

Resumen ejecutivo

Desde su aparición en 2022, el grupo **Qilin**, también conocido inicialmente como Agenda, se ha consolidado como una de las mayores amenazas dentro del ámbito del **ransomware como servicio** (RaaS, por sus siglas en inglés). Su actividad se caracteriza por un alto grado de sofisticación técnica, una evolución constante en sus métodos, y un enfoque estratégico que apunta a sectores críticos, como por ejemplo el sector sanitario. A nivel nacional se han identificado 10 víctimas en el último año.

Su capacidad de adaptación y versatilidad técnica permite personalizar los ataques en función del entorno de cada víctima (sistemas Windows, Linux y VMware ESXi), aumentando la efectividad y el impacto de sus operaciones. Además, Qilin emplea una **estrategia de doble extorsión**, exigiendo pagos tanto para descifrar los datos robados como para evitar su publicación, lo que incrementa la presión sobre las víctimas.

Qilin representa, por tanto, una amenaza avanzada, persistente y en evolución, con un enfoque claro hacia sectores donde el tiempo de recuperación es crítico. Su habilidad para comprometer entornos complejos mediante phishing dirigido (spear phishing), vulnerabilidades o uso de credenciales robadas, junto con el uso de técnicas de evasión de medidas defensivas, lo sitúa como una amenaza crítica a tener en cuenta. Ante este panorama, es imprescindible que las organizaciones refuercen sus defensas con medidas avanzadas de detección y respuesta, y se mantengan informados a través del servicio de vigilancia digital y alerta temprana de Cyberzaintza.

Grupo de ransomware: Qilin

Qilin es un grupo de ransomware que comenzó sus operaciones en julio de 2022 y se consolidó bajo el nombre actual en septiembre del mismo año. Este grupo opera bajo un modelo de Ransomware-as-a-Service (RaaS), ofreciendo su infraestructura y herramientas a afiliados a cambio de un porcentaje de las ganancias obtenidas. Esta estrategia ha contribuido a la expansión de Qilin en el ecosistema cibercriminal, haciéndolo atractivo para operadores independientes.

Qilin destaca por su estrategia de doble extorsión, en la cual, además de cifrar los archivos robados de las víctimas, exfiltra la información confidencial a través de la red Tor si no se paga el rescate. Esta táctica aumenta la presión sobre las víctimas, ya que se enfrentan tanto a la interrupción operativa como a la exposición pública de datos potencialmente sensibles.

Países y sectores afectados





Qilin se caracteriza por un enfoque amplio y oportunista, sin un ámbito geográfico definido, lo que le ha permitido comprometer organizaciones en múltiples regiones, como Estados Unidos, Reino Unido, Alemania, España, Francia, Canadá, Japón y Australia.

A nivel sectorial, Qilin ha centrado sus esfuerzos en industrias críticas como salud, manufactura, energía, educación, servicios legales y financieros, telecomunicaciones, defensa y administración pública, destacando su capacidad para generar un alto impacto en servicios esenciales y altamente dependientes de sus sistemas digitales.

Análisis técnico

Qilin combina técnicas avanzadas con una estructura altamente organizada y flexible, lo que le permite adaptarse rápidamente a distintos entornos y dificultar su detección, análisis y mitigación.

Características técnicas principales:

