LOTE 5: Servicios de información y consultoría especializada de ciberseguridad

Informe de programas malignos recientes

10 de abril de 2026

Castilla-La Mancha

Índice de contenidos

1. Resumen ejecutivo 3
2. Introducción y contexto 4
3. Descripción técnica del malware analizado 6
   Arquitectura y capacidades multiplataforma 6
   Vectores de acceso inicial y explotación de vulnerabilidades 8
   Innovaciones técnicas del sistema 8
   Comportamiento post-explotación y extorsión 9
4. Impacto potencial y consecuencias 10
   Para empresas (PYMES y corporaciones) 10
   Para la ciudadanía 10
5. Medidas preventivas y estrategia defensiva 11
   Recomendaciones para empresas 11
   Recomendaciones para la ciudadanía 12
6. Anexos y referencias 13
   Referencias bibliográficas y fuentes. 13
      Fuentes institucionales y normativa: 13
      Informes de inteligencia de amenazas (Threat Intelligence): 13

Castilla-La Mancha

1. Resumen ejecutivo

Este documento analiza una de las amenazas de ransomware más activas y sofisticadas del primer trimestre de 2026: Qilin.

Qilin es una operación criminal que actúa bajo el modelo Ransomware-as-a-Service (RaaS), especializada en ataques de alto impacto contra infraestructuras empresariales complejas y sectores críticos.

Desde mediados de 2025, Qilin ha mostrado una aceleración significativa en sus capacidades técnicas, destacando por su orientación multiplataforma, su capacidad para atacar entornos virtualizados y su uso intensivo de técnicas de evasión avanzadas. Su actividad se ha concentrado especialmente en organizaciones con alta dependencia de sistemas ERP, hipervisores y servicios gestionados.

El ransomware Qilin debe considerarse una amenaza estratégica, no limitada al ámbito tecnológico, sino con implicaciones directas en la continuidad del negocio, el cumplimiento normativo y la estabilidad operativa de organizaciones públicas y privadas.

Síntesis de la amenaza: Qilin

Qilin representa una evolución madura del ransomware industrializado.

No se trata únicamente de un software de cifrado, sino de una plataforma criminal completa, diseñada para maximizar el impacto económico, operacional y reputacional de la organización víctima. Entre los elementos que definen la amenaza destacan:

- **Capacidad multiplataforma real**, con binarios específicos para Windows, Linux y ESXi.
- **Ataque directo a infraestructuras de virtualización**, afectando simultáneamente a decenas de servicios corporativos.
- **Uso intensivo de técnicas Living-off-the-Land (LotL)**, reduciendo su huella y dificultando la detección.
- **Doble extorsión sistemática**, con exfiltración previa de información sensible.
- **Elevado reparto de beneficios a afiliados**, lo que incentiva campañas especialmente agresivas.

El objetivo principal de Qilin no es únicamente el cifrado de archivos, sino forzar una situación de colapso operativo que limite las opciones de respuesta del afectado y aumente la probabilidad de pago.

Nivel de criticidad y sectores de mayor riesgo (PYMEs y corporaciones)

Criticidad:

La capacidad de Qilin para inutilizar entornos virtualizados completos y sistemas ERP centrales eleva el riesgo de parálisis operativa total.

A diferencia de otros ransomware, Qilin no distingue entre tamaños de organización: tanto PYMEs con servicios externalizados como grandes corporaciones con infraestructuras propias pueden verse gravemente afectadas si existe dependencia de terceros, virtualización o accesos remotos mal protegidos.

Sectores objetivo

- **Manufactura e industria**, donde cada minuto de parada supone pérdidas económicas directas elevadas.
- **Sanidad y sector salud**, debido a la criticidad de los sistemas y a la presión por mantener la continuidad asistencial.
- **Administración pública y servicios al ciudadano**, por la sensibilidad de los datos gestionados y el impacto social de las interrupciones.
- **Sector financiero y asegurador**, tanto por su capacidad de pago como por el riesgo regulatorio asociado a la exposición de datos.

