Nro. Alerta:	AL-2025-017	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	8-may-2025	**Ransomware QILIN**	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de Incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

Táctica, técnica y procedimiento (TTP) de Ransomware QILIN.

Figura 1.- Vulnerabilidad QILIN - figura referencial

III. INTRODUCCIÓN

QILIN, también identificado como Agenda, es un grupo de ransomware activo en 2025 que opera bajo un modelo de Ransomware como Servicio (RaaS). Se caracteriza por emplear técnicas avanzadas como BYOVD (Bring Your Own Vulnerable Driver) para evadir herramientas EDR, y el uso de herramientas legítimas del sistema (LotL) para evitar la detección. Su enfoque combina cifrado de datos con amenazas de filtración, consolidándolo como una amenaza crítica en entornos corporativos y gubernamentales.

IV. VECTOR DE ATAQUE

Se detalla la cadena de ataque:

Etapa	Táctica (MITRE ATT&CK)	Técnica	Procedimientos
Acceso Inicial	Cuentas válidas (T1078)	Credenciales VPN comprometidas	Se usaron credenciales robadas para iniciar sesión a través de una VPN SSL.
Ejecución	Intérprete de comandos y scripts (T1059)	Ejecución remota mediante RDP y herramientas de administración	Se utilizó PsExec y WMIC para moverse lateralmente en la red.
Persistencia	Carga lateral de DLL (T1574.002)	DLL maliciosa cargada mediante upd.exe	upd.exe cargó avupdate.dll, lo que llevó a la ejecución de web.dat.
Escalada de Privilegios	Explotación de controladores vulnerables (T1068)	Ataque BYOVD con TPwSav.sys	Se usó un controlador firmado para desactivar el sistema EDR.
Evasión de Defensas	Desactivación de herramientas de seguridad (T1562.001)	Eliminación de callbacks del kernel y ejecución de EDRSandblast	Se eliminaron procesos del EDR y se deshabilitó el rastreo de eventos.
Impacto	Cifrado de datos para impacto (T1486)	Ejecución del ransomware	Se exfiltró información y se cifraron archivos críticos.

Tabla 1.- Fase de ataque - QILIN

1. **Acceso Inicial-Táctica: Cuentas válidas (T1078)**

Técnica: Uso de credenciales VPN comprometidas.
Descripción: Los atacantes obtuvieron credenciales robadas (por ejemplo, mediante Phishing o compradas en la Dark Web) y las usaron para ingresar a la red corporativa a través de una conexión VPN SSL (que normalmente se usa para el acceso remoto seguro).

2. **Ejecución- Táctica: Intérprete de comandos y scripts (T1059)**

Técnica: Ejecución remota vía RDP y herramientas de administración.
Descripción: Una vez dentro, los atacantes se movieron lateralmente dentro de la red usando herramientas legítimas de administración de sistemas como PsExec y WMIC.

3. **Persistencia- Táctica: Carga lateral de DLL (T1574.002)**

Técnica: DLL maliciosa cargada con upd.exe.
Descripción: Utilizaron una técnica conocida como "DLL sideloading", donde un archivo ejecutable legítimo (upd.exe) carga una DLL maliciosa (avupdate.dll), que a su vez ejecuta otro archivo (web.dat). Esto les permite permanecer en el sistema sin ser detectados fácilmente.

4. **Escalada de Privilegios- Táctica: Explotación de controladores vulnerables (T1068)**

Técnica: Ataque BYOVD ("Bring Your Own Vulnerable Driver") con TPwSav.sys.
Descripción: Introdujeron un controlador firmado pero vulnerable, que luego explotaron para deshabilitar las soluciones de seguridad (EDR). Esta técnica es peligrosa porque el controlador está firmado y es visto como legítimo por el sistema operativo.

5. **Evasión de Defensas- Táctica: Desactivación de herramientas de seguridad (T1562.001)**

Técnica: Eliminación de "callbacks" del kernel y ejecución de EDRSandblast.
Descripción: Mataron procesos relacionados con software de detección y desactivaron el registro de eventos, ocultando así sus movimientos. EDRSandblast es una herramienta conocida para desactivar soluciones EDR (Endpoint Detection and Response).

6. **Impacto-Táctica: Cifrado de datos (T1486)**

Técnica: Ejecución del ransomware.
Descripción: En esta etapa final, el ransomware se ejecuta para exfiltrar información y cifrar archivos críticos, dejando a la organización inoperante y presionándola para pagar el rescate.

V. INDICADORES DE COMPROMISO

Los indicadores de compromiso (IoC) vinculados al ataque QILIN incluyen los siguientes hashes de archivos:

MD5	SHA-1	SHA-256
64ca549e78ad1bd3a4bd2834b0f81080	493ff413528f752c5fce3ceabd89d2ab37397b86	93c16c11ffca4ede29338eac53ca9f7c4fbcf68b8ea85ea5ae91a9e00dc77f01
eb6fff4ee0f03ae5191f11570ff221c5	c2dfbf554e068195ecc40bebd0617ce09ad65784	54ff98956c3a0a3bc03a5f43d2c801ebcc1255bed644c78bad55d7f7beebd294
923c5af6fd29158b757fb876979d250b	6b3e3ff0495d39c85eca41f336bfd5ff92c97412	9e1f8165ca3265ef0ff2d479370518a5f3f4467cd31a7b4b006011621a2dd752
31edb01d243e8d989eb7e5aeeeef54dc	05f60fc706754b317ffc7839a2b0490f7cd6f71d	e4882b8e8e414e983cf003a5c4038043002a004b63c4f0844a15268332597e80
a7ab0969bf6641cd0c7228ae95f6d217	002971b6d178698bf7930b5b89c201750d80a07e	117fc30c25b1f28cd923b530ab9f91a0a818925b0b89b8bc9a7f820a9e630464
417ad60624345ef85e648038e18902ab	e18e6f975ef8fce97790fb8ae583caad1ec7d5b3	555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4
e01776ec67b9f1ae780c3e24ecc4bf06	3ef805009f8694e78699932563c09ac3b6bc08a5	0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1
63b89a42c39b2b56aae433712f96f619	50927809fa3f1ec408d7a1715a714831f41160db	bf9fc34ef4734520a1f65c1ec0a91b563bf002ac63982cbd2df10791493e9147
d0a711e4a51891ddf00f704d508b1ef2	d9ea05933353d1f32b18696877a3396140022f03	cd27a31e618fe93df37603e5ece3352a91f27671ee73bdc8ce9ad793cad72a0f

MD5	SHA-1	SHA-256
14dec91fdcaab96f513 82a43adb84016	a85d9d2a3913011cd282ab c7d9711b2346c23899	37546b811e369547c8bd631fa4399730d3bd aff635e744d83632b74f44f56cf6
88bb86494cb9411a96 92f9c8e67ed32c	82f8060575de96dc4edc4f7 b02ec31ba7637fa03	c26ce932f3609ecd710a3a1ca7f7b96f1b103a 11b49a86e9423e03664eaabd40
470d0261d18ed69990 ce94f05d940de1	890581fca724935118606a4 d92dbc206f9eff04c	411b2ed12df1ace6559d3ea666c672617ce2 3e2ace06806bb53c55bcccb83303
d67303ba66bcb4dd89 de87c83f3f831f	34bfe0c8aa61f90ca03b7e8 0271d5a8afae0be4b	8e1eb0ad22236e325387fdb45aea63f318a67 2c5d035a21d7b3a64eeafb4c5a2
440810b008eed766f0 85b69b1723f54b	9692644974071cd484455e 355f8d79ce8c486e20	aa0772fc6784799d59649654879c2b4a2391 9cda410bede0162751e6d6d6b558
6b7eeb860917aa4498 2d8bd2d971aff1	d4e3a066e1c1a21e3d44f2e f81a94aec42f5df11	ebb2a1b46a13c308ffe62dda4d9da316d5504 33707b2c2a38ad710ea4456c608
a42d36f1af2c396e645 ffa356fa47a1e	5914e976598ece1a271a60 615a17420319a77812	ceed9fdce420c0558e56bb705664d59f67d62 c12d7356ca8643908261638b256

Tabla 2.- (IoC) vinculados - QILIN

NOMBRE DE ARCHIVO
decryptor_399060b2.exe
enc.exe
8e1eb0ad22236e325387fdb45aea63f318a672c5d035a21d7b3a64eeafb4c5a2
555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4.elf
99.dll
update.exe
inter.exe
ceed9fdce420c0558e56bb705664d59f67d62c12d7356ca864390826
e1d41939dc4cc4116cc3439a01cfb666
BackupsFrst.exe1
2023-12-15_63b89a42c39b2b56aae433712f96f619_revil
update.exe
31edb01d243e8d989eb7e5aeeeef54dc.virus
2023-11-14_d0a711e4a51891ddf00f704d508b1ef2_revil
0629cd5e187174cb69f3489675f8c84cc0236f11f200be384ed6c1a9aa1ce7a1.elf
c26ce932f3609ecd710a3a1ca7f7b96f1b103a11b49a86e9423e03664eaabd40.dll

Tabla 3.- (IoC) vinculados - QILIN

DOMINIO
account[.]microsoftonline[.]com[.]ec
cloud[.]iscreenconnect[.]com
cloud[.]screenconect[.]com[.]mx
cloud[.]screenconect[.]eu
cloud[.]screenconnect[.]app
cloud[.]screenconnect[.]cl
cloud[.]screenconnect[.]co[.]com
cloud[.]screenconnect[.]co[.]za
cloud[.]screenconnect[.]com[.]am
cloud[.]screenconnect[.]com[.]bo

DOMINIO
cloud[.]screenconnect[.]com[.]cm
cloud[.]screenconnect[.]com[.]ly
cloud[.]screenconnect[.]com[.]ms
cloud[.]screenconnect[.]com[.]ng
cloud[.]screenconnect[.]com[.]ph
cloud[.]screenconnect[.]com[.]se
cloud[.]screenconnect[.]com[.]so
cloud[.]screenconnect[.]com[.]vc
cloud[.]screenconnect[.]de[.]com
cloud[.]screenconnect[.]gr[.]com
cloud[.]screenconnect[.]is
cloud[.]screenconnect[.]jpn[.]com
cloud[.]screenconnect[.]uk[.]com
cloud[.]screenconnect[.]us[.]com

Tabla 4.- (IoC) vinculados - QILIN

FILE	SHA-256
TPwSav.sys	011df46e94218cbb2f0b8da13ab3cec397246fdc63436e58b1bf597550a647f6
avupdate.dll	d3af11d6bb6382717bf7b6a3aceada24f42f49a9489811a66505e03dd76fd1af
main.exe	aeddd8240c09777a84bb24b5be98e9f5465dc7638bec41fb67bbc209c3960ae1
web.dat	08224e4c619c7bbae1852d3a2d8dc1b7eb90d65bba9b73500ef7118af98e7e05
upd.exe	3dfae7b23f6d1fe6e37a19de0e3b1f39249d146a1d21102dcc37861d337a0633

Tabla 5.- (IOC) vinculados - QILIN

IP
216.120.203[.]26
31.192.107[.]144

Tabla 6.- (IoC) vinculados - QILIN

SERVIDOR FTP
ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS@85.209.11.49
ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@188.119.66.189

Tabla 7.- (IoC) vinculados - QILIN

DARK WEB / C2 URL
http://ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd.onion/
http://24kckepr3tdbcomkimbov5nqv2alos6vmrmlxdr76lfmkgegukubctyd.onion
http://wlh3dpptx2gt7nsxcor37a3kiyaiy6qwhdv7o6nl6iuniu5ycze5ydid.onion/blog
http://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad.onion/
http://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd.onion
https://31.41.244.100/
http://ijzn3sicrcy7quixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvad.onion
http://kbsqoiyihadmwczmxkbovk7ss2dcynitwhhfu5yw725dbogo5kthfaad.onion

Tabla 8.- (IoC) vinculados – QILIN

VI. RECOMENDACIONES:

- Utilizar herramientas de detección y respuesta en endpoints que identifiquen comportamientos anómalos, como la ejecución no autorizada de scripts o la eliminación de registros de eventos.
- Establecer sistemas de monitoreo que detecten la eliminación o modificación de registros de eventos, una táctica común de QILIN para evadir la detección.
- Vigilar conexiones salientes inusuales o a direcciones IP sospechosas que puedan indicar comunicación con servidores de comando y control.
- Aplicar autenticación multifactor (MFA) en todos los accesos, especialmente en cuentas privilegiadas y accesos remotos, para prevenir el uso de credenciales comprometidas.
- Asegurar que los usuarios y servicios solo tengan los permisos estrictamente necesarios para sus funciones.
- Implementar soluciones que controlen y monitoreen el uso de cuentas con altos privilegios, reduciendo el riesgo de escalamiento de privilegios por parte de atacantes.
- Realizar respaldos regulares que no puedan ser alterados o eliminados por ransomware, almacenándolos en ubicaciones desconectadas de la red principal.
- Educar a los empleados sobre las tácticas de ingeniería social y phishing utilizadas por grupos como QILIN para obtener acceso inicial.
- Dividir la red en segmentos para limitar el movimiento lateral de los atacantes en caso de una brecha de seguridad.
- Implementar un proceso continuo de identificación y remediación de vulnerabilidades en sistemas y aplicaciones.
- Implementar en la organización o instituciones planes de contingencia, planes de continuidad del negocio y planes de recuperación y copias de seguridad.

VII. 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.

VIII. REFERENCIAS:

EcuCERT (2025). Alertas de Seguridad: Funcionamiento interno del ransomware Qilin. https://www.ecucert.gob.ec/wp-content/uploads/2022/02/AL-2024-16-Ramsonware-Qilin.pdf

Red Piranha (2025). Qilin Ransomware: All you need to know. https://redpiranha.net/news/qilin-ransomware-all-you-need-know

MyCERT (2025). MA-1300.032025: MyCERT Advisory – Qilin Ransomware. https://www.mycert.org.my/portal/advisory?id=MA-1300.032025

Picus (2025). Ransomware Qilin: Descubriendo las tácticas y técnicas detrás de una de las campañas de ransomware más activas de 2024. https://www-picussecurity-com.translate.goog/resource/blog/qilin-ransomware?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

SoS Ransomware (2025). Todo lo que necesitas saber sobre el ransomware Quilin. https://sosransomware.com/es/grupos-de-ransomware/ransomware-quilin-3/