ultraviolet

THREAT ADVISORY

BYOVD Threats

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
April 7, 2026
TLP:GREEN

Executive Snapshot

Bring Your Own Vulnerable Driver (BYOVD) has become a high-impact ransomware enabler because it allows threat actors to weaponize legitimate signed but vulnerable kernel drivers to disable endpoint security controls, reduce visibility, and create the conditions needed for broader intrusion activity such as lateral movement, data theft, and encryption. Recent reporting tied to Qilin and Warlock shows that this technique is being used in real-world operations to terminate EDR processes, suppress monitoring, and weaken defensive response across enterprise environments, underscoring that BYOVD is no longer a niche tradecraft but an increasingly operationalized method for blinding defenders before the most destructive phase of an attack begins.

- Enforce strict driver control policies by enabling vulnerable driver blocklists, application control, kernel integrity protections, and centralized monitoring for unauthorized driver or service installation across all endpoints and servers.

- Reduce attacker opportunity by aggressively patching internet-facing systems, hardening privileged access, and monitoring for stolen credential use, suspicious administrative activity, and unusual Group Policy changes that could be used to deploy BYOVD tooling at scale.

- Validate resilience through detection engineering and testing by ensuring the SOC can alert on known BYOVD behaviors, driver-loading anomalies, EDR tampering attempts, and defense evasion activity before ransomware operators can disable security visibility.

TIDE Team Analysis

Bring Your Own Vulnerable Driver, or BYOVD, remains one of the more dangerous trends in modern ransomware operations because it allows threat actors to weaponize legitimate signed kernel drivers against the security tools designed to stop them. In the April 2026 reporting on Qilin and Warlock, both groups were observed using vulnerable drivers to interfere with or disable endpoint protections, reinforcing that BYOVD is no longer a specialized edge case. It is becoming a practical and repeatable method for ransomware operators seeking to blind defenders before encryption, lateral movement, or data theft begins in earnest.

The Qilin activity illustrates why this technique is so effective. Researchers analyzed a malicious msimg32.dll used in Qilin intrusions and found a multi-stage infection chain built specifically to disable local endpoint detection and response controls. The malware uses DLL side-loading to gain execution, then prepares an in-memory EDR-killer component capable of terminating more than 300 EDR drivers across many security vendors. That scale suggests the operators are designing for broad enterprise applicability rather than tailoring the capability to a single defensive product.

What makes the Qilin intrusion chain particularly concerning is the amount of layered defense evasion surrounding the driver abuse. The loader was observed neutralizing user-mode hooks, suppressing telemetry visibility, obscuring execution flow through exception handling, and keeping the most sensitive parts of the payload in memory. It also deployed helper drivers, including a renamed vulnerable driver that enabled access to physical memory and another used to terminate EDR-related processes after security monitoring callbacks were removed. In practical terms, that means defenders can lose both visibility and enforcement at precisely the point when rapid containment is most important.

This reporting also shows that BYOVD is not unique to a single ransomware family. The same driver combination has reportedly appeared in previous attacks linked to other ransomware operators, indicating that vulnerable-driver abuse is becoming part of a broader criminal tradecraft ecosystem. For leadership teams, that changes the conversation from a narrow malware-analysis issue into an enterprise resilience problem. Once a trusted but vulnerable signed driver is loaded into the kernel, assumptions about endpoint telemetry, tamper protection, and process-kill resistance become far less reliable.

The Warlock case demonstrates the same pattern in a slightly different operational model. In that intrusion set, the group reportedly exploited unpatched internet-facing Microsoft SharePoint servers for initial access, then expanded its foothold with a mix of remote administration, tunneling, proxying, and exfiltration tooling. Within that broader sequence, BYOVD served as the mechanism for disabling security products at the kernel level, allowing the rest of the intrusion to move forward with less resistance and a lower likelihood of early detection.

Warlock's use of the technique is notable because it highlights how operationalized BYOVD has become. In the reported January 2026 intrusion, the group used a loader disguised as a legitimate security-related executable to exploit a vulnerable kernel driver, then used Group Policy deployment to push that capability across the compromised domain. The tool continuously terminated security processes from multiple major vendors, showing that the goal was not simply to evade protection on one endpoint but to degrade defensive coverage at scale across the environment. That represents a meaningful escalation because a single foothold can quickly become a mechanism for weakening enterprise-wide detection and response.

From a risk-management perspective, the larger lesson is that BYOVD compresses the defender's response window. In observed Qilin intrusions, attackers were noted to rely on stolen credentials for access and to delay ransomware

execution by several days. Under normal circumstances, that interval can provide defenders with an opportunity to detect post-compromise activity and contain the intrusion before encryption occurs. BYOVD directly undermines that opportunity by targeting the tools, drivers, and telemetry required to capitalize on that time. If attackers can disable EDR or suppress monitoring early enough, standard containment playbooks may fail before responders fully understand how degraded visibility has become.

For CTO and CISO audiences, the strategic takeaway is that BYOVD should now be treated as a core ransomware defense problem rather than a niche malware technique. The relevant controls go beyond standard patching and antivirus deployment into driver governance, kernel integrity protections, application control, monitoring for new driver and service installation, hardening of exposed systems such as SharePoint, and faster detection of privileged administrative abuse after initial compromise. The activity associated with Qilin and Warlock shows that ransomware groups are increasingly pairing access operations with deliberate attacks on endpoint defenses, and organizations that do not explicitly plan for vulnerable-driver abuse may discover too late that their controls were present but no longer functioning.

Why It Matters

BYOVD matters because it breaks one of the assumptions many security programs still rely on: that a legitimately signed driver can be broadly trusted once it reaches the kernel. Microsoft has explicitly framed BYOVD as a class of attacks in which an adversary with administrative privileges installs a legitimately signed but vulnerable driver, then uses that kernel-level access to interfere with the operating system and security controls. That makes the issue historically important because it is not just another malware loader or evasion script; it is a way to convert trusted code into a privilege-enforcement and visibility problem at the deepest part of the host. Once attackers reach that layer, they can disable protections that would otherwise stop ransomware, credential theft, or post-compromise reconnaissance.

The historical threat is that BYOVD has steadily moved from a specialist technique into repeatable criminal tradecraft. Cisco Talos documented a DeadLock ransomware campaign in December 2025 that used a BYOVD loader against a vulnerable Baidu Antivirus driver to terminate EDR processes, disable Windows Defender, stop services, and impair recovery. More recently, Talos reporting on Qilin described broader ransomware activity in 2025 and emphasized that Qilin was one of the most impactful ransomware groups observed, while separate April 2026 reporting tied Qilin to a BYOVD-enabled intrusion chain designed to weaken endpoint defenses before ransomware deployment. In other words, the historical pattern is not isolated experimentation; it is a progression toward standardized ransomware use of vulnerable drivers as a pre-encryption force multiplier.

The current threat is that BYOVD is now being operationalized across longer, more deliberate enterprise intrusions rather than only short smash-and-grab attacks. Trend Micro's March 2026 analysis of Warlock showed operators spending 15 days inside a victim environment, using a persistent BYOVD technique based on the NSec driver alongside tools for persistence, tunneling, and lateral movement. That matters because it shows vulnerable drivers are being used not only to dodge one security product on one machine, but to help sustain access, degrade detection, and create safer operating conditions for the attackers across the broader intrusion lifecycle. For security leadership, the implication is clear: vulnerable-driver abuse now sits at the intersection of endpoint protection, privileged access, incident response, and ransomware resilience, so organizations that do not plan for it are exposed to a failure mode where security controls remain installed but can no longer be trusted to function when they are needed most.

How to Respond

- Strictly adhere to cybersecurity Fundamentals and ensure all personnel undergo annual phishing and social engineering training. Speak with your UltraViolet Cyber TAM Representative to schedule a live phishing engagement.
- Leverage Vulnerable Driver Blocklists and Code Integrity checks along with hardened administrative rights.
- Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a RedTeam or PurpleTeam engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Monitoring Driver Load and Service Installation Events using Sysmon Event ID 6, 3033, and 7045 in customer provide logs.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---