-  Desarrollado en Golang y Rust, lo que le permite una alta portabilidad y ejecución tanto en Windows como en Linux.
-  Utiliza algoritmos de cifrado simétricos y asimétricos robustos como ChaCha20, AES-256 y RSA-4096.
-  Qilin emplea múltiples técnicas de acceso inicial como phishing, explotación de vulnerabilidades y uso de credenciales robadas.
-  Utiliza diferentes técnicas de persistencia y escalada de privilegios como el uso de tareas programadas, la inyección de procesos y el volcado de credenciales de memoria.
-  Implementa medidas de ofuscación de código, además de técnicas para detectar si se está ejecutando en entornos de análisis, como máquinas virtuales o sistemas de prueba, y elimina cualquier rastro tras completar el ataque.
-  Utiliza canales de comunicación cifrados y portales web en la red TOR, asegurando el anonimato y dificultando su trazabilidad.
-  Los rescates son exigidos en criptomonedas (Bitcoin, Monero), sin garantía de recibir herramientas de descifrado tras el pago.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	T1078 – Valid Accounts T1566 – Phishing T1190 – Exploit Public-Facing Application
Execution	T1059 – Command and Scripting Interpreter T1569.002 – Service Execution
Persistence	T1037 – Boot or Logon Initialization Scripts T1053 – Scheduled Task/Job
Privilege Escalation	T1068 – Exploitation for Privilege Escalation T1548 – Abuse Elevation Control Mechanism T1055 – Process Injection
Defense Evasion	T1014 – Rootkit T1211 – Exploitation for Defense Evasion T1480 – Execution Guardrails T1497 – Virtualization/Sandbox Evasion T1027 – Obfuscated Files or Information
Credential Access	T1003 – OS Credential Dumping
Discovery	T1082 – System Information Discovery T1010 – Application Window Discovery T1046 – Network Service Discovery T1018 – Remote System Discovery
Lateral Movement	T1021 – Remote Services T1570 – Lateral Tool Transfer
Collection	T1005 – Data from Local System
Exfiltration	T1011 – Exfiltration Over Other Network Medium
Command and Control	T1001 – Data Obfuscation
Impact	T1486 – Data Encrypted for Impact T1485 – Data Destruction T1490 – Inhibit System Recovery T1561.001 – Disk Content Wipe

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados (T1078 - Valid Accounts).
- ❑ Aplicar control de ejecución de scripts y macros (ej. AppLocker, WDAC) y reforzar detección mediante EDRs (T1059 - Command and Scripting Interpreter).
- ❑ Monitorización de creación de tareas, hardening de políticas de tareas programadas (T1053 – Scheduled Task/Job).
- ❑ Asegurar que las copias de seguridad del controlador de dominio estén protegidas adecuadamente (T1003 - OS Credential Dumping).
- ❑ Segmentar la red de forma adecuada para proteger servidores y dispositivos críticos (T1046 - Network Service Discovery).
- ❑ Configurar los permisos para no permitir que usuarios interactúen con servicios de un nivel de permiso superior (T1569.002 – Service Execution).

Reactivas

- ❑ Configurar el firewall del sistema para bloquear o limitar el intercambio de archivos no autorizado entre equipos (T1570 - Lateral Tool Transfer).
- ❑ Eliminación de accesos remotos innecesarios a recursos compartidos de archivos, hipervisores, sistemas críticos, etc. (T1021 - Remote Services).
- ❑ Configurar el Control de Cuentas de Usuario (UAC por sus siglas en inglés) en su nivel más estricto para evitar la ejecución no autorizada de acciones con privilegios elevados (T1548 - Abuse Elevation Control Mechanism).

Conclusiones y recomendaciones

Qilin se consolida como una amenaza de alto impacto dentro del ecosistema de ransomware como servicio (RaaS, por sus siglas en inglés). Su modelo operativo destaca por una estructura profesionalizada y adaptable, que permite a una red de afiliados desplegar campañas altamente personalizadas y técnicamente avanzadas. Esta versatilidad implica el uso de múltiples técnicas, tácticas y procedimientos (TTPs), así como de indicadores de compromiso (IoCs), lo que dificulta su detección mediante mecanismos defensivos tradicionales.

Por otro lado, la creciente proliferación de grupos RaaS como Qilin, junto con grupos estatales o patrocinados por estados, incrementa el nivel de riesgo y extiende el alcance de las campañas hacia sectores críticos a nivel global. Frente a este panorama, resulta imprescindible implementar una defensa en profundidad y adoptar una estrategia de ciberdefensa proactiva, coordinada, y basada en inteligencia.

