I. DATOS GENERALES:

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

II. ALERTA

Figura 1. Grupo Qilin - figura referencial

Recientemente, Trend Research de Trend Micro identificó que el grupo Qilin implementó un binario de su ransomware basado en Linux en sistemas Windows, aprovechando indebidamente herramientas de administración remota y transferencia de archivos. Un aspecto llamativo del grupo Qilin es la evolución de su modelo de Ransomware como Servicio (RaaS), ya que ahora ofrece asesoría legal a sus afiliados para ejercer mayor presión durante las negociaciones de rescate

III. INTRODUCCIÓN

Activo desde el 2022, este grupo Qilin se detectó cuando sus atacantes tuvieron acceso a redes VPN usando protocolos de Escritorio Remoto (RDP) accediendo a servidores Microsoft System Center Configuration Manager (SCCM) donde establecieron persistencia para nuevos ataques. Meses después se presentó como un servicio RaaS bajo el nombre "Agenda" presentándose en un sitio de fugas dedicadas (DLS) confirmando así su presencia como un ransomware.

En 2023 una compañía de Asia reporto ser atacada por el grupo Qilin en la que los atacantes utilizaron SMB, RDP y WMI para el movimiento lateral de credenciales con lo cual exfiltraron aproximadamente 30 GB de datos al almacenamiento en la nube de MEGA a través de SSL.

En 2024, fue el año de ataques a varios países como Australia, Malaysia, Arabia Saudita, Indonesia, España, Reino Unido y EEUU. En EEUU comprometió una empresa (no divulgada) utilizando credenciales predeterminadas y RDP para el acceso inicial como el movimiento lateral. La exfiltración de datos se observó a través de FTP. En Reino Unido se centró su ataque en un proveedor de servicios de patología del Servicio Nacional de Salud con el robo de 400 GB de datos de pacientes.

Ahora en 2025 presento una creciente en su actividad maliciosa, en abril, una empresa de inversión en Corea del Sur fue el blanco del cual exfiltraron más de 1Tb de datos corporativos confidenciales, también en el mismo mes en EEUU, el Grupo Qilin se atribuyó la responsabilidad de exponer 150 GB de datos personales y legales de empleados del gobierno local, en los que incluían fotos de autopsia, licencias de conducir, números de seguro social.

En el mes de junio, un auge para el grupo Qilin, Trend Research identificó un sofisticado ataque de ransomware por parte del grupo Qilin, que desplegó su variante de ransomware para Linux en sistemas Windows en el que se utilizaron MeshAgent y MeshCentral para el despliegue. En este incidente reciente, los autores de la amenaza utilizaron un novedoso método de despliegue que combinaba WinSCP para la transferencia segura de archivos y Splashtop Remote para ejecutar el binario del ransomware para Linux en máquinas Windows. Con este ataque se desafía los controles de seguridad tradicionales centrados en Windows. La implementación de ransomware para Linux en sistemas Windows demuestra cómo los actores maliciosos se están adaptando para eludir los sistemas de detección de endpoints que no están configurados para detectar o impedir la ejecución de binarios Linux a través de canales de gestión remota.

En este mismo mes, un administrador del grupo Qilin llamado Haise, publico en el foro ruso RAMP (un sitio en la dark web de paga que es de interés para investigadores y ciberdelincuentes) el anuncio de sus planes de añadir una función de asistencia jurídica denominada "Call Lawyer" al panel RaaS. Este servicio pseudojurídico se

presentó como un asesoramiento jurídico destinado a ayudar a los afiliados a gestionar las negociaciones de extorsión y aumentar la presión sobre las víctimas, lo que reflejaba la madurez del ecosistema RaaS.

En el mes de julio el grupo Qilin reporto 73 víctimas en su sitio de filtración de fuga de datos (DLS), para luego entre agosto y septiembre alcanzar las 84 víctimas, convirtiéndolo en el grupo más activo del mundo, lo que demuestra un aumento en las actividades de reclutamiento de nuevos afiliados.

