Advertencia

Técnica

Actividad de Akira Ransomware

COLCERT AD-20251115-031

TLP:CLEAR

Resumen Ejecutivo

NIVEL DE RIESGO

ALTO

La operación del *ransomware* **Akira** continúa activa y en evolución, dirigiendo ataques contra organizaciones de múltiples sectores mediante la explotación de vulnerabilidades conocidas, accesos remotos expuestos y abuso de credenciales válidas. Este grupo mantiene un modelo de doble extorsión y ha ampliado sus capacidades para comprometer entornos **Windows**, **Linux** y plataformas de virtualización como **ESXi** y **Nutanix**, lo que evidencia una campaña sostenida con alta capacidad de adaptación. La actividad reciente confirma que los actores siguen buscando perímetros vulnerables, sin parchear y servicios VPN expuestos, por lo que esta amenaza representa un riesgo inmediato para cualquier organización que no haya aplicado medidas de mitigación y controles de seguridad prioritarios.

Métodos de acceso inicial

Explotación de aplicaciones expuestas (T1190): los actores de Akira explotan vulnerabilidades en servicios VPN públicos sin MFA. Las debilidades identificadas son:

CVE	Tecnología afectada	CVSS	Descripción
CVE-2020-3259	Cisco ASA y Cisco FTD	**7.5 (Alto)**	Permite a un atacante remoto recuperar contenidos de memoria al enviar URL especialmente formadas.
CVE-2023-20269	Cisco ASA y FTD — Remote access VPN feature	**5.0 (Medio)**	Permite ataques tipo *brute-force* sobre credenciales o establecimiento de sesiones SSL VPN no autorizadas.
CVE-2020-3580	Cisco ASA y FTD	**6.1 (Medio)**	Permiten a un atacante inducir a un usuario a ejecutar scripts en el contexto del administrador/web UI.
CVE-2023-28252	Microsoft Windows - Common Log File System (CLFS)	**7.8 (Alto)**	Elevación de privilegios (EoP) por escritura fuera de límites en el driver CLFS
CVE-2024-37085	VMware (ESXi / VMware Cloud Foundation components)	**7.2 (Alto)**	Permite a un atacante remoto obtener acceso a funciones administrativas en infraestructuras virtualizadas.
CVE-2023-27532	Veeam Backup & Replication	**7.5 (Alto)**	Permite a un atacante sin autenticación dentro del perímetro de backup obtener credenciales cifradas desde la base de configuración (config DB),
CVE-2024-40711	Veeam Backup & Replication (vulnerabilidad de deserialización)	**9.8 (Crítico)**	Deserialización de datos no confiables que permite ejecución remota de código (RCE) sin autenticación en instancias vulnerables de Veeam.
CVE-2024-40766	SonicWall SonicOS / Firewalls (Gen5/Gen6/Gen7)	**9.8 (Crítico)**	Permite a un atacante remoto sin privilegios ejecutar acciones no autorizadas y comprometer dispositivos perimetrales.

Servicios remotos externos (T1133): uso de conexiones RDP (Remote Desktop Protocol) para entrar a sistemas. Conexiones vía VPN cuando no está habilitado el MFA, lo que facilita el acceso no autorizado.

***Phishing* dirigido** (T1566.001 - T1566.002): *spearphishing* mediante adjuntos o enlaces maliciosos que ejecutan código o descargan *malware*.

Uso de credenciales válidas (T1078): abuso de cuentas legítimas (con credenciales previamente comprometidas) para entrar en sistemas críticos. Esto puede combinarse con los otros vectores para escalar el acceso inicial.

Actividades observadas en la intrusión

Durante las fases posteriores al acceso, se han identificado los siguientes comportamientos:

Reconocimiento y descubrimiento dentro de la red: una vez obtienen acceso inicial, los actores de amenaza comienzan a mapear el entorno para entender la estructura del dominio y localizar activos sensibles. Ejecutan comandos como "*nltest /dclist*" o "*net group "Domain Admins" /dom*" para identificar controladores de dominio, grupos privilegiados y relaciones de confianza. (T1018 - T1069.002). Además, realiza una lista de recursos compartidos y equipos accesibles en la red con el fin de planear el movimiento lateral. (T1087 - T1135).

