I. DATOS GENERALES:

Clase de alerta: Ransomware
Tipo de Incidente: Compromiso de sistemas mediante evasión de EDR y cifrado de información
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Ransomware Qilin - Figura referencial

El grupo de Ransomware Qilin ha implementado una nueva cadena de infección multi etapa capaz de deshabilitar más de 300 Endpoint Detection and Response (EDR) correspondiente a los principales proveedores de seguridad, conocida como EDR Killer, el intercambio de este malware, como si, se tratase de uno open source entre actores de amenaza representa un auge en la coordinación y efectividad del cibercrimen.

III. INTRODUCCIÓN

Las herramientas de detección y respuesta de endpoints (EDR) son soluciones de ciberseguridad avanzada que monitorean continuamente los dispositivos finales (móviles, laptops, servidores) para detectar, investigar y bloquear amenazas.

Entre sus beneficios permite el monitoreo para registrar actividades sospechosas, procesos y conexiones de red. Análisis de comportamiento basado en IA y aprendizaje automático para identificar anomalías como las de ransomware. Respuestas automáticas para aislar equipos infectados dentro de una red y bloqueo de IPs maliciosas. Análisis forense, para la recopilación y almacenamiento de datos con fin de investigar las causas raíz de un incidente.

Este malware crea un archivo DLL malicioso que ejecuta un payload en la memoria y evita los hooks de los EDR. Empleando técnicas avanzadas de ofuscación basada en SEH (Structured Exception Handling) /VEH (Vectored Exception Handling), evasión de llamadas al sistema (syscall bypass), manipulación de objetos del kernel y IAT hooking todo esto sin activar alertas en el sistema, con el único objetivo principal de desactivar los EDR.

IV. VECTOR DE ATAQUE

Lo investigadores de CISCO TALOS han encontrado que los ataques del grupo de Ransomware Qilin está usando este malware como una sofisticada cadena de infección.

La fase inicial consiste en cargar PE Loader (componente del Windows OS que se encarga de cargar archivos ejecutables .exe, .dll, .sys) encargado de preparar el entorno de ejecución del EDR killer.

El ataque comienza empleando la técnica DLL side-loading, es decir engañando una aplicación legítima, como FoxitPDFReader.exe, para descarga una DLL maliciosa de nombre msimg32.dll, en lugar de la biblioteca de Windows genuina (DllMain). Embebido en la DLL maliciosa esta encriptado el payload del EDR KILLER.

El cargador DLL implementa una serie de técnicas para evadir la detección. Neutraliza los hooks en modo usuario, suprime los registros de eventos de Event Tracing for Windows (ETW) y toma medidas para ocultar el flujo de control y los patrones de invocación de la API. Como resultado, permite que el payload principal del EDR killer se descifre, se cargue y se ejecute íntegramente en memoria sin que se detecte en absoluto.

Una vez ejecutado, el malware carga dos controladores a nivel del kernel para desmantelar las herramientas de seguridad de adentro hacia afuera.

rwdrv.sys, una versión renombrada de ThrottleStop.sys, este controlador expone: Una funcionalidad muy potente y puede ser cargado por aplicaciones arbitrarias de modo usuario. Críticamente, implementa estas capacidades sin hacer cumplir controles de seguridad significativos, lo que lo hace particularmente atractivo para el abuso.

Una interfaz de acceso de hardware de bajo nivel al modo de usuario a través de controles de entrada / salida (IOCTL) que permite que una aplicación en modo de usuario interactúe directamente con el hardware del sistema., tales como:

- Acceso al puerto de E/S
- Acceso al Registro Específico del Modelo de CPU (MSR)
- Memoria física/acceso a MMIO
- Acceso directo a la memoria física
- Acceso al espacio de configuración PCI

El controlador rastrea el número de manejadores abiertos y asocia las asignaciones de memoria con el ID de proceso de llamada.

En general, este controlador funciona como una capa de acceso de hardware de modo kernel genérico, exponiendo primitivas para las operaciones de E/S del puerto, acceso MSR, mapeo de memoria física y configuración de PCI. Dicha funcionalidad se utiliza típicamente por herramientas de diagnóstico de hardware, utilidades de firmware o utilidades de sistema de bajo nivel, pero también proporciona poderosas primitivas que podrían ser abusadas si son accesibles desde el modo de usuario sin privilegios.

hlpdrv.sys, utilizado exclusivamente para terminar los procesos asociados a más de 300 controladores EDR diferentes, protegidos a través del código IOCTL 0x2222008, evitando los mecanismos de protección de procesos de Windows.

Finalmente deshabilita temporalmente la aplicación de la integridad del código de Windows para modificar el sistema sin alertas. Tras neutralizar las defensas, restaura las protecciones para ocultar rastros y ejecutar el Ransomware Qilin. Esto refleja una evolución en los ataques, donde ya no solo se evaden defensas, sino que se desmantelan antes de desplegar la carga maliciosa.

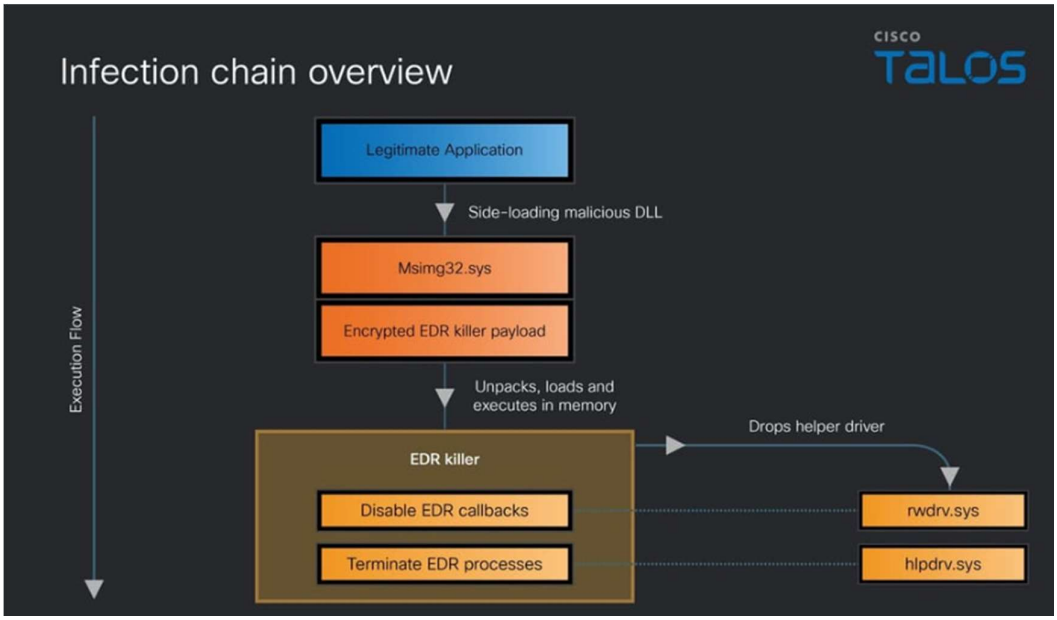

Figura 2. **-** Visión general de la cadena de infección – Ransomware Qilin

V. IMPACTO

Componentes	Descripción
Windows OS	Sistema afectado donde el malware ejecuta técnicas avanzadas de evasión
rwdrv.sys	Driver legítimo abusado para acceso a memoria y evasión de seguridad
hlpdrv.sys	Driver utilizado para manipulación del sistema y desactivación de defensas
Soluciones EDR	Más de 300 controladores de EDR pueden ser deshabilitados por el malware