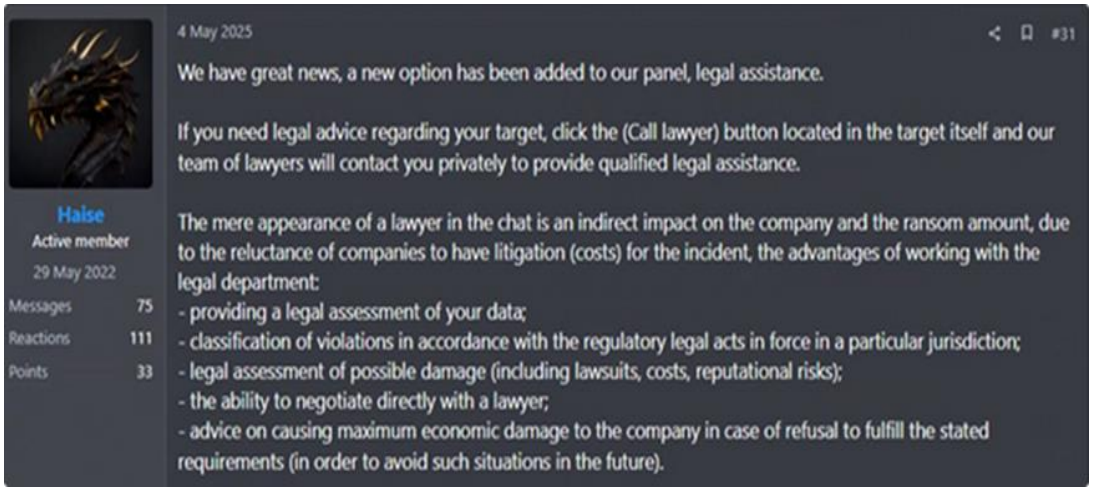

Figura 2. Anúncio del administrador en RAMP, Fuente: Malware News - Grupo Qilin

IV. VECTOR DE ATAQUE

Las técnicas de explotación empleadas por el grupo Qilin han cambiado a lo largo del tiempo, desde el uso de Spear Phishing, robo y compra de credenciales para acceso a empresas mediante conexiones VPN SSL.

Trend Micro Research que es la división de investigación y ciber inteligencia de Trend Micro, reporto la implementación de un binario del ransomware basado en Linux en Windows al abusar de herramientas legítimas de administración y transferencia de archivos.

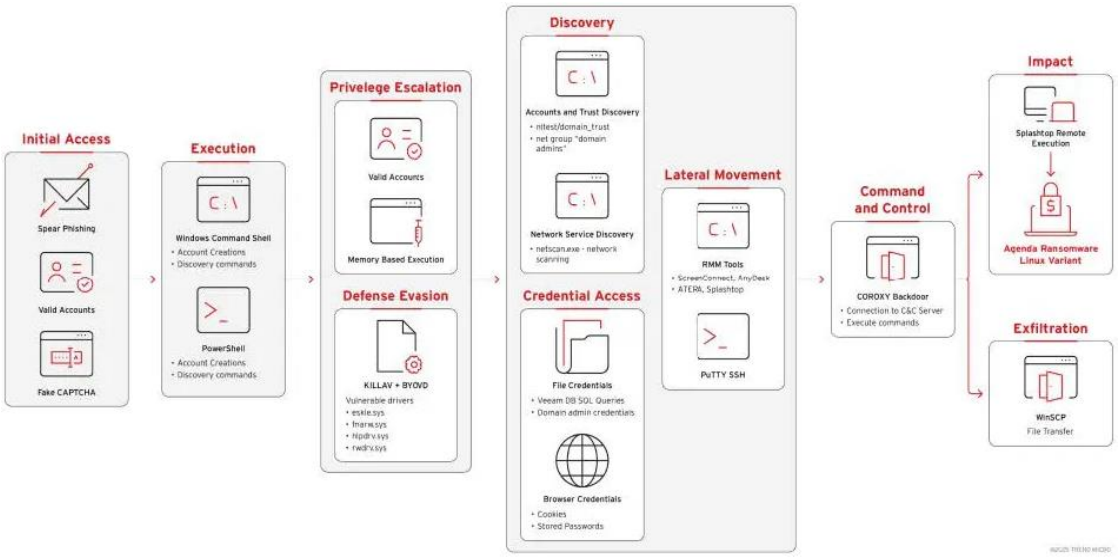

Figura 3. La cadena de infección basada en Linux en Windows - Grupo Qilin

Para esto los actores del grupo Qilin emplearon un enfoque híbrido. Hicieron uso de un ransomware multiplataforma Linux binario, difundiéndolo y ejecutándolo en los endpoints de Windows a través de servicios de administración remota o transferencia segura de archivos. Como resultado, la presencia del grupo se amplificó en Windows, Linux y entornos virtualizados.

