Nro. Alerta:	AL-2025-042	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	12-ago-2025	Akira Ransomware	Pág.: **1** of **11**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Akira Ransomware - figura referencial

Akira Ransomware reaparece teniendo como principal objetivo a los MSP o Managed Service Providers (Proveedores de Servicios Gestionados) empresas que ofrecen servicios de gestión de Tecnologías de información (TI).

III. INTRODUCCIÓN

Akira Ransomware usa un modelo de negocio RaaS (Ransomware as a Service) en el que desarrolladores de malware venden o alquilan su software a otros atacantes. Emplea también el modelo de doble extorsión, que es la encriptación de los datos y el robo de información confidencial con amenaza de filtración publica sino se paga el rescate.

Akira Ransomware se enfoca en atacar los MSP con credenciales robadas de inicio de sesión robadas y la explotación de vulnerabilidades, lo cual representa un cambio estratégico hacia la maximización de su impacto, ya que los atacantes al comprometer estos proveedores otorga acceso a extensas redes de clientes y amplifica los pagos potenciales de rescate.

IV. VECTOR DE ATAQUE

Se detalla el proceso de ataque técnico:

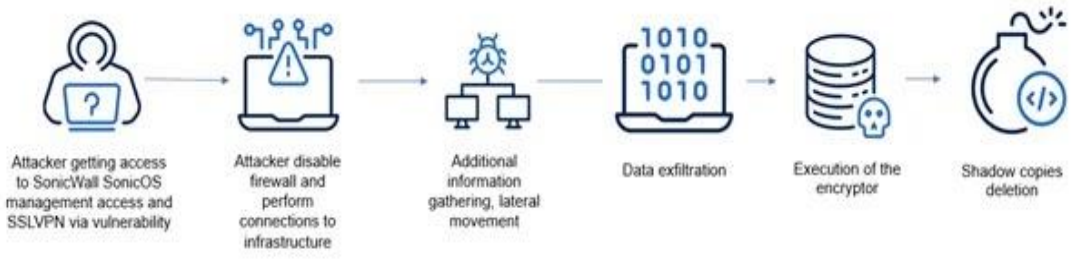

Figura 2.- Flujo de ataque (Fuente Acronis) – Akira Ransomware

Acceso inicial

Inicio sus ataques en el 2023, mediante la modalidad de phishing aprovechando una vulnerabilidad para tener acceso a los dispositivos de sus víctimas, documentada bajo el CVE-2023-20269: Es una vulnerabilidad en la función de acceso remoto VPN del software Cisco Adaptive Security Appliance (ASA) y del software Cisco Firepower Threat Defense (FTD) permite a un atacante remoto no autenticado llevar a cabo un ataque de fuerza bruta con el fin de identificar combinaciones válidas de nombre de usuario y contraseña o a un atacante remoto autenticado establecer una sesión SSL VPN sin cliente o con un usuario no autorizado.

En 2024, se centró principalmente en las VPN de los usuarios, al aprovechar diversas vulnerabilidades, incluida la de SonicWall Firewall que permitía a los atacantes desactivar firewalls y conectarse a las infraestructuras objetivo, documentada bajo CVE-2024-40766: Una vulnerabilidad de control de acceso inadecuado en el acceso de administración de SonicWall Sonic OS, lo que podría dar lugar a un acceso no autorizado a los recursos y en condiciones específicas, provocar el bloqueo del firewall. Este problema afecta a los dispositivos SonicWall Firewall Gen 5 y Gen 6, así como a los dispositivos Gen 7 que ejecutan SonicOS 7.0.1-5035 y versiones anteriores.

En 2025, la Unidad de investigación de amenazas (TRU) de Qualys (plataforma líder en seguridad y cumplimiento basada en la nube), detectó que los operadores de Akira Ransomware estaban utilizando credenciales de administradores robadas o compradas para intentar obtener acceso a máquinas y servidores.

Investigación del FBI, revela el proceso de ataque de Akira Ransomware, una vez que gana el acceso inicial, intenta abusar de las funciones de los controladores de dominio, creando nuevas cuentas para mantener el acceso persistente en este entorno, FBI informa que observo una cuenta administrativa creada con el nombre itadm, con esto Akira Ransomware busca moverse lateralmente, escalar privilegios y evadir detección.