Medidas correctivas (Empresas y ciudadanía)

Para empresas y PYMEs (Enfocado a continuidad)

Las medidas deben orientarse no solo a la prevención, sino también a la resiliencia y capacidad de recuperación:

- Refuerzo de infraestructuras críticas (virtualización, ERP, accesos remotos).
- Priorización del parcheo de servicios perimetrales y soluciones ampliamente explotadas.
- Endurecimiento de la autenticación y control de accesos privilegiados.
- Aseguramiento de copias de seguridad resilientes frente al cifrado.

Para la ciudadanía (Enfocado a prevención)

Aunque el ciudadano no suele ser el objetivo directo, puede convertirse en **vector indirecto** o víctima colateral:

- Protección de credenciales personales reutilizadas en entornos laborales.
- Uso de autenticación multifactor en servicios clave.
- Desconfianza ante comunicaciones urgentes o no solicitadas.

2. Introducción y contexto

Durante el primer trimestre de 2026, se ha observado una aceleración significativa en la actividad de los grupos de ransomware que operan bajo modelos RaaS (Ransomware-as-a-Service) en el ecosistema global de ciberamenazas. En este contexto, Qilin se consolida como uno de los actores con mayor capacidad disruptiva debido a su elevado nivel de sofisticación técnica, su rápida

adaptación a entornos emergentes y su orientación agresiva hacia sectores críticos. Esta tendencia forma parte de un escenario más amplio caracterizado por la profesionalización del cibercrimen, la explotación de vulnerabilidades de alto impacto y el uso creciente de tácticas avanzadas de ingeniería social.

Alcance y propósito del informe

El presente informe detalla el alcance del análisis realizado, el cual se basa en inteligencia de amenazas de acceso abierto, informes gubernamentales, observaciones técnicas del primer trimestre de 2026 y tendencias derivadas de incidentes recientes en diversos sectores. Este contexto facilita la comprensión de la naturaleza real del riesgo asociado a Qilin y sirve como marco de referencia para interpretar las secciones posteriores del informe, donde se profundiza en el impacto operativo, la exposición de la ciudadanía y las medidas preventivas recomendadas.

Diferenciando dos niveles de impacto:

- **Empresas y PYMEs**: análisis técnico y recomendaciones orientadas a la resiliencia operativa.
- **Ciudadanía**: concienciación sobre el impacto indirecto y los riesgos derivados de brechas en servicios esenciales.

El análisis se alinea con las directrices de INCIBE, CCN-CERT y los marcos europeos de gestión del riesgo TIC.

Contexto: panorama del ciberdelito (Q1 2026)

El presente informe examina la evolución reciente de Qilin, contextualizando su actividad dentro del panorama europeo y global de amenazas y destacando los elementos que justifican su creciente relevancia. Se analizan los vectores de acceso empleados por sus afiliados, las innovaciones técnicas identificadas en las últimas variantes y las implicaciones operativas que estas introducen en entornos corporativos modernos, en particular en infraestructuras hiperconvergentes, servicios perimetrales y sistemas ERP ampliamente implantados.

Durante el primer trimestre de 2026 se ha consolidado un escenario caracterizado por:

- Incremento de ataques dirigidos a entornos virtualizados.
- Uso sistemático de vulnerabilidades críticas en servicios corporativos.
- Crecimiento de modelos RaaS altamente especializados.

Qilin se posiciona como uno de los grupos que capitaliza esta tendencia, ofreciendo a sus afiliados una plataforma preparada para comprometer infraestructuras híbridas complejas.

3. Descripción técnica del malware analizado

Qilin es una sofisticada operación de cibercrimen que funciona bajo el modelo de Ransomware-as-a-Service (RaaS). Surgido a mediados de 2022 y originalmente desarrollado en el lenguaje Go, el malware ha experimentado una profunda evolución técnica, transformándose en una de las herramientas de intrusión y secuestro de datos más avanzadas y difíciles de detectar del mercado negro actual.

Evolución de Qilin

La evolución de Qilin refleja una tendencia clara hacia la industrialización del ransomware y la adaptación a entornos corporativos modernos:

Fase inicial (2022–2023):

Las primeras variantes de Qilin, desarrolladas en Go, mostraban funcionalidades de cifrado relativamente convencionales y estaban orientadas principalmente a entornos Windows. El impacto de estas campañas era elevado, pero todavía limitado a infraestructuras poco segmentadas.