La implementación final de ransomware mostró la ejecución multiplataforma. WinSCP se utilizó para la transferencia segura de archivos del binario de ransomware Linux al sistema Windows:

- C:\Users\<Username>\AppData\Local\Programs\WinSCP\WinSCP.exe
- C:\Users\<Username>\Desktop\mmh_linux_x86-64.filepart
- C:\Users\<Username>\Desktop\mmh_linux_x86-64

Una característica única de esta técnica era el uso del servicio de gestión de Splashtop Remote (SRManager.exe) para ejecutar el binario del ransomware Linux directamente en sistemas Windows:

- C:\Program Files (x86)\Splashtop\Splashtop Remote\Server\SRManager.exe
- C:\Users\<Username>\Desktop\mmh_linux_x86-64

Para ejecutar el binario de Linux en sistemas Windows, es probable que los atacantes habilitaran el Subsistema de Windows para Linux (WSL), que permite ejecutar archivos ejecutables nativos de Linux directamente en Windows sin necesidad de una máquina virtual completa. Es posible que hayan habilitado WSL mediante scripts automatizados o que lo hayan instalado manualmente a través de PowerShell o la línea de comandos, asegurándose de que el entorno estuviera listo para ejecutar malware basado en Linux. A través del acceso remoto proporcionado por Splashtop, pudieron desplegar y ejecutar el binario del ransomware Linux dentro del entorno WSL.

Este enfoque poco convencional parece combinar herramientas legítimas de administración remota con WSL para implementar malware multiplataforma, lo que podría evadir los controles de seguridad tradicionales centrados en Windows. El método de ejecución es significativo, ya que es posible que la mayoría de los sistemas de detección de endpoints no estén configurados para supervisar los binarios de Linux que se ejecutan a través de WSL, especialmente cuando se inician mediante herramientas legítimas de administración remota. Es posible que el binario del ransomware de Linux proporcionara capacidad multiplataforma, lo que permitía a los atacantes afectar tanto a los sistemas Windows como a los Linux del entorno utilizando un payload.

Se detalla el TTP actualizado usado por el grupo Qilin:

TÁCTICA	TÉCNICA	IDENTIFICACIÓN DE MITRE ATT&CK	DESCRIPCIÓN
Acceso inicial	Explotar una aplicación pública	T1190	Los actores de amenazas del grupo Qilin aprovechan las siguientes vulnerabilidades de FortiOS y FortiProxy: • CVE-2024-21762 para ejecución remota de código. • CVE-2024-55591 por eludir la autenticación.
Acceso inicial	Spearphishing (archivos adjuntos y enlaces)	T1566	Se ha observado que los actores de amenazas del grupo Qilin distribuyen malware a través de archivos adjuntos y enlaces de correo electrónico maliciosos.

TÁCTICA	TÉCNICA	IDENTIFICACIÓN DE MITRE ATT&CK	DESCRIPCIÓN
Ejecución	PowerShell	T1059.001	Los actores de amenazas del grupo Qilin utilizan scripts de PowerShell integrados para implementar la variante Rust de Qilin en servidores VMware vCenter y ESXi (sistemas de virtualización empresarial), así como PsExec (una herramienta de ejecución remota de Windows utilizada para movimiento lateral).
Ejecución	API nativa	T1106	El grupo Qilin llama a la función "LogonUserW" de la API nativa, proporcionando credenciales robadas válidas integradas en su configuración. Dado que las credenciales son válidas, Windows crea un inicio de sesión normal y devuelve un token de usuario utilizable.
Persistencia	Inicio automático mediante claves de ejecución del registro	T1547.001	Tras ejecutarse, el grupo Qilin crea una entrada de registro RunOnce llamada "aster" que apunta a enc.exe, una copia del malware alojada en la carpeta pública. Esto obliga a Windows a ejecutar automáticamente el ransomware una vez más en el siguiente reinicio.
Persistencia	Inicio automático basado en Winlogon	T1547.004	El grupo Qilin altera la configuración de Winlogon, por lo que Windows ejecuta automáticamente ejecutables de Qilin cada vez que un usuario inicia sesión.
Persistencia	Permitir el uso compartido de red para cifrar más archivos	T1112	El grupo Qilin altera la configuración del registro para hacer visibles las unidades de red asignadas por el administrador en todos los procesos, lo que brinda mucho más acceso a carpetas compartidas, servidores de archivos y almacenamiento de red que se pueden usar para cifrar datos a cambio de un rescate.
Escalada de privilegios	Explotación para la escalada de privilegios (BYOVD)	T1068	Los actores de amenazas del grupo Qilin pueden explotar vulnerabilidades en controladores firmados legítimos pero vulnerables (Bring Your Own Vulnerable Driver) u otros