La técnica de ataque posterior a la explotación es Kerberoasting, un ataque cibernético que explota el protocolo Kerberos**,** que es usado en redes de Windows Active Directory para extraer credenciales almacenadas en la memoria de proceso del Servicio del Subsistema de Autoridad de Seguridad Local (LSASS), utilizando herramientas como Minikatz. Otras herramientas que revelan la investigación son LaZagne para facilitar el escalamiento de privilegios, SofPerfect y Advanced IP Scanner se utilizan para descubrimiento de dispositivos de red y comandos Net de windows para identificar controladores de dominios con el fin de recopilar información de los dominios.

Evasión de Defensa

Según investigaciones realizadas por terceros de confianza, han observado a Akira Ransomware desplegando dos variantes distintas de ransomware contra diferentes arquitecturas de sistemas dentro del mismo evento de compromiso. Esto supone un cambio con respecto a la actividad del ransomware recientemente reportada. En un primer momento, se observó que Akira Ransomware desplegaba el ransomware Megazord, específico para Windows, pero un análisis más detallado reveló que en este ataque se desplegó simultáneamente un segundo payload (que más tarde se identificó como una nueva variante del cifrador Akira Ransomware ESXi, Akira_v2).

Cuando Akira Ransomware se prepara para el movimiento lateral, desactiva el software de seguridad para evitar ser detectado, se observó que utilizan PowerTool para explotar el controlador Zemana AntiMalware y terminar los procesos relacionados con el antivirus.

Exfiltración e Impacto

Más herramientas en uso, FileZilla, WinRAR, WinSCP y RClone son usados para la extracción de datos. Para establecer canales de comando y control (C2), Akira Ransomware utiliza herramientas fácilmente disponibles como AnyDesk, MobaXterm, RustDesk, Ngrok y Cloudflare Tunnel, lo que les permite extraer datos a través de diversos protocolos, como el Protocolo de Transferencia de Archivos (FTP), el Protocolo Seguro de Transferencia de Archivos (SFTP) y servicios de almacenamiento en la nube como Mega para conectarse a servidores de extracción de datos.

La nota de rescate de Akira Ransomware (archivo akira_readme.txt) proporciona a cada empresa un código único e instrucciones para ponerse en contacto con los autores de la amenaza a través de la dark web (.onion). No dejan una demanda inicial de rescate 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 del rescate se realizan en bitcoins a direcciones de monederos de criptomonedas proporcionadas por los autores de la amenaza.

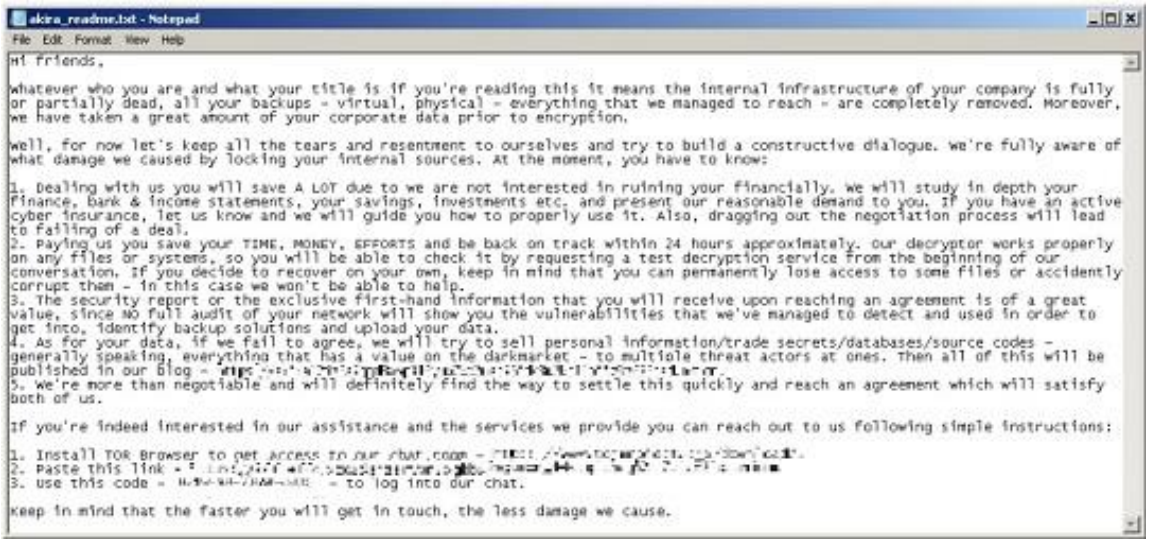

Figura 3.- Nota de Rescate – Akira Ransomware

Encriptación

Encriptación de Akira Ransomware, utiliza un sofisticado esquema de cifrado híbrido para bloquear los datos. Esto implica combinar un algoritmo de cifrado ChaCha20 con un sistema criptográfico de clave pública RSA para lograr velocidad y un intercambio seguro de claves.

