrador y superior.** Por ejemplo, el método de acceso Just-in-Time (JIT) proporciona acceso privilegiado cuando es necesario y puede respaldar la aplicación del principio de privilegio mínimo (así como el modelo Zero Trust). Este es un proceso en el que se establece una política para toda la red para deshabilitar automáticamente las cuentas de administrador en el nivel de Active Directory cuando

la cuenta no tiene una necesidad directa. Los usuarios individuales pueden enviar sus solicitudes a través de un proceso automatizado que les otorga acceso a un sistema específico durante un período de tiempo determinado cuando necesitan respaldar la finalización de una determinada tarea.

- **Desactive las actividades y permisos de línea de comandos y secuencias de comandos.** La escalada de privilegios y el movimiento lateral a menudo dependen de utilidades de software que se ejecutan desde la línea de comandos. Si los actores de amenazas no pueden ejecutar estas herramientas, tendrán dificultades para escalar privilegios y/o moverse lateralmente.

- **Mantener copias de seguridad de los datos sin conexión y realizar copias de seguridad y restauraciones de forma regular.** Al implementar esta práctica, la organización ayuda a garantizar que no se verán gravemente interrumpidas y/o que solo tendrán datos irrecuperables.

- **Garantizar que todos los datos de copia de seguridad estén cifrados**, sean inmutables (es decir, no se puedan alterar ni eliminar) y cubran toda la infraestructura de datos de la organización.

- **Utilizar herramientas de análisis de tráfico de red** para monitorear y examinar el tráfico en busca de patrones o comportamientos sospechosos. Esto puede ayudar a identificar posibles comunicaciones de comando y control utilizadas por el ransomware para comunicarse con los servidores de los atacantes.

- **Implementar una solución de filtrado de contenido web** que bloquee el acceso a sitios web maliciosos o de alto riesgo. Esto puede evitar que los usuarios accedan accidentalmente a páginas que contienen descargas de ransomware o enlaces a sitios comprometidos.

- **Dividir la red en segmentos o subredes más pequeñas y restringir el tráfico entre ellas**. Esto limita la propagación del ransomware en caso de una infección, ya que el malware tendría dificultades para moverse de un segmento a otro. Además, se pueden aplicar políticas de seguridad más estrictas en los segmentos críticos que contienen datos sensibles.

Adicional, se recomienda visitar la página web del EcuCert, la sección de “CONSEJOS”, en la cual se publica información relacionada con recomendaciones para la seguridad digital respecto a Ransomware.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- **CISA (2024).** *#StopRansomware: Akira Ransomware* https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
- **Basque CyberSecurity Centre (2024).** *Akira Ransomware* https://www.ciberseguridad.eus/sites/default/files/2023-08/BCSC-Malware-Akira-TLPClear_v2.pdf
- **Mitre ATT&CK (2024).** Akira. **https://attack.mitre.org/groups/G1024/**