MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Executive Threat Brief
April 2026

Prominent Qilin Ransomware Leveraging Tool to Disable Endpoint Security Products

Critical Intelligence for Decision Makers

Executive Summary

Last week, Cisco Talos released a report advising Qilin ransomware operators have deployed a new tool designed to disable endpoint detection and response (EDR) security products prior to network encryption. The tool leverages a sophisticated, two-phase attack sequence that Cisco Talos assessed can neutralize over 300 EDR products across major security vendors.[1] The tool's first stage evades detection by executing entirely in memory. The second stage loads a vulnerable signed driver to gain privileged access to the operating system kernel and forcibly terminates security monitoring processes, leaving the system without critical defenses before ransomware deployment.[2, 3]

Qilin was the most prolific ransomware operation of 2025.[4, 5, 6] The CIS Cyber Threat Intelligence (CTI) team identified Qilin as the top ransomware threat to State, Local, Tribal, and Territorial (SLTT) organizations throughout 2025, and the group accounted for the second most SLTT ransomware incidents reported to the MS-ISAC through Q1 2026.[7] Qilin's adoption of EDR killer capabilities reflects a broader shift across the ransomware ecosystem. As defenders continue to adopt effective capabilities like EDR, attackers have placed a greater premium on subverting those protections to ensure successful encryption. To better defend against the growing deployment of EDR tampering tools and techniques, SLTT executives should direct their security teams to verify endpoint protection tamper safeguards are enabled and functioning, and confirm that driver loading policies restrict unauthorized kernel-level software.

New Tool Designed to Blind Defenders

EDR products have become foundational to government cybersecurity programs since 2022, when federal grant funding through the State and Local Cybersecurity Grant Program (SLCGP) accelerated deployment to local governments. By 2023, 40% of states were delivering endpoint detection as a shared service to local jurisdictions, replacing traditional antivirus with EDR's continuous behavioral monitoring to detect and disrupt malicious processes like file encryption in real time.[8] EDR tools are designed to detect and prevent activity across the ransomware kill chain and include capabilities to specifically defend against encryption. In March, an ESET cybersecurity researcher speaking to the Hacker News advised that ransomware encryption is susceptible to EDR detection because it must modify many files in a short period of time, which makes it extremely difficult to evade EDR's behavioral monitoring.[9]

Beyond defensive tool deployment, ransomware operators have been facing increasing pressure to innovate across the attack chain. Coveware, a cybersecurity organization focused on ransomware recovery, assessed in Q3 2025 that increasingly shrinking profits are forcing ransomware actors to become more creative and targeted across their operations.[10] EDR killers address this obstacle by providing operators a reliable utility to neutralize endpoint defenses prior to encryption. Qilin operates as a Ransomware-as-a-Service (RaaS) platform with a

© 2026 - Center for Internet Security, Inc. You are encouraged to share this document within the state, local, tribal, and territorial (SLTT) executive leadership community.

broad affiliate network. Qilin affiliates commonly gain initial access through compromised VPN credentials and unpatched perimeter devices.[11, 12] Cisco Talos' analysis of Qilin's EDR killer's infection chain builds on Sophos's December 2025 reporting, which documented the tool's underlying delivery mechanism.[13, 14] Qilin affiliates typically deploy the EDR killer late in the intrusion chain, after gaining administrative privileges and conducting lateral movement using legitimate remote management tools that blend with normal network activity.[15] The attack leverages two distinct phases:

1. In the first phase, a legitimate application loads a malicious library file instead of the genuine system component, a technique known as DLL side-loading. The rogue library maintains normal application behavior to avoid suspicion, while silently executing a multi-stage payload entirely in memory with no files written to disk.[16]
2. In the second phase, the tool loads a legitimately signed but vulnerable driver to gain kernel-level access, a technique called Bring Your Own Vulnerable Driver (BYOVD). Using that privileged access, it disables all EDR monitoring at the kernel level and forcibly terminates security processes, clearing the path for ransomware deployment.[17, 18]

The tool contains a hardcoded list of over 300 EDR driver names across major security vendors.[19, 20]

Qilin's EDR killer highlights a broader trend across the ransomware ecosystem. ESET tracked close to 90 distinct EDR killer tools active in the wild as of early 2026, 54 of which leveraged BYOVD-based tools abusing 35 different vulnerable drivers.[21, 22] Sophos and incident response firm Arete reported that a separate EDR-disabling tool called EDRKillShifter, originally developed by RansomHub operators, has been deployed through a coordinated effort across at least eight ransomware groups including Qilin, Medusa, and Play.[23, 24] Separately, Trend Micro documented the Warlock ransomware group employing a similar BYOVD technique in a January 2026 intrusion, using a different vulnerable driver to disable security products at the kernel level before deploying ransomware via unpatched Microsoft SharePoint servers.[25] Additionally, the CISA/FBI/MS-ISAC #StopRansomware joint Cybersecurity Advisory for Medusa explicitly warned that Medusa actors attempted to use vulnerable or signed drivers to disable EDR tools, and similar warnings appeared in advisories for Akira, RansomHub, and Play.[26, 27, 28, 29]

Impact Assessment

SLTT organizations relying on EDR should ensure they have protections in place against EDR disabling tools like Qilin's. The tool's scope, targeting over 300 products from virtually every major vendor, means that SLTTs should not assume their EDR product is immune to this technique. The three following factors highlight the risk Qilin's use of EDR killers pose to SLTT networks:

- **Broad product coverage:** The tool targets products across major EDR vendors, and the BYOVD technique leverages a security blind spot in the Windows driver ecosystem rather than a flaw in any individual security product.
- **Cross-group proliferation.** Numerous ransomware groups have been sharing EDR-disabling tools through their affiliate networks, meaning EDR-disabling techniques are likely to appear across incidents beyond Qilin.[30]
- **Sector exposure.** Qilin affiliates have demonstrated a willingness to breach government, education, and healthcare organizations.[31, 32]

The operational consequence of threat actors disabling EDR is a loss of endpoint protection. In these attacks, the security products designed to detect and block ransomware execution become targets within the attack.

© Center for Internet Security, Inc. 2026.

Outlook

The CIS CTI team assesses that ransomware actors will likely continue to adopt EDR-disabling techniques throughout 2026. Due to the large supply of legitimately signed but vulnerable drivers available for similar BYOVD techniques, Qilin's approach will likely remain effective in the near term. In addition to ESET reporting 90 EDR killer tools across the threat environment, academic research has identified over 900 known vulnerable signed drivers. This suggests the supply of exploitable drivers far exceeds the rate at which organizations can block them.[33, 34] CIS analysts assess that the economic pressures driving ransomware operators toward more creative and targeted methods are likely to sustain deployment of EDR-disabling tools.[35] Qilin's cross-platform capabilities and sustained operational tempo mean the group is likely to remain a prominent threat to SLTTs through 2026. Qilin accounted for 24% of SLTT ransomware incidents reported to the MS-ISAC in 2025 and 16% in Q1 of 2026.

Recommendations

SLTT leaders should direct their security teams to take the following steps to address the threat posed by ransomware groups like Qilin leveraging EDR-disabling tools:

- Verify that endpoint protection tamper safeguards are enabled and functioning across all managed systems. EDR products include built-in protections against process termination, but these features are not always enabled by default and can be inadvertently disabled during deployment. See **CIS Control 10: Malware Defenses, Safeguard 10.1**.
- Ensure that driver loading policies restrict unauthorized kernel-level software. Direct your security team to confirm that the Windows Vulnerable Driver Blocklist is enabled and current, and evaluate whether application control policies can restrict unsigned driver installation to approved change windows. See **CIS Control 2: Inventory and Control of Software Assets, Safeguard 2.5**.
- Confirm that multi-factor authentication is enforced on all remote access portals, VPN gateways, and administrative interfaces. Compromised VPN credentials continue to be Qilin's most common initial access method, and MFA is the single most effective control against this vector. See **CIS Control 6: Access Control Management, Safeguard 6.3, 6.4, and 6.5**.
- Direct your security team to review perimeter devices, particularly Fortinet appliances, for unpatched vulnerabilities actively exploited by Qilin affiliates. Prioritize patching internet-facing systems. See **CIS Control 7: Continuous Vulnerability Management, Safeguard 7.4**.
- Verify that offline or immutable backups exist for critical systems and data, and that restoration procedures have been tested. Backup integrity is the most reliable safeguard against ransomware encryption. See **CIS Control 11: Data Recovery, Safeguard 11.1, 11.4, and 11.5**.

For additional support, or information regarding services, please contact CIS here.

© Center for Internet Security, Inc. 2026.

Referenc

1. https://blog.talosintelligence.com/qilin-edr-killer/
2. https://blog.talosintelligence.com/qilin-edr-killer/
3. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html
4. https://www.nccgroup.com/newsroom/ncc-group-annual-cyber-threat-intelligence-2025/
5. https://www.guidepointsecurity.com/newsroom/ransomware-victims-and-threat-groups-surge-to-record-levels/
6. https://www.breachsense.com/ransomware-reports/march-2026/
7. https://www.cisecurity.org/insights/blog/qilin-top-ransomware-threat-to-sltts-in-q2-2025
8. https://www.nascio.org/wp-content/uploads/2023/09/NASCIO_2023-State-CIO-Survey-A.pdf
9. https://thehackernews.com/2026/03/54-edr-killers-use-byovd-to-exploit-34.html
10. https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet
11. https://www.cisecurity.org/insights/blog/qilin-top-ransomware-threat-to-sltts-in-q2-2025
12. https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/
13. https://blog.talosintelligence.com/qilin-edr-killer/
14. https://news.sophos.com/en-us/2025/12/06/inside-shanya-a-packer-as-a-service-fueling-modern-attacks/
15. https://blog.talosintelligence.com/qilin-edr-killer/
16. https://blog.talosintelligence.com/qilin-edr-killer/
17. https://blog.talosintelligence.com/qilin-edr-killer/
18. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html
19. https://blog.talosintelligence.com/qilin-edr-killer/
20. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html
21. https://www.welivesecurity.com/en/eset-research/edr-killers-explained-beyond-the-drivers/
22. https://thehackernews.com/2026/03/54-edr-killers-use-byovd-to-exploit-34.html
23. https://www.sophos.com/en-us/blog/shared-secret-edr-killer-in-the-kill-chain
24. https://areteir.com/resources/threat-groups-use-updated-edrkillshifter-tool
25. https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html
26. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a
27. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a
28. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
29. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
30. https://www.sophos.com/en-us/blog/shared-secret-edr-killer-in-the-kill-chain
31. https://industrialcyber.co/ransomware/qilin-ransomware-escalates-rapidly-in-2025-targeting-critical-sectors-with-700-attacks-amid-ransomhub-shutdown/
32. https://www.cisecurity.org/insights/blog/qilin-top-ransomware-threat-to-sltts-in-q2-2025
33. https://www.welivesecurity.com/en/eset-research/edr-killers-explained-beyond-the-drivers/
34. https://www.s3.eurecom.fr/post/2025/10/13/unveiling-byovd-threats-malwares-use-and-abuse-of-kernel-drivers/
35. https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet

© Center for Internet Security, Inc. 2026.

© 2026 - Center for Internet Security, Inc. You are encouraged to share this document within the state, local, tribal, and territorial (SLTT) executive leadership community.