Este enfoque multicapa adapta los métodos de cifrado en función del tipo y el tamaño del archivo y es capaz de realizar un cifrado total o parcial. Los archivos cifrados se añaden con la extensión .akira o .powerranges. Para inhibir aún más la recuperación del sistema, el cifrador de Akira Ransomware (w.exe) utiliza comandos de PowerShell para eliminar los servicios de instantáneas de volumen (VSS) en los sistemas Windows.

Un análisis realizado por terceros de confianza identificó que el cifrador Akira_v2 es una actualización de su versión anterior, que incluye funcionalidades adicionales debido al lenguaje en el que está escrito (Rust). Las versiones anteriores del cifrador ofrecían opciones para insertar argumentos en tiempo de ejecución, entre ellas:

- -p --encryption_path (targeted file/folder paths)
- -s --share_file (targeted network drive path)
- -n --encryption_percent (percentage of encryption)
- --fork (create a child process for encryption.

La capacidad de insertar subprocesos adicionales permite a Akira Ransomware tener un control más granular sobre el número de núcleos de CPU en uso, lo que aumenta la velocidad y la eficiencia del proceso de cifrado. La nueva versión también añade una capa de protección, utilizando el ID de compilación como condición de ejecución para dificultar el análisis dinámico. El cifrador no puede ejecutarse correctamente sin el ID de compilación único. También se ha observado que Akira_v2 tiene la capacidad de desplegarse solo en máquinas virtuales utilizando vmonly y la capacidad de detener máquinas virtuales en ejecución con las funcionalidades stopvm. Después del cifrado, la variante Linux ESXi puede incluir la extensión de archivo akiranew o añadir una nota de rescate llamada akiranew.txt en los directorios donde se cifraron los archivos con la nueva nomenclatura.

Se muestra la TABLA MITRE ATT&CK's de Akira Ransomware:

TACTICA	TECNICA	DESCRIPCION
Initial Access	T1078 – Valid Accounts	Los atacantes obtienen y utilizan indebidamente las credenciales de cuentas existentes como medio para obtener acceso inicial.
	T1190 – Exploit Public-Facing Application	Los atacantes obtienen acceso inicial a las organizaciones a través de un servicio de red privada virtual (VPN) sin autenticación multifactorial (MFA) configurada
	T1133 - External Remote Services	Otros métodos de acceso inicial incluyen el uso de servicios externos como el Protocolo de Escritorio Remoto (RDP).
	T1566 – Phishing	Los atacantes usan tecnicas de phishing con archivos adjuntos o mediante links enviado a las victimas
Credential Access	T1003 - OS Credential Dumping	Uso de herramientas como Mimikatz y LaZagne para extraer credenciales.
	T1003.001 – Credential Dumping LSASS Memory	Los atacantes intentan acceder al material de credenciales almacenado en la memoria de proceso del LSASS.

TACTICA	TECNICA	DESCRIPCION
Discovery	T1016 – System Network Configuration Discovery	Uso de herramientas para escanear sistemas e identificar servicios que se ejecutan en hosts remotos y en la infraestructura de red local.
	T1082 - System Information Discovery	Utilizan herramientas como PCHunter64 para obtener información detallada sobre los procesos y el sistema.
	T1482 - Domain Trust Discovery	Uso del comando net de Windows para enumerar la información del dominio.
	T1057 - Process Discovery	Uso de la utilidad Tasklist para obtener detalles sobre los procesos en ejecución a través de PowerShell.
	T1069.001 - Permission Groups Discovery: Local Groups	Los atacantes utilizan el grupo local de net localgroup /dom para encontrar grupos de sistemas locales y configuraciones de permisos.
	T1069.002 - Permission Groups Discovery: Local Groups	Los atacantes utilizan el comando net group /domain para intentar encontrar grupos a nivel de dominio y configuraciones de permisos.
	T1018 – Remote System Discovery	Los atacantes utilizan nltest / dclist para recopilar una lista de otros sistemas por dirección IP, nombre de host u otros identificadores lógicos en una red.
Persistence	T1136.002 - Create Account: Domain Account	Los atacantes intentan abusar de las funciones de los controladores de dominio creando nuevas cuentas de dominio para establecer persistencia.
Defense Evasion	T1562.001 - Impair Defenses: Disable or Modify Tools	Los atacantes utilizan ataques BYOVD para desactivar el software antivirus.
Command and Control (C2)	T1219 - Remote Access Software	Los atacantes utilizan software legítimo de soporte técnico para ordenadores de escritorio, como AnyDesk, para obtener acceso remoto a los sistemas de las víctimas.
	T1090 – Proxy	Los atacantes utilizaron Ngrok para crear un túnel seguro hacia los servidores que facilitó la filtración de datos.
Collection	T1560.001 - Archive Collected Data: Archive via Utility	Los autores de amenazas Akira utilizan herramientas como WinRAR para comprimir archivos.
Exfiltration	T1048 – Exfiltration Over Alternative Protocol	Los atacantes utilizan herramientas de transferencia de archivos como WinSCP para transferir datos.
	T1537 – Transfer Data to Cloud Account	Los atacantes utilizan herramientas como CloudZilla para extraer datos a una cuenta en la nube y conectarse a

