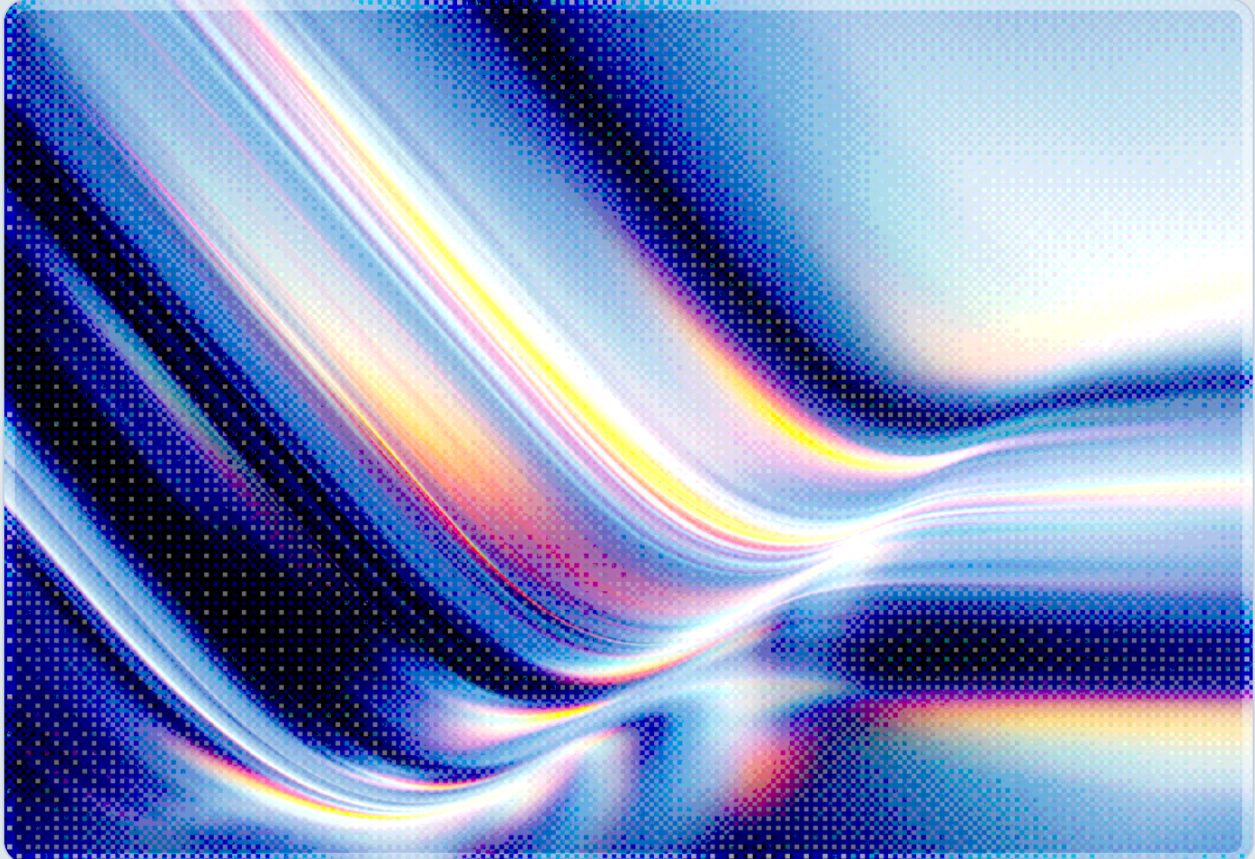


Warlock Ransomware: Year-Old SharePoint Flaws, Modern EDR Evasion

Security Implications and Guidance

2026-10-05

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Symantec and Carbon Black researchers report that the Warlock ransomware operation, tracked by Microsoft as Storm-2603, has spent roughly the past two months (since at least late July 2026) compromising at least four organizations through on-premises SharePoint flaws that the reporting describes as "ToolShell and related SharePoint flaws," the family first disclosed in July 2025 [1][2]. The sources we reviewed do not name the specific CVEs used in the 2026 intrusions. Two of the victims were critical infrastructure operators, a water utility and a telecommunications provider. The others were a regional government body and a university, located in Portuguese- and Spanish-speaking countries across Europe, Africa, and Latin America [1]. All campaign figures in this note are as reported by The Hacker News and Security Affairs; we could not locate the primary Symantec or Carbon Black publication.

The campaign matters less for the age of the vulnerabilities than for what happens after initial access. In one intrusion, the attackers pushed a tool designed to disable security software to at least 40 hosts in about two hours and then deployed ransomware to at least 33 hosts by staging it in the domain's SYSVOL share, which delivered it through ordinary domain replication [1]. The security-tool disabler relies on a signed, vulnerable kernel driver, an approach known as "bring your own vulnerable driver" (BYOVD) [1][3].