Tabla 1.- Componentes afectados - Ransomware Qilin

VI. INDICADORES DE COMPROMISO

Tipo de Hash	Valor	Detección
MD5	89ee7235906f7d12737679860264feaf	Win[.]Malware[.]Bumblebee-10056548-0
SHA1	01d00d3dd8bc8fd92dae9e04d0f076cb3158dc9c	Win[.]Tool[.]EdrKiller-10059833-0
SHA256	7787da25451f5538766240f4a8a2846d0a589c59391e15f188aa077e8b888497	Win[.]Tool[.]ThrottleStop-10059849-0

Tabla 2.- Archivo: msimg32[.]dll - Ransomware Qilin

Tipo de Hash	Valor
MD5	6bc8e3505d9f51368ddf323acb6abc49
SHA1	82ed942a52cdcf120a8919730e00ba37619661a3
SHA256	16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eeedb777a3ffefa99c97f0

Tabla 3.- Archivo: rwdrv[.]sys - Ransomware Qilin

Tipo de Hash	Valor
MD5	cf7cad39407d8cd93135be42b6bd258f
SHA1	ce1b9909cef820e5281618a7a0099a27a70643dc
SHA256	bd1f381e5a3db22e88776b7873d4d2835e9a1ec620571d2b1da0c58f81c84a56

Tabla 4.- Archivo: hlpdrv[.]sys - Ransomware Qilin

Campo	Valor
MD5	1305e8b0f9c459d5ed85e7e474fbebb1
SHA1	84e2d2084fe08262c2c378a377963a1482b35ac5
SHA256	12fcde06ddadf1b48a61b12596e6286316fd33e850687fe4153dfd9383f0a4a0
Time Stamp	14 de junio de 2025, 08:33:52 UTC
ImpHash	05aa031a007e2f51e3f48ae2ed1e1fcb

Tabla 5.- Archivo: EDRKiller[.]exe (non-fixed memory dump with overlay) - Ransomware Qilin

VII. RECOMENDACIONES:

- Fortalecer la protección de endpoints mediante soluciones EDR/XDR con capacidades de protección contra manipulación (tamper protection).
- Aplicar el principio de mínimo privilegio y restringir el uso de cuentas administrativas.
- Implementar autenticación multifactor (MFA) en accesos críticos.
- Restringir la ejecución de binarios no autorizados mediante listas blancas (application whitelisting).
- Monitorear eventos relacionados con la desactivación de soluciones de seguridad y ejecución de herramientas sospechosas.
- Mantener actualizados los sistemas operativos y aplicaciones con los últimos parches de seguridad.
- Implementar segmentación de red para limitar el movimiento lateral.
- Mantener copias de seguridad offline o inmutables y verificar su restauración periódicamente.
- Fortalecer la capacitación del personal en ciberseguridad y prevención de ataques.

- Contar con un plan de respuesta a incidentes actualizado e incluir el aislamiento inmediato de sistemas comprometidos.
- Vigilar cualquier actividad sospechosa de carga lateral de archivos DLL
- Instalaciones inesperadas de controladores (rwdrv.sys, hlpdrv.sys) y cualquier intento de escribir en la memoria física desde procesos en modo usuario.
- Confiar en un único producto de seguridad ya no es suficiente frente a adversarios diseñados específicamente para neutralizarlo.

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:

CISCO TALOS (2026). *Qilin EDR killer infection chain*. https://blog.talosintelligence.com/qilin-edr-killer/

EcuCERT (2025). *Alerta de Seguridad: Qilin Ransomware*. https://www.ecucert.gob.ec/wp-content/uploads/2025/12/Al-2025-064-Qilin.pdf

CYBER PRESS (2026). *Qilin Ransomware Analysis*. https://cyberpress.org/qilin-ransomware-4/

THE HACKER NEWS (2026). *Qilin and Warlock ransomware use vulnerable drivers to disable 300+ EDR tools*. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html

CYBERSECURITY NEWS (2026). *Qilin ransomware uses EDR killer to disable security tools*. https://cybersecuritynews.com/qilin-ransomware-kill-edr/