TACTICA	TECNICA	DESCRIPCION
		servidores de extracción que ellos controlan.
	T1657.002 – Exploit Public-Facing Application	Los atacantes utilizaron RClone para sincronizar archivos con servicios de almacenamiento en la nube con el fin de extraer datos.
Impact	T1486 - Date Encrypted for Impact	Los atacantes cifran los datos de los sistemas objetivos para interrumpir la disponibilidad de los recursos del sistema y de la red.
	T1490 - Inhibit System Recovery	Los atacantes eliminan las **Volume Shadow Copies** (VSS) en los sistemas Windows.
	T1657 - Financial Theft	Los atacantes utilizan un modelo de doble extorsión para obtener beneficios económicos.

Tabla 1. - TÁCTICAS Y TÉCNICAS DE MITRE ATT&CK – Akira Ransomware

V. IMPACTO

Akira ransomware tiene su impacto en:

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

Además de utilitarios propios del sistema:

UTILITARIOS	DESCRIPCION
AdFind	AdFind.exe se utiliza para consultar y recuperar información de Active Directory.
Advanced IP Scanner	Un escáner de red se utiliza para localizar todos los ordenadores de una red y realizar un análisis de sus puertos. El programa muestra todos los dispositivos de red, da acceso a las carpetas compartidas y permite el control remoto de los ordenadores (a través de RDP y Radmin).
AnyDesk	Un software común que puede ser utilizado de forma maliciosa por los actores maliciosos para obtener acceso remoto y mantener la persistencia. AnyDesk también admite la transferencia remota de archivos.
LaZagne	Permite a los usuarios recuperar contraseñas almacenadas en sistemas Windows, Linux y OSX.
PCHunter64	Una herramienta utilizada para obtener información detallada sobre procesos y sistemas.
PowerShell	Una solución multiplataforma para la automatización de tareas compuesta por un shell de línea de comandos, un lenguaje de scripting y un marco de gestión de la configuración, que se ejecuta en Windows, Linux y macOS.
MiniKatz	Permite a los usuarios ver y guardar credenciales de autenticación, como los tickets Kerberos.
Ngrok	Una herramienta de proxy inverso utilizada para crear un túnel seguro hacia servidores protegidos por cortafuegos o máquinas locales sin dirección IP pública.

UTILITARIOS	DESCRIPCION
RClone	Un programa de línea de comandos utilizado para sincronizar archivos con servicios de almacenamiento en la nube como Mega.
SoftPerfect	Un escáner de red (netscan.exe) utilizado para hacer ping a ordenadores, escanear puertos, descubrir carpetas compartidas y recuperar información sobre dispositivos de red a través de Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) y PowerShell. También escanea servicios remotos, el registro, archivos y contadores de rendimiento.
WinRAR	Se utiliza para dividir datos comprometidos en segmentos y comprimir archivos en formato .RAR para su exfiltración.
WinSCP	Windows Secure Copy es un cliente gratuito y de código abierto para el protocolo de transferencia de archivos SSH, el protocolo de transferencia de archivos, WebDAV, Amazon S3 y el protocolo de copia segura. Los autores de amenazas Akira lo han utilizado para transferir datos desde una red comprometida a cuentas controladas por ellos.