TÁCTICA	TÉCNICA	IDENTIFICACIÓN DE MITRE ATT&CK	DESCRIPCIÓN
			componentes de software para obtener mayores privilegios en los hosts comprometidos, logrando potencialmente acceso a nivel de kernel y deshabilitando controles de seguridad para facilitar la implementación de ransomware.
Escalada de privilegios	Cuentas válidas: Cuentas de dominio	T1078.002	Los actores de amenazas del grupo Qilin pasan de un inicio de sesión de Citrix de bajo acceso a una cuenta de Active Directory filtrada o robada con altos privilegios mediante RDP (una herramienta de inicio de sesión remoto que brinda acceso completo al escritorio), lo que les permite impulsar cambios en todo el sistema mediante GPO (objetos de política de grupo) para implementar Qilin en toda la red.
Evasión de defensa	Eliminar artefactos	T1562 / T1070	El grupo Qilin oculta la actividad borrando los registros de eventos de Windows, eliminando o marcando el tiempo en los archivos y eliminando automáticamente malware para obstaculizar el análisis forense.
Descubrimiento	Panel de servicios en la nube y descubrimiento de copias de seguridad	T1538 / T1083	Los actores de amenazas del grupo Qilin revisan los portales de administración de la nube para realizar un seguimiento de los usuarios, sus roles y si las protecciones como la autenticación multifactor están habilitadas, luego buscan en SharePoint, recursos compartidos de archivos y consolas de respaldo para localizar rutas de respaldo, credenciales e instantáneas, preparándose para deshabilitar la recuperación y priorizar los objetivos
Movimiento lateral	Servicios remotos	T1021.002	El grupo Qilin activa MaxMpxCt en Windows para que se propague más rápido por la red. Integra PsExec y lo coloca en %Temp% con un nombre aleatorio para evitar la detección basada en archivos.

TÁCTICA	TÉCNICA	IDENTIFICACIÓN DE MITRE ATT&CK	DESCRIPCIÓN
Exfiltración	Exfiltración a través de servicio web/nube	T1567	Los atacantes del grupo Qilin comprimen los archivos robados con WinRAR. Luego abren Chrome en modo incógnito (para que el navegador no guarde el historial) y suben esos archivos ZIP a easyupload.io, un sitio público para compartir archivos, para que parezca tráfico web HTTPS normal.
Impacto	Datos cifrados para evitar impactos y eliminación VSS	T1486 / T1490	Los actores de amenazas de grupo Qilin utilizan consolas ScreenConnect robadas para distribuir Qilin a muchos clientes, deshabilitar las copias de seguridad para bloquear las restauraciones, forzar el modo seguro con funciones de red para que las herramientas de seguridad no se inicien y eliminar las instantáneas de volumen para evitar las reversiones. También borran los registros de eventos para ocultar la actividad, mapean más máquinas para priorizar los objetivos, establecen un fondo de pantalla con una nota de rescate para obtener ventajas, utilizan enlaces simbólicos para acelerar el cifrado, se autoeliminan para borrar evidencias y cifran cada inquilino con una contraseña única de 32 caracteres para que un mismo descifrador no pueda reutilizarse entre las víctimas.

Tabla 1.- MITRE ATT&CK - Grupo Qilin

V. IMPACTO

El grupo Qilin con esta nueva variante de Linux, centra sus ataques en Windows y entornos virtualizados.

Algunas de las herramientas y utilitarios que emplea para sus diferentes etapas son:

Para acceso remoto y ejecución de comandos

- cmd.exe

- rundll32.exe

Para descubrimiento de red o escaneo de la red y conexión:

- netscan.exe
- anydesk.exe

Para su movimiento lateral emplea:

- PuTTY SSH

Y comando y control C2

- socks64.dll

VI. INDICADORES DE COMPROMISO

Esta actualización incorpora nuevos Indicadores de Compromiso (IOCs) recientemente detectados.

Familias / Detecciones relacionadas
trojan.qilin/qilinloader
trojan.qilin/encoder
ransomware.qilin/agenda
trojan.gqgm/qilin
ransomware.qilin/kvilim
ransomware.qilin/qilinloader

Tabla 2.- Detecciones relacionadas - Grupo Qilin

Hash SHA-256 identificados por archivo
.exe
18550a8b193b52f8fdd86e9e8d66affdab001ed8feca5585065388a66ceebb5c
55d51a57aa4ae7086e9eff4a33602c03f051464996af419c6c79214fcc04be47
60bc22a15a52fe605c337fd9b53bb6c1593c5c8deff18fcc2817ac51d0d300a2
f1f3fddcea2b7d98617aae0707c5bcaf6ea354498b3e77a8810c0cce702040b9
56e1d092c07322d9dad7d85d773953573cc3294b9e428b3bbbaf935ca4d2f7e7
73b1fffd35d3a72775e0ac4c836e70efefa0930551a2f813843bdfb32df4579a
5bd26a1b8b7c11a04ab63b6cdfc35424b332747c0a8a62432bff8268bd966ec5
13fda99fae67bcb810c018c9db2913aa0426798ea818b12134da97af261f058f
0ed04a6f924b2757e64940fb909ae1e8b46eb7dcf377985074434a44c38ff64f