Obtención y abuso de credenciales: Akira busca elevar privilegios para ganar control real sobre la infraestructura. Realiza la extracción de credenciales a través del volcado del proceso LSASS, una técnica clásica para recolectar usuarios y contraseñas (T1003.001). También hace uso de técnicas de *Kerberoasting* para obtener hashes de cuentas de servicio con privilegios elevados (T1558.003). Estas credenciales capturadas son clave para acceder a servidores críticos y expandir la intrusión sin generar alertas visibles.

Movimiento lateral: Akira tiende a evitar herramientas intrusivas que los defensores puedan detectar rápidamente. En su lugar, aprovechan utilidades o plataformas comunes como el acceso a sistemas mediante AnyDesk, MobaXterm o Ngrok, aprovechando su apariencia legítima para saltar entre equipos (T1219 - T1090). Realiza autenticación con las cuentas comprometidas previamente para desplazarse sin disparar detecciones basadas en comportamiento (T1078).

Evasión de defensas y persistencia: mientras avanzan, también se encargan de reducir la capacidad de detección de la organización. Hace uso de herramientas como PowerTool para deshabilitar componentes de seguridad o finalizar procesos asociados a antivirus y EDR (T1562.001). Además, crea nuevas cuentas en el dominio para mantener acceso continuo y evitar bloqueos posteriores (T1136.002).

Preparación y exfiltración de información: antes de cifrar los sistemas, Akira recopila y extrae información con fines de doble extorsión. Usa rclone, FTP/SFTP o servicios *cloud* para mover grandes volúmenes de datos fuera de la red comprometida (T1048 - T1567.002).

Cifrado y acciones de impacto: una vez tienen control suficiente y han asegurado la información exfiltrada, ejecutan el componente final: el cifrado. Eliminan copias de seguridad para impedir recuperación local (T1490). Luego cifran los sistemas críticos con extensiones como .akira o .powerranges, lo que detiene operaciones y habilita la fase de extorsión (T1486).

Mitigaciones recomendadas

MITIGACIÓN	ID MITIGACIÓN	DESCRIPCIÓN
Multi-factor Authentication (MFA)	M1032	Reduce significativamente el riesgo de acceso con credenciales robadas o reutilizadas (vector frecuente en campañas de Akira: uso de cuentas válidas y acceso remoto). Recomendable aplicar MFA en VPN, RDP, cuentas de administrador y servicios *cloud*.
Network Segmentation	M1030	Limita el movimiento lateral y el alcance del cifrado y exfiltración al aislar servidores críticos (controladores de dominio, backups, servidores de archivos). Muy útil frente a la enumeración de dominio y desplazamiento que realizan los operadores de Akira.
Privileged Account Management (PAM)	M1026	Controla y limita el uso de cuentas privilegiadas mediante políticas de mínimos privilegios, rotación de contraseñas, vaults, sesiones controladas y monitoreo. Dificulta que el actor escale privilegios y comprometa sistemas críticos como servidores AD.
Execution Prevention (application control / script blocking)	M1038	Evita o dificulta la ejecución de payloads y scripts maliciosos (PowerShell, herramientas de carga lateral, ejecución de binarios no autorizados). Ayuda a bloquear componentes de cifrado y etapas intermedias usadas por Akira
Network Intrusion Prevention / Filtering	M1031	Detecta y bloquea patrones de C2, exfiltración y descargas maliciosas (rclone, FTP, túneles como Ngrok) en el perímetro y entre segmentos. Útil para interceptar transferencias de datos y tráfico de herramientas remotas legítimas usadas por el adversario.

Recomendaciones

- **Actualizar de manera prioritaria todos los sistemas afectados por las vulnerabilidades explotadas por Akira**, especialmente Cisco ASA/FTD, Veeam Backup & Replication, SonicWall y plataformas VMware. Aplicar parches reduce significativamente la superficie de ataque y evita que el actor utilice *exploits* ya conocidos para obtener acceso inicial o elevar privilegios.

- **Restringir el acceso externo a servicios expuestos** como VPN, RDP, SSH, puertos administrativos, paneles web y consolas de backup, aplicando listas de control (ACL), reglas de firewall, geobloqueo y limitación por direcciones IP de confianza. Esta acción disminuye la probabilidad de explotación remota y ataques de fuerza bruta contra credenciales.

- **Implementar autenticación multifactor (MFA)** en todos los accesos a VPN, consolas administrativas y aplicaciones críticas, de manera que incluso si el adversario obtiene credenciales válidas, no pueda autenticarse ni moverse lateralmente con facilidad dentro del entorno.

- **Monitorear de forma continua los logs y eventos relacionados con intentos fallidos de autenticación**, anomalías en conexiones VPN, creación de cuentas inesperadas, modificaciones en políticas de backup y accesos sospechosos a infraestructura crítica. La detección temprana ayuda a identificar actividad de intrusión antes de que se complete el ciclo del ataque.

- **Segmentar la red** para limitar la capacidad del actor de acceder a múltiples sistemas una vez que compromete un solo punto. Aislar servidores de backup, controladores de dominio, infraestructura de virtualización y dispositivos perimetrales reduce drásticamente el impacto potencial del movimiento lateral.

- **Reforzar la seguridad de la infraestructura de respaldo asegurando que los servidores Veeam estén en redes aisladas**, sin exposición a Internet y con credenciales diferenciadas, además de activar repositorios inmutables que dificulten el borrado o cifrado de copias de seguridad por parte del actor.

- **Deshabilitar servicios web innecesarios**, interfaces administrativas remotas y funciones de VPN que no se utilicen. Minimizar la cantidad de servicios expuestos disminuye las oportunidades de explotación de vulnerabilidades como las observadas en ASA, FTD y SonicWall.

- Auditar las configuraciones de dispositivos de red, firewalls perimetrales y appliances de seguridad para verificar que no existan configuraciones débiles, credenciales por defecto o reglas que permitan el acceso desde cualquier origen. Este proceso asegura que el entorno no tenga brechas inadvertidas.

- **Fortalecer los controles** de privilegios implementando el principio de mínimo privilegio, rotación de contraseñas, vaults de credenciales y supervisión activa de cuentas de administrador. Reducir el abuso de privilegios limita el alcance de la intrusión cuando el actor logra obtener una cuenta privilegiada.

- **Revisar detenidamente los indicadores de compromiso (IOC) proporcionados**, los cuales pueden ser integrados en los sistemas de seguridad perimetral. Se sugiere realizar la validación correspondiente para asegurar que su implementación no afecte la disponibilidad operativa ni la continuidad de los servicios.

Tácticas, técnicas y Procedimientos (TTP) identificadas

El siguiente gráfico presenta la matriz de Tácticas, Técnicas y Procedimientos (TTP) observadas en la operación de **Akira**, mapeados al *framework* MITRE ATT&CK. Esta vista permite identificar el comportamiento del actor a lo largo de cada fase de la intrusión y entender cómo avanza desde el acceso inicial hasta el impacto final.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1098: Account Manipulation	T1222: File and Directory Permissions Modification	T1110: Brute Force	T1087: Account Discovery	T1021: Remote Services	T1560: Archive Collected Data	T1105: Ingress Tool Transfer	T1048: Exfiltration Over Alternative Protocol	T1486: Data Encrypted for Impact
T1133: External Remote Services	T1059.001: PowerShell	T1136: Create Account	T1068: Exploitation for Privilege Escalation	T1562: Impair Defenses	T1555: Credentials from Password Stores	T1482: Domain Trust Discovery	T1550: Use Alternate Authentication Material		T1572: Protocol Tunneling	T1567: Exfiltration Over Web Service	T1657: Financial Theft
T1566: Phishing	T1059.005: Visual Basic	T1133: External Remote Services	T1078: Valid Accounts	T1036: Masquerading	T1003: OS Credential Dumping	T1046: Network Service Discovery			T1090: Proxy	T1537: Transfer Data to Cloud Account	T1490: Inhibit System Recovery
T1078: Valid Accounts	T1059.003: Windows Command Shell	T1078: Valid Accounts		T1027: Obfuscated Files or Information		T1069: Permission Groups Discovery			T1219: Remote Access Tools		
	T1569: System Services			T1550: Use Alternate Authentication Material		T1057: Process Discovery					
	T1569.002: Service Execution			T1078: Valid Accounts		T1018: Remote System Discovery					
						T1082: System Information Discovery					
						T1016: System Network Configuration Discovery					