Fase de maduración (2024):

Se observa una ampliación progresiva hacia entornos Linux y servidores, junto con la adopción sistemática de técnicas de doble extorsión. En esta etapa, Qilin comienza a priorizar víctimas con mayor dependencia tecnológica y procesos críticos.

Fase avanzada (2025–2026):

Qilin se reescribe parcialmente en Rust, mejorando rendimiento, estabilidad y evasión. Se incorporan binarios específicos para VMware ESXi, soporte multiplataforma real y técnicas avanzadas de ocultación (Living-off-the-Land, WSL). El foco se desplaza claramente hacia infraestructuras virtualizadas, ERP y servicios centrales, elevando el impacto operativo de manera exponencial.

Esta evolución no es casual: responde a una estrategia deliberada para maximizar la presión sobre la víctima y reducir sus opciones de recuperación sin pago.

Arquitectura y capacidades multiplataforma

La actual variante de Qilin ha abandonado sus raíces en Go para ser reescrita en Rust, un lenguaje de programación que otorga a los atacantes una enorme ventaja en términos de eficiencia de procesamiento, evasión de análisis estático y capacidades cruzadas.

- **Ataque a la hiperconvergencia:** Qilin cuenta con ejecutables diseñados específicamente para entornos Windows y binarios en formato ELF orientados a sistemas Linux y, de manera crítica, hipervisores VMware ESXi. Esto permite a los afiliados destruir infraestructuras virtualizadas completas, maximizando el impacto operativo.

- **Cifrado intermitente y criptografía:** Para asegurar la máxima velocidad y evadir detecciones basadas en el volumen de lectura/escritura en disco, Qilin emplea parámetros de "cifrado intermitente" (cifrando solo bloques específicos de grandes archivos). Utiliza una combinación de cifrado de flujo rápido (AES-256-CTR o ChaCha20) junto con cifrado asimétrico robusto (RSA-4096 OAEP) para proteger las claves.

Funcionamiento de Qilin

Qilin ejecuta sus ataques siguiendo una cadena operativa estructurada, diseñada para mantener el control de la situación desde el acceso inicial hasta la negociación final del rescate.

1. Acceso inicial

El acceso inicial suele lograrse mediante:

- Explotación de vulnerabilidades críticas en servicios corporativos expuestos (portales, VPN, firewalls, ERP).
- Uso de credenciales comprometidas obtenidas por phishing, filtraciones previas o compra en mercados ilícitos.
- Abuso de configuraciones inseguras en accesos remotos (VPN, RDP, herramientas de gestión).

El objetivo de esta fase es establecer una presencia persistente en la red sin generar alertas tempranas.

2. Reconocimiento y movimiento lateral

Una vez dentro, Qilin realiza un reconocimiento exhaustivo del entorno, identificando:

- Controladores de dominio.
- Servidores de virtualización.
- Sistemas ERP, bases de datos y almacenamiento centralizado.
- Soluciones de backup y monitorización.

Para el movimiento lateral se prioriza el uso de herramientas legítimas (PowerShell, PsExec, AnyDesk, WinRM), lo que dificulta la detección basada en firmas y minimiza la huella del ataque.

3. Exfiltración de información

Antes de proceder al cifrado, Qilin ejecuta una exfiltración sistemática de datos sensibles. Esta información se utiliza posteriormente como elemento clave en la doble extorsión, incrementando la presión económica y reputacional.

4. Cifrado coordinado

El cifrado se ejecuta de forma coordinada y selectiva, priorizando:

- Sistemas centrales.
- Servidores virtualizados.
- Volúmenes compartidos de alto impacto.

El uso de cifrado intermitente permite acelerar el proceso y reducir la probabilidad de detección temprana por parte de soluciones de seguridad.

5. Extorsión y negociación

Tras el cifrado, los operadores de Qilin establecen canales de negociación, habitualmente a través de portales en la dark web. La amenaza de publicación de la información robada actúa como palanca adicional para forzar el pago, incluso en organizaciones con capacidad técnica de recuperación.

Vectores de acceso inicial y explotación de vulnerabilidades

Los afiliados de Qilin son notablemente versátiles en sus métodos de acceso inicial, combinando ingeniería social avanzada con la explotación de vulnerabilidades críticas de "día cero" en el perímetro corporativo.