Three lessons can be drawn, two from the reported intrusions and one from Microsoft's 2025 guidance. First, although the reporting does not say whether the victim servers were patched, Microsoft's guidance indicates that a SharePoint server patched but never re-keyed may still be exploitable or already compromised, a distinction that patch-compliance dashboards do not capture [2]. Second, endpoint detection and response (EDR) tooling should be treated as a control that a domain-privileged attacker can switch off, so detection must not depend on it alone. Third, SYSVOL and Group Policy are write paths that deserve the same monitoring as any other mass-deployment mechanism.

Background

ToolShell is the name given to a chain of SharePoint vulnerabilities exploited as zero-days beginning in July 2025. Microsoft's guidance identified CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771, all affecting on-premises SharePoint Server only [2]. The chain allowed an

attacker to obtain remote code execution, drop a web shell, and extract the server's ASP.NET machine keys. Possession of those keys lets an attacker forge validly signed payloads, which is why Microsoft's mitigation list included rotating the keys and restarting IIS alongside installing the security updates [2].

Microsoft attributed ransomware deployment in that first wave to Storm-2603, a China-based actor, with Warlock ransomware distribution beginning on July 18, 2025 [2]. Its observed 2025 chain used credential harvesting with Mimikatz, lateral movement with PsExec and Impacket, and Group Policy Object modification to distribute the ransomware [2]. Symantec tracks overlapping activity as Longlegs, and other vendors use additional names such as Gold Salem [1]. This note uses "Warlock" for the operation and "Storm-2603" where Microsoft's attribution is the relevant source. Readers should treat the link between the 2025 and 2026 activity as a vendor assessment and not as a confirmed identity.

The new reporting, summarized in early October 2026, shows the same operation returning to the same vulnerability family a year later [1][3]. Symantec assesses that ToolShell and related SharePoint flaws remain a viable initial access route against deployments that have not been patched or otherwise mitigated, and that the victim pattern suggests either opportunistic exploitation of exposed servers or deliberate regional focus [1]. The reporting does not establish which explanation is correct, and defenders should avoid assuming that organizations outside these regions are out of scope.

Security Analysis

The campaign can be read as a sequence of stages, each of which offers a different opportunity for detection. The first two stages, initial access and persistence, take place on the SharePoint tier. The third, defense evasion, is where the operators remove the endpoint tooling that would otherwise observe the rest. The final stage uses domain infrastructure itself to deliver the payload.

Initial access and persistence

The observed intrusions follow a recognizable sequence. Attackers exploit SharePoint, place web shells (in one case in the LAYOUTS directory), and collect the ASP.NET machine keys needed to forge signed payloads that execute inside the SharePoint application pool [1][3]. In the intrusion Symantec describes in most detail, the web shell appeared on July 22, 2026, reconnaissance followed within days, and security-tool disabling began on July 31, roughly nine days after initial access [3]. In this intrusion, that interval gave defenders with SharePoint-tier visibility a window in which to act before the EDR was disabled.

For persistence and command-and-control, the operators combined techniques that blend into administrative activity. Reporting describes DLL sideloading, payload hosting on legitimate file-sharing and cloud storage services (catbox.moe and wasabisys.com), and abuse of the Visual Studio Code tunnel feature for remote access [1][3]. These techniques use legitimate software or services and can be harder for reputation-based filtering to catch. The VS Code tunnel deserves particular attention because it can establish an outbound-initiated remote session through a Microsoft-operated relay, which may be difficult to distinguish from developer use unless the organization restricts where it is allowed.

Disabling endpoint protection

The reported security-tool disabler abuses K7RKScan.sys, a driver from the K7 Security anti-malware suite, through CVE-2025-1055 [1][3]. NVD describes the flaw as missing access control in the driver's IOCTL handler that allows a local low-privilege user to terminate processes running with administrative or system privileges, other than those the operating system protects [4]. The driver is legitimately signed, so Windows will load it, and the BYOVD approach therefore turns a trusted signature into a means of ending security processes. The record carries a CNA-assigned CVSS v3.1 score of 5.6 (Medium), and NVD lists K7 Security Anti-Malware versions before 23.0.0.10 as affected [4]. CVSS base scores do not account for chaining, so this rating does not reflect the flaw's role as one step in a ransomware chain.

Two features of the reported operation deserve emphasis. The first is speed: the disabler reached at least 40 hosts within about two hours [1][3]. Reaching that many hosts that quickly suggests the attackers held domain-level or management-plane privileges, consistent with the credential theft and lateral movement documented in 2025 [2]; the reporting we reviewed does not describe how those privileges were obtained in 2026. The second is the use of an exploit against a vulnerable driver instead of a fully custom EDR killer, which means that blocking the specific driver is useful but not sufficient, since attackers can substitute another signed driver with a similar flaw.

Ransomware distribution through SYSVOL

After disabling protections, the operators staged the ransomware in the domain's SYSVOL share and let ordinary domain replication carry it to machines, ultimately running on at least 33 hosts [1][3]. This is an efficient design from the attacker's perspective, because no external tooling is needed to copy the payload to each host and the traffic is domain-controller-to-member replication that defenders expect. The 2025 reporting describes a related approach using Group Policy modification [2]. In both cases the control being abused is the same: write access to the domain's policy distribution path.