Indicadores de compromiso

TIPO DE IOC	VALOR
MD5	EEFCD1AB5B3638C870730E459D3545ED
SHA1	EFB651A5C755A9A5A96B08DDDA736EFD0BC03315
SHA256	3298D203C2ACB68C474E5FDAD8379181890B4403D6491C523C13730129BE3F75
MD5	7D827558E7841CC2887FC99537C1C97E
SHA1	94ED0A9C9C9FE568DC814218EDEB17B951FC78A8
SHA256	0EE1D284ED663073872012C7BDE7FAC5CA1121403F1A5D2D5411317DF282796C
MD5	FD380DB23531BB7BB610A7B32FC2A6D5
SHA1	A129C2CFF13F7672E27F4C43608DA2293E1B5BB7
SHA256	DFE6FDDC67BDC93B9947430B966DA2877FDA094EDF3E21E6F0BA98A84BC53198
MD5	4EDC0EFE1FD24F4F9EA234B83FCAEB6A
SHA1	02BB630FAF77A91C7DE6B031B54DE4467AB9DA6F
SHA256	131DA83B521F610819141D5C740313CE46578374ABB22EF504A7593955A65F07
MD5	3F63951399F8CD578E2A6FAED2C9C0F0
SHA1	B8C1772DD0AD018CF3ED4C67EABD16C5C4E751CD
SHA256	9F393516EDF6B8E011DF6EE991758480C5B99A0EFBFD68347786061F0E04426C
MD5	E5CF95B6BD04B89447E6C4ED71105A1C
SHA1	D640D5E632D260AC5A9E26DF1BDB9B337F32CBBC
SHA256	9585AF44C3FF8FD921C713680B0C2B3BBC9D56ADD848ED62164F7C9B9F23D065
MD5	64F8E1B825887AFE3130AF4BF4611C21
SHA1	09F85D9C0DE66C8F807BD1E12F55617E3FED3BF8
SHA256	2F629395FDFA11E713EA8BF11D40F6F240ACF2F5FCF9A2AC50B6F7FBC7521C83
MD5	A18D79E94229FDF02EF091CF974ED546
SHA1	73EE462CB96F4857F9F5BBDC4CADA5800F2B8932
SHA256	7F731CC11F8E4D249142E99A44B9DA7A48505CE32C4EE4881041BEEDDB3760BE
MD5	9F801240AF1124B66DEFCD4B4AE63F2A
SHA1	1FF0C089C5A3B93E95C337E7644119C7BD7133C6
SHA256	95477703E789E6182096A09BC98853E0A70B680A4F19FA2BF86CBB9280E8EC5A
MD5	74D5D4E9A556A6170F19893E7FFDEFFA
SHA1	F8425E27FB5340B4D50BDEE1800DCC428A7D388F
SHA256	0C0E0F9B09B80D87EBC88E2870907B6CACB4CD7703584BAF8F2BE1FD9438696D
MD5	9DF999F142F137B0794B8AFCAAEDC588
SHA1	A420FBD6CB9D10DB807251564C1C9E1718C6FBC5
SHA256	C9C94AC5E1991A7DB42C7973E328FCEEB6F163D9F644031BDFD4123C7B3898B0
MD5	0F7B6BB3A239CF7A668A8625E6332639
SHA1	5263A135F09185AA44F6B73D2F8160F56779706D
SHA256	18051333E658C4816FF3576A2E9D97FE2A1196AC0EA5ED9BA386C46DEFAFDB88
MD5	8EA891A3B4049AA059F9BCE52574BE5C
SHA1	57E46697761AA19423765497E9E6A8ABBD3F94A9
SHA256	5E1E3BF6999126AE4AA52146280FDB913912632E8BAC4F54E98C58821A307D32
MD5	6B7BBA769DB3701E13214CB70CA5A54D
SHA1	669CB358392A71DD68F684C0BA68DF2106E6DB36
SHA256	58359209E215A9FC0DAFD14039121398559790DBA9AA2398C457348EE1CB8A4D
MD5	02F307E1B6F1C44FCB0A06E9E8A572BE
SHA1	AAA5CB0A1939303F37EAFA6B6D12811069F7D15E
SHA256	58AFEF43CEC0EE7A2FBFD9CDD5B71F55F971672D5E523A400B82B98C752CA5B7
MD5	DE8F808BA308E34097AFA5C3136A0640
SHA1	5961A99181DF157B81D35A50EEB27F96577A2FA2
SHA256	4CB8365B18B1C319D374BE0B9D219144C20FB8714E9CF346E655F854D2C60170