- **Asalto a sistemas ERP (SAP NetWeaver):** Una de las tácticas más devastadoras observadas recientemente es la explotación de la vulnerabilidad *CVE-2025-31324 (CVSS 10.0).* Este fallo crítico, que reside en el componente Visual Composer de SAP NetWeaver, permite a atacantes no autenticados **subir archivos arbitrarios y lograr la ejecución remota** de código (RCE). Qilin aprovecha esto para instalar web shells (puertas traseras) y tomar el control directo del núcleo de la planificación de recursos empresariales.
- **Ataque a VPNs y herramientas de gestión:** El grupo también explota activamente **fallos en firewalls perimetrales** de FortiGate y en software de monitorización y gestión remota (RMM) sin parchear, como SimpleHelp, utilizándolos como puente hacia la red interna.
- **Fatiga de MFA y SIM Swapping:** En los accesos basados en credenciales, las variantes de Qilin de 2025 y 2026 han incorporado el uso de **"MFA Bombing"** (inundar al usuario con peticiones de aprobación) y **"SIM swapping" (duplicado de tarjetas SIM)** para eludir los sistemas de Autenticación Multifactor tradicionales.

Innovaciones técnicas del sistema

Qilin destaca por su maestría en el uso de herramientas legítimas para fines maliciosos, minimizando el despliegue de malware personalizado que alertaría a los sistemas de seguridad.

- **Abuso del subsistema de Windows para Linux (WSL):** En una de sus innovaciones más peligrosas, los operadores de Qilin han sido observados abusando de WSL para ejecutar sus binarios de cifrado de Linux (ELF) directamente sobre máquinas Windows host. Esta táctica **ciega efectivamente a la gran mayoría de las soluciones EDR** tradicionales de Windows, que no están diseñadas para monitorizar procesos maliciosos que se ejecutan dentro del subsistema de Linux.
- **Herramientas legítimas (LotL):** Una vez dentro de la red, los atacantes utilizan software legítimo de gestión remota como AnyDesk, ScreenConnect o Splashtop para moverse lateralmente sin levantar sospechas, así como WinSCP o Cyberduck para extraer los datos.
- **Evasión de defensas:** El malware manipula los tokens de acceso para elevar privilegios, oculta procesos mediante ventanas invisibles y borra sistemáticamente los registros del

sistema (logs) tanto en Linux como en Windows (técnicas T1134, T1564.003 y T1070.002 de MITRE ATT&CK).

Comportamiento post-explotación y extorsión

Los operadores de Qilin ofrecen a sus afiliados **hasta un 80-85% de las ganancias del rescate**, lo que incentiva campañas sumamente agresivas. A diferencia de grupos que operan con cierta ética criminal y evitan hospitales, Qilin ataca de manera implacable a infraestructuras críticas. Operan un modelo de doble extorsión en su portal de la dark web, robando la información sensible de la víctima antes de cifrar la red y amenazando con publicar los datos en caso de no recibir el pago exigido.

4. Impacto potencial y consecuencias

La evolución de Qilin hacia un modelo altamente eficiente y multiplataforma se traduce en daños tangibles y a menudo irreversibles para el tejido empresarial y la sociedad.

Para empresas (PYMES y corporaciones)

Las organizaciones -independientemente de su tamaño o madurez digital- se encuentran especialmente expuestas a las capacidades ofensivas de Qilin. Este tipo de operaciones criminales no solo compromete activos tecnológicos, sino que altera profundamente la continuidad del negocio y genera un efecto en cascada que afecta a procesos críticos, proveedores y clientes. A continuación, se detallan los principales impactos identificados sobre el tejido empresarial.

- **Impacto operativo y parálisis de negocio:** El ataque a hipervisores (ESXi) y la vulneración del ecosistema SAP NetWeaver significa que **Qilin es capaz de derribar el corazón operativo de la empresa** (finanzas, logística, bases de datos de clientes y producción) en cuestión de minutos. La recuperación desde cero en este estado de destrucción implica caídas de servicio prolongadas que pueden durar semanas.
- **Impacto económico y regulatorio:** Las demandas económicas de Qilin son exorbitantes. En un asalto destacado, el grupo exigió 50 millones de dólares de rescate. Además del coste de recuperación o lucro cesante, el robo masivo de información expone a las organizaciones a multas regulatorias severas por **incumplimiento del Esquema Nacional de Seguridad (ENS) o la Directiva NIS2**, así como a una enorme crisis reputacional.
- **Sectores en riesgo crítico:** En España y Europa, Qilin ha dirigido sus ataques prioritariamente hacia el **sector de la manufactura**. A nivel internacional, también se ha centrado ferozmente en el **sector salud y sanidad**, sumando decenas de ataques en periodos muy cortos y asfixiando proveedores de servicios críticos y hospitales.

Para la ciudadanía

El impacto de Qilin afecta principalmente al ámbito empresarial, pero también termina afectando de forma indirecta a miles de ciudadanos. Las interrupciones de servicios esenciales, la exposición de datos personales y la dependencia de cadenas de suministro digitalizadas sitúan a la población en una zona vulnerable frente a incidentes de gran escala. A continuación, se describen los efectos más relevantes para la ciudadanía.

- **Caída de servicios críticos y de salud:** Cuando Qilin ataca a proveedores de servicios hospitalarios, como ocurrió con el ataque al proveedor de patología Synnovis, los hospitales se ven forzados a cancelar operaciones quirúrgicas, reprogramar citas urgentes y retrasar diagnósticos vitales, poniendo en riesgo la integridad física de los pacientes.
- **Efecto dominó en cadenas de suministro:** El compromiso de proveedores externos, empresas de software y hubs logísticos (como operadores de aeropuertos) causa disrupciones

en servicios públicos esenciales, generando retrasos masivos en viajes, envíos y trámites administrativos.

- **Exposición de datos personales:** La doble extorsión lleva a que el historial médico, los datos censales y la información financiera de miles de ciudadanos terminen subastados en foros del mercado negro, exponiendo al individuo a futuras campañas de fraude de identidad o phishing hiper-personalizado entre otros.

5. Medidas preventivas y estrategia defensiva

Contener una amenaza de la sofisticación de Qilin requiere abandonar el enfoque reactivo tradicional. Es fundamental adoptar modelos de arquitectura Zero Trust (Confianza Cero) y establecer una defensa en profundidad que abarque la tecnología, los procesos y el factor humano.

Recomendaciones para empresas

Dada la naturaleza avanzada y la agresividad operativa demostrada por Qilin, resulta imprescindible que las organizaciones adopten un enfoque proactivo respecto a la ciberseguridad. Las siguientes recomendaciones sintetizan las medidas prioritarias que, desde una perspectiva defensiva, permiten mitigar significativamente el riesgo de compromiso y mejorar la resiliencia frente a ataques de este tipo.

- **Gestión ágil de vulnerabilidades y parcheo:** Resulta vital reducir la superficie de exposición. Se debe aplicar parcheo inmediato en servicios perimetrales, prestando especial atención a la actualización de los sistemas SAP NetWeaver para mitigar la vulnerabilidad *CVE-2025-31324*. De igual forma, las VPN corporativas y dispositivos FortiGate deben estar actualizados a sus últimas versiones de firmware.
- **Afinamiento de EDR contra técnicas LotL y WSL:** Los equipos de seguridad (SOC) deben ajustar las plataformas EDR/XDR para detectar el comportamiento anómalo de utilidades legítimas. Es prioritario implementar alertas sobre la instalación o el uso inusual del Subsistema de Windows para Linux (WSL), así como restringir la ejecución de binarios ELF dentro de estos entornos si no responden a una necesidad de negocio documentada.
- **Autenticación Multifactor (MFA) robusta:** Debido a las tácticas avanzadas de evasión de Qilin, las empresas deben transitar hacia sistemas MFA resistentes al phishing y a la "fatiga de MFA" (MFA Bombing). Se recomienda el **uso de tokens físicos** basados en el estándar FIDO2, limitando la dependencia de la autenticación por SMS, vulnerable al SIM swapping. En el caso del MFA Bombing la **formación efectiva de los empleados** en esta área puede ayudar a reducir enormemente el riesgo humano.
- **Blindaje de la virtualización (ESXi):** Las consolas de administración (vCenter y clientes de host ESXi) deben ser segmentadas en redes fuera de banda (OOB) independientes de la red general, y el acceso por SSH debe deshabilitarse por defecto.

- **Copias de seguridad inmutables (Regla 3-2-1-1):** Mantener al menos 3 copias de los datos, en 2 soportes distintos, con 1 copia externa (offsite) y, de manera crítica, asegurar que al menos 1 copia mantenga inmutabilidad a nivel de almacenamiento (Object Lock / WORM) o permanezca físicamente desconectada (offline) de la red corporativa.

Recomendaciones para la ciudadanía

Si bien Qilin orienta sus campañas principalmente contra organizaciones, la ciudadanía representa un componente clave en la superficie de exposición global. El comportamiento individual impacta directamente en la seguridad de empresas, administraciones y servicios esenciales. Por ello, se recogen a continuación una serie de prácticas fundamentales que pueden aplicarse para minimizar la vulnerabilidad y contribuir a un entorno digital más seguro.

- **Prudencia y escepticismo digital:** Aunque el ciudadano no constituye el objetivo principal del ransomware Qilin, los dispositivos o credenciales particulares pueden llegar a ser el punto de entrada a una organización. Es recomendable desconfiar por defecto de correos electrónicos no solicitados, enlaces a facturas urgentes o descargas de software desde sitios web no oficiales.
- **Protección de la identidad:** Se aconseja habilitar el **segundo factor de autenticación (2FA/MFA)** mediante aplicaciones como Google Authenticator o Microsoft Authenticator en todas las cuentas personales de correo electrónico y servicios bancarios. **Evitar la reutilización de contraseñas** resulta esencial, dado que las credenciales expuestas en brechas previas se emplean rutinariamente para ataques iniciales.
- **Notificación de brechas:** Es conveniente mantenerse atento a alertas de instituciones y empresas sobre incidentes de seguridad que puedan afectar a los datos personales. Resulta recomendable monitorizar cuentas y contraseñas a través de webs como Have I been pwned y modificar las credenciales si fuera necesario.

6. Anexos y referencias

Referencias bibliográficas y fuentes.

La información detallada y analizada en este reporte ha sido procesada mediante la síntesis y revisión técnica de inteligencia de acceso abierto y reportes gubernamentales emitidos por la comunidad de inteligencia de amenazas (CTI) durante el primer trimestre de 2026.

Fuentes institucionales y normativa:

[1] España Digital / INCIBE. (2025). *INCIBE gestionó 122.223 incidentes de ciberseguridad en 2025, un 26% más que el año anterior*. https://espanadigital.gob.es/ca/actualidad/incibe-gestiono-122223-incidentes-de-ciberseguridad-en-2025-un-26-mas-que-el-ano

[2] Ciberseguridad TIC. (2026, febrero 10). *La actividad del CERT de INCIBE crece un 26% en un año marcado por el fraude digital*. https://ciberseguridadtic.es/mercado/la-actividad-del-cert-de-incibe-crece-un-26-en-un-ano-marcado-por-el-fraude-digital-2026021011730.htm

[3] European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/topics/threats-and-trends/threat-landscape

Informes de inteligencia de amenazas (Threat Intelligence):

[4] Cyfirma. (2026, marzo 13). *Weekly Intelligence Report – 13 March 2026*. https://www.cyfirma.com/news/weekly-intelligence-report-13-march-2026/

[5] Areté. (2026, enero). *Ransomware trends: Data & insights – January 2026*. https://areteir.com/resources/ransomware-trends-data-insights-january-2026

[6] GuidePoint Security. (2026). *Ransomware trends by industry: 2026 ransomware cyber threat report*. https://www.guidepointsecurity.com/blog/ransomware-trends-by-industry-2026-ransomware-cyber-threat-report/

[7] SentinelOne. (2026). *Cybersecurity statistics*. https://www.sentinelone.com/es/cybersecurity-101/cybersecurity/cyber-security-statistics/

[8] Red Seguridad. (2026, febrero 17). *La industria en España centra el foco de los ciberataques con tres incidentes graves al día*. https://www.redseguridad.com/actualidad/cibercrimen/la-industria-en-espana-centra-el-foco-de-los-ciberataques-con-tres-incidentes-graves-al-diala-industria-espanola-centra-el-foco-de-los-ciberataques-con-tres-incidentes-graves-al-dia_20260217.html