***Tabla* 2** - Herramientas utilizadas - Akira Ransomware

VI. INDICADORES DE COMPROMISOS

Archivos maliciosos asociados con Akira Ransomware:

ARCHIVO	HASH (SHA-256)	DESCRIPCION
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9ace-bda37df6da1987bf48e5b05e	Encriptador Akira ransomware.
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Aplicación de escritorio remoto.
Gcapi.dll	73170761d6776c0debac-fbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	DLL File ayuda con la ejecución de AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Ngrok herramienta para la persistencia.
Rclone.exe	aaa647327ba5b855bedea8e889b3fa-fdc05a6ca75d1cfd98869432006d6fecc9	Herramienta de Exfiltracion
Winscp.rnd	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Programa de transferencia de archivos de red
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Programa de transferencia de archivos de red
Akira_v2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75	Akira_v2 ransomware
	0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc	Akira “Megazord” ransomware
	dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198	
	131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07	
	9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c	

ARCHIVO	HASH (SHA-256)	DESCRIPCION
	9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065	
	2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83	
	7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be	
	95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a	
	0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d	
	C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Herramienta para filtrar credenciales de texto sin formato.
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	Script de PowerShell para obtener y descifrar cuentas de servidores Veeam
PowershellKerberosTicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Herramienta de volcado de tickets Kerberos desde la caché LSA
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	OpenSSH Backdoor
ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Escáner de red que escanea direcciones IP y puertos.

Tabla 3.- Archivos maliciosos SHA-256 – Akira Ransomware

ARCHIVO	HASH (MD5)	DESCRIPCION
winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c	Programa de transferencia de archivos por red

Tabla 4.- Archivos maliciosos MD5 - Akira Ransomware

Hash (SHA-256)
0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2
643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64

Tabla 5.- Muestras de Windows - Akira Ransomware

Hash (SHA-256)
e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f
74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1
3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4

Tabla 6.- Muestras de formato ejecutable y enlazable (ELF) – Akira Ransomware para Linux/Unix

Persistencia y descubrimiento
nltest /dclist
nltest /DOMAIN_TRUSTS
net group “Domain admins” /dom
net localgroup “Administrators” /dom
tasklist
rundll32.exe c:\Windows\System32\comsvcs.dll, MiniDump ((Get-Process lsass).Id) C:\windows\temp\lsass.dmp full

Tabla 7.- Comandos asociados – Akira Ransomware

Acceso a credenciales -Para acceder a los datos de Firefox.
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”

Tabla 8.- Comandos asociados – Akira Ransomware en Firefox

Acceso a credenciales -Para acceder a los datos de Chrome.
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”

Tabla 9.- Comandos asociados – Akira Ransomware en Chrome

VII. RECOMENDACIONES:

- Limita las conexiones VPN solo a direcciones IP conocidas y de confianza.
- Aunque se ha observado que Akira puede evadir la autenticación multifactor, sigue siendo una capa adicional de seguridad importante.
- Mantén todos los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad.
- Revisa regularmente las cuentas de usuario y elimina aquellas que no estén en uso.
- Implementa políticas de contraseñas fuertes y cámbialas periódicamente.
- Utiliza herramientas de detección y respuesta en endpoints para identificar y bloquear actividades maliciosas.
- Aprovecha las capacidades de protección en la nube para detectar amenazas emergentes.
- Asegúrate de que las configuraciones de seguridad no puedan ser alteradas por malware.

- Haz copias de seguridad frecuentes de los datos críticos y almacénalas en ubicaciones seguras y desconectadas de la red principal.
- Asegúrate de que las copias de seguridad sean completas y funcionales mediante pruebas periódicas.
- Ofrece formación regular sobre buenas prácticas de ciberseguridad y concienciación sobre phishing y otras técnicas de ingeniería social.
- Realiza simulacros de ataques para evaluar la preparación y respuesta del personal ante incidentes de seguridad.

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:

RANSOMWAREHELP (2025). Análisis del Ransomware Akira. https://www.ransomwarehelp.com/es/tipos-de-ransomware/akira-analisis-2025/

ACRONIS (2025). MSPs, un objetivo principal para Akira y LYNX Ransomware. https://www.acronis.com/es-es/tru/posts/msps-a-top-target-for-akira-and-lynx-ransomware/

CYBERSECURITY NEWS (2025). Akira and LYNX Ransomware Target MSPs in Coordinated Attacks. https://cybersecuritynews.com/akira-and-lynx-ransomware/

CISA (2024). Cybersecurity Advisory: AA24-109A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

EcuCERT (2024). Alerta Técnica: Ransomware Akira. https://www.ecucert.gob.ec/wp-content/uploads/2024/08/Ransomware_Akira.pdf

QUALYS (2024). Threat Brief: Understanding Akira Ransomware. https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware