Grupo de ransomware Akira

Resumen ejecutivo

Desde su aparición a principios de 2023, el grupo **Akira ransomware** se ha posicionado como una de las amenazas más activas y agresivas dentro del modelo ransomware como servicio **(RaaS).** Su actividad ha crecido rápidamente, con más de un centenar de víctimas a nivel global, aunque mantiene un enfoque geográfico claro en Estados Unidos, distribuidas en sectores críticos, siendo el sector sanitario una de las principales industrias a las que se dirige Akira.

Akira destaca por su **capacidad técnica** y **enfoque selectivo**, adaptando sus cargas dañinas tanto a entornos **Windows** como **Linux**, lo que le permite operar en infraestructuras híbridas. Se apoya principalmente en el uso de credenciales comprometidas para acceder inicialmente a las redes de sus víctimas. Una vez dentro, ejecuta una estrategia de **doble extorsión**, cifrando los sistemas y exigiendo un pago adicional a cambio de no divulgar la información robada en su portal de filtraciones

El uso de **credenciales robadas y servicios VPN vulnerables** le permite a Akira obtener acceso inicial de forma sigilosa, evadiendo las defensas en etapas tempranas y manteniendo acceso persistente antes del despliegue del ransomware. A esto se suma el uso de herramientas legítimas como AnyDesk o aquellas basadas en Remote Desktop Protocol (RDP), lo que dificulta aún más su detección.

Akira se presenta como una **amenaza organizada** y con un enfoque estratégico claro. Su actividad creciente exige que las organizaciones refuercen la defensa en profundidad, priorizando la monitorización de accesos remotos, la detección de movimientos laterales, la segmentación de red y una capacidad de respuesta rápida, apoyándose en servicios de Ciberinteligencia.

Actor de amenazas: Akira

Akira es un grupo Ransomware-as-a-Service (RaaS) que emergió en marzo de 2023. Se considera que tiene vínculos con ex integrantes del grupo Conti, aprovechando ese legado técnico para consolidarse rápidamente en el panorama del ransomware.

Desde sus inicios, el grupo ha evolucionado lanzado versiones más avanzadas como Akira_v2 y herramientas escritas en Rust, como Megazord. Esto les permite realizar cifrados más específicos, atacando archivos críticos y sistemas virtualizados como VMware ESXi

Países y sectores afectados

Hasta enero de 2024, Akira habría comprometido más de 250 organizaciones y recaudado cerca de 42 millones USD en rescates. Sus ataques se concentran especialmente en Estados Unidos, seguido de países europeos y Australia.

España es uno de los países europeos más afectados por Akira. Durante 2025, el grupo ha atacado varias organizaciones españolas, entre ellas Druni S.A., Ste Group Key Corp y GPS 909, entre otras. Estos incidentes han evidenciado vulnerabilidades críticas en la protección de accesos remotos y en la gestión de vulnerabilidades, subrayando la necesidad de fortalecer las defensas en ciberseguridad.

Respecto a los sectores afectados, ataca principalmente a grandes empresas de los sectores educativo, financiero, manufacturero y sanitario, utilizando campañas de phishing y explotación de vulnerabilidades. Publica los datos robados en su sitio en la red Tor mediante una interfaz tipo consola, desde la cual también gestiona la comunicación con las víctimas

Análisis técnico

Akira emplea técnicas sofisticadas y un modelo operativo profesionalizado que le permiten una rápida adaptación a diferentes entornos. Utiliza vulnerabilidades en accesos remotos, movimientos laterales y herramientas legítimas para evadir detección, dificultando su análisis y mitigación.

Características técnicas principales:

- Ha retomado el uso de su **cifrador en C++ para sistemas Windows**, abandonando temporalmente las versiones en Rust para Linux. La nueva variante es una optimización de su carga útil original de 2023.
- Uso de un esquema de cifrado híbrido que combina los **algoritmos ChaCha20 y RSA**, orientado a tipos y tamaños de archivos específicos.
- Acceso inicial mediante **phishing**, **explotación de vulnerabilidades** en VPNs (como SonicWall y Cisco) y uso de **credenciales comprometidas** o **cuentas inactivas.**
- Realiza **movimientos laterales** mediante el uso de **herramientas legítimas** (LOLBAS), como RClone, WinSCP y Advanced IP Scanner.
- Akira aplica un modelo de **doble extorsión**: primero cifra los sistemas afectados y luego exige un rescate en bitcoins. Si la víctima no paga, amenaza con divulgar la información robada a través de su sitio en la red Tor.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1078 –** Valid Accounts **T1133 –** External Remote Services
Execution	**T1059.001 –** Command and Scripting Interpreter: PowerShell
Persistence	**T1133** – External Remote Services **T1078 –** Valid Accounts
Privilege Escalation	**T1078 –** Valid Accounts
Defense Evasion	**T1562.001 –** Impair Defenses: Disable or Modify Tools **T1036.005 –** Masquerading: Match Legitimate Resource Name or Location **T1027.001 –** Obfuscated Files or Information: Binary Padding
Credential Access	**T1558 –** Steal or Forge Kerberos Tickets
Discovery	**T1482 –** Domain Trust Discovery **T1018 –** Remote System Discovery
Lateral Movement	**T1021.001 –** Remote Services: Remote Desktop Protocol
Collection	**T1560.001 –** Archive Collected Data: Archive via Utility **T1213.002 –** Data from Information Repositories: Sharepoint
Exfiltration	**T1567.001 –** Exfiltration to Cloud Storage
Command and Control	**T1219 –** Remote Access Tools
Impact	**T1486 –** Data Encrypted for Impact **T1531 –** Account Access Removal **T1657 –** Financial Theft

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados (T1078 - Valid Accounts) y para accesos remotos (T1021.001 – Remote Services: RDP)
- ❑ Limitar el acceso a servicios remotos mediante concentradores gestionados como VPNs y otros sistemas de acceso remoto. (T1133 – External Remote Services)
- ❑ Auditar los cambios en herramientas de seguridad y configurar alertas ante modificaciones o desactivaciones para detectar actividad dañina. (T1562.001 - Impair Defenses: Disable or Modify)
- ❑ Limitar el acceso y activar el registro de actividades en SharePoint. (T1213.002 – Data from Information Repositories: Sharepoint)
- ❑ Segmentar la red para limitar el descubrimiento. (T1482 – Domain Trust Discovery)

Reactivas

- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos, desactivar PowerShell cuando no sea necesario o usar el modo "Constrained Language“ para restringir el acceso (T1059.001 - Command and Scripting Interpreter: PowerShell).
- ❑ Usar herramientas que detecten binarios con padding u ofuscación anómalos. (T1027.001 – Obfuscated Files or Information: Binary Padding)

Conclusiones y recomendaciones

Akira se posiciona como una amenaza destacada dentro del panorama de ransomware, operando bajo un modelo sofisticado que combina técnicas avanzadas con una estructura profesionalizada. Su capacidad para explotar vulnerabilidades en servicios remotos y emplear tácticas de doble extorsión lo convierte en un actor especialmente peligroso, capaz de afectar a organizaciones de gran tamaño en múltiples sectores y regiones.

La creciente actividad de grupos como Akira, junto con otros actores cibercriminales organizados, eleva el nivel de riesgo global, ampliando el impacto de sus campañas sobre infraestructuras críticas y empresas estratégicas. En este contexto, resulta fundamental implementar estrategias de defensa en profundidad y adoptar un enfoque proactivo y coordinado en ciberseguridad para mitigar sus efectos y proteger los activos más sensibles.