Hash SHA-256 identificados por archivo
1c9e06d6bdf8d307a8860e5b47f8c4ec8ebd9e37e6b519c5a72b16db8dad2ade
4b3312a6e5be6e3afbae4ee89a7a50a27e2489678b7d66824ce7a83b3592f43c
4f62e909c14af137dc07d4b990c53bb28fa7c5344966b7b18f157eb235d0d796
5edb3f2f5789eca3866b7f5cdbde8016b2552239d2cfe5ea602184ba7071aa07
f3d09afc535097b0c5523579054b381e73ca58a2568e028fac0046ce73139d54
b01dff27adffe5c43253bb33fb78b40f3bbb9853a510ee978abb821c38ffced0
55.exe
43691290ac03ebb26754203f1cc3940b32f036babb7cfab3cb14fe2128389c0c
.elf
555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4
a0625699c01bad9545d87764f267aea9e9893f3b3f7ce562e28b60e75a66a707
0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1
3b10127e65fa3e215d21e0a2e7fd32be.bin
6d38d24c7ccb303089b015622d7b9fb084048a7d0dc68e86268b33d79da603a8
download_2024-11-15_15-34-02.zip
7678896abeddec985080edf08fe0365d8af0070d79f565aa6508a9ca00cb6ab4

Tabla 3.- Hash - Grupo Qilin

VII. RECOMENDACIONES:

- Asegúrate de aplicar todos los parches disponibles en sistemas Windows/Linux, servidores, y aplicaciones vulnerables.
- Limita o bloquea el acceso remoto (RDP, SSH) desde internet. Usa VPN y autenticación multifactor (MFA).
- Aísla los entornos críticos (servidores, backups, bases de datos) del resto de la red para evitar la propagación.
- Agrega los hashes de Qilin en tus herramientas de detección. Monitoriza anomalías de comportamiento.
- Mantén copias de respaldo offline y verifica regularmente su integridad y restauración.
- Usa listas de reputación y analiza tráfico sospechoso.

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:

ECUCERT. (2025). TTP – Qilin. https://www.ecucert.gob.ec/wp-content/uploads/2025/05/AL-2025-017-TTP-Qilin.pdf

TREND MICRO (2025). Agenda Ransomware deploys Linux variant on Windows systems. https://www.trendmicro.com/en_us/research/25/j/agenda-ransomware-deploys-linux-variant-on-windows-systems.html

WELIVESECURITY (2025). Qilin Ransomware y la asesoría legal en la extorsión digital. https://www.welivesecurity.com/es/ransomware/qilin-ransomware-asesoria-legal/

SOCRADAR (2025). Dark Web Profile: Qilin / Agenda Ransomware. https://socradar.io/blog/dark-web-profile-qilin-agenda-ransomware/

DEVEL GROUP (2025). Qilin Ransomware rompe barreras: usa binarios Linux en Windows para evadir defensas. https://devel.group/blog/qilin-ransomware-rompe-barreras-usa-binarios-linux-en-windows-para-evadir-defensas/

FORTINET FORTIGUARD (2025). Threat Actor: Qilin Ransomware. https://fortiguard.fortinet.com/threat-actor/6254/qilin-ransomware

TALOS INTELLIGENCE (2025). Uncovering Qilin attack methods exposed through multiple cases. https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

THE HACKER NEWS (2025). Qilin Ransomware combines Linux payloads on Windows to evade detection. https://thehackernews.com/2025/10/qilin-ransomware-combines-linux-payload.html

INDUSTRIAL CYBER (2025). Qilin Ransomware escalates rapidly in 2025, targeting critical sectors with 700+ attacks amid RansomHub shutdown. https://industrialcyber.co/ransomware/qilin-ransomware-escalates-rapidly-in-2025-targeting-critical-sectors-with-700-attacks-amid-ransomhub-shutdown/

CYBER FLORIDA (2025). Qilin Ransomware: A double extortion campaign. https://cyberflorida.org/qilin-ransomware-a-double-extortion-campaign/

SANS INSTITUTE (2025). Evolution of Qilin RaaS. https://www.sans.org/blog/evolution-qilin-raas