TIPO DE IOC	VALOR
MD5	0BB4254ED7B3C281968516A0C87D5510
SHA1	EF328F68C6D865BA4EF4223B5D8EE9EFB5667420
SHA256	71BB8B15B1FBAB1EBE7CD7898397D8A8A627AF06DC510437F25887AA0AA0E4E1
MD5	7E4DE8AF0F2EB3686AB73212EDBA48F7
SHA1	5BF2ADC96DB955268326FB5C58796CCFACD3C673
SHA256	0B5B31AF5956158BFBD14F6CBF4F1BCA23C5D16A40DBF3758F3289146C565F43
MD5	603D91D52BE2D92E2D67866D06272FB0
SHA1	9D0C956524C0D93A1B215AE37753F05BC18BB343
SHA256	0D700CA5F6CC093DE4ABBA9410480EE7A8870D5E8FE86C9CE103EEC3872F225F
MD5	3D18A75D8BAA6693B471D0FA85A62C39
SHA1	2347CBA8679297A3547AA0E250F48690CB18CBC5
SHA256	A2DF5477CF924BD41241A3326060CC2F913AFF2379858B148DDEC455E4DA67BC
MD5	33A406D761BBA10D201BDBF87D42953B
SHA1	CA5F0EF0CDF6B6599C4DA650A20A6064117BA3A6
SHA256	03AA12AC2884251AA24BF0CCD854047DE403591A8537E6ABA19E822807E06A45
MD5	2940779F88CF063CA5DCF861EC7BF325
SHA1	DE858B475BF1B0C16BBC0AB15B21690F739344CD
SHA256	2E88E55CC8EE364BF90E7A51671366EFB3DAC3E9468005B044164BA0F1624422
MD5	3D55EC08F082E2F149216C6CD60E0FDF
SHA1	525D1D0CC5EB6CEEC9C16EE76D316DB3FEB849A6
SHA256	40221E1C2E0C09BC6104548EE847B6EC790413D6ECE06AD675FFF87E5B8DC1D5
MD5	9CE8E06F1DE868E553758B242B82A1C4
SHA1	FA4F010FFA3A8E970CC4F47E86FF13DBB50C9FEC
SHA256	5EA65E2BB9D245913AD69CE90E3BD9647EB16D99230114537256548 6C77568A2
MD5	D24CD19A50E6D574A0CFDFC07C6D22BB
SHA1	4F43F7A18761312F7E71C2FBDEF2CAE39C55CF56
SHA256	643061AC0B51F8C77F2ED202DC91AFB9879F796DDD974489209D45F84F644562
MD5	A94A0BC0FF90B0466C36326598714FA4
SHA1	9F4F702B7A1D9DF0FBC93570AA2046316DFEAAE4
SHA256	6F9D50BAB16B2532F4683EEB76BD25449D83BDD6C85BF0B05F716A4B49584F84
MD5	EFD6896140A769C2F7142CEFBD68FC3D
SHA1	5D868FEFB0CB93A2FE79D97D95ABF1474CFB4456
SHA256	FEF09B0AA37CBDB6A8F60A6BD8B473A7E5BFFDC7FD2E952444F781574ABCCF64
MD5	EF29DC7B8F5A7B05706215F0F71F7995
SHA1	7866D3DF2C8A14C3C09089D874CE3D80D76FFFDA
SHA256	E1321A4B2B104F31ACEAF4B19C5559E40BA35B73A754D3AE13D8E90C53146C0F
MD5	2ACF0461CB310AD4109CCE68E4C07AFE
SHA1	72078BB1FBA164E99308763C05D273FA24549C4F
SHA256	74F497088B49B745E6377B32ED5D9DFAEF3C84C7C0BB50FABF30363AD2E0BFB1
MD5	CF1951F7084A180094C7092C7BB54998
SHA1	33339E5C0523123343E211E3B73CA89360D10621
SHA256	3D2B58EF6DF743CE58669D7387FF94740CEB0122C4FC1C4FFD81AF00E72E60A4

Fuentes

Cybersecurity and Infrastructure Security Agency (CISA) – United States, 13 noviembre 2025, título: #StopRansomware: Akira Ransomware, clasificación de la fuente: Alerta/Advisory gubernamental, URL:

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a