Why this matters for critical infrastructure

Two of the four reported victims were critical infrastructure operators, which is the observation that makes the campaign relevant to this audience. Operators in these sectors commonly face change-control and availability constraints that can slow patching and key rotation, although the reporting does not say whether that applied to these victims. The reported victims suggest that a year is not enough for every deployment to complete remediation, though the available reporting does not state how the compromised servers were exposed or whether they had received the 2025 updates [1][3]. We treat both "unpatched" and "patched but with unrotated machine keys" as possible explanations, and recommend verifying both.

The table below summarizes the stages reported in the October 2026 campaign and the defensive control we suggest as best positioned to interrupt each one. Technique entries are drawn from the cited reporting; the control column reflects CSA analysis.

Stage	Reported technique	Suggested control (CSA analysis)
Initial access	ToolShell exploitation of on-premises SharePoint [1]	Patching, AMSI in Full Mode, removing internet exposure [2]
Foothold	Web shell; ASP.NET machine key theft [1][2]	Machine key rotation, IIS restart, web shell hunting [2]
Remote access	VS Code tunnel; DLL sideloading [1][3]	Egress policy, application allow-listing
Defense evasion	BYOVD via K7RKScan.sys (CVE-2025-1055) [1][4]	Driver block rules, tamper protection, alerting on agent health
Lateral movement	Credential theft, remote execution [2]	LSA protection, tiered administration
Impact	Ransomware staged in SYSVOL and replicated [1][3]	SYSVOL write monitoring, segmentation, offline backups

Recommendations

The recommendations follow the stages in the table above, beginning with the actions that close the SharePoint entry point and then moving to the controls that limit damage if an attacker reaches the domain. The first group addresses the exposed server tier, where the reported intrusions began.

Immediate Actions

Organizations running on-premises SharePoint Server should confirm that the 2025 ToolShell security updates are installed on every farm member, including servers that are rarely administered, such as test and disaster-recovery instances [2]. Confirming patch status is not enough on its own. Machine keys should be rotated and IIS restarted on all SharePoint servers, as Microsoft advised in 2025, because a server patched after compromise can still be accessed with stolen keys [2]. Teams should also hunt for web shells in the SharePoint LAYOUTS directory and for the spinstall0.aspx file name Microsoft reported in 2025 [1][2].

Next, review which SharePoint servers are reachable from the internet and whether they need to be. Where exposure is required, enable Antimalware Scan Interface (AMSI) in Full Mode with a supported antivirus product, as Microsoft recommended [2]. Teams should also review recent outbound connections to catbox.moe and wasabisys.com from server-tier hosts and any Visual Studio Code tunnel activity on servers, neither of which has a typical reason to occur there [1][3]. Finally, confirm that K7 Security software, if present anywhere in the estate, is at version 23.0.0.10 or later [4].

Short-Term Mitigations

Enable EDR tamper protection and LSA protection as general hardening against the credential theft and security-tool termination described above; these are our recommendations, and we did not confirm that Microsoft's 2025 guidance lists them. Apply a vulnerable-driver blocklist, for example Windows Defender Application Control or Microsoft's recommended driver block rules, and add the K7RKScan.sys hash to any local deny list. Because attackers can switch to another driver, also create an alert for security agents that stop reporting, treating a silent endpoint as an incident signal and not a connectivity problem. In the reported intrusion, the disabler reached at least 40 hosts in about two hours [1]; an alert on agents ceasing to report would have had a window of that length in which to fire, provided the alerting does not depend on the disabled agents.

Monitor SYSVOL and Group Policy for unexpected file creation and modification, and restrict who can write to them. Restrict the VS Code tunnel feature and similar developer remote-access services to approved hosts. Review egress filtering for server subnets so that file-hosting services are not reachable by default. Offline or immutable backups are a primary determinant of recovery outcomes if the earlier layers fail.

Strategic Considerations

The broader lesson is that a vulnerability's disclosure date is a poor guide to its operational life. Remediation programs should track completion criteria that include post-patch actions (key rotation, credential resets, compromise assessment), and not only whether a CVE appears in a scanner report. Organizations should also plan for on-premises SharePoint's lifecycle, since a platform that is difficult to patch and exposed to the internet carries accumulating risk; migration to a supported cloud service or strict network isolation are the most durable options.

Second, security teams should decide in advance how they operate when EDR is disabled. That means having network-level detection, identity-layer alerting on domain administrator activity, and tested procedures for isolating a domain segment. Finally, critical infrastructure operators should evaluate how a compromise of an enterprise collaboration server could reach domain-wide privileges, and use segmentation and tiered administration to break that path.

CSA Resource Alignment

CSA has published two rapid-research notes on actively exploited SharePoint vulnerabilities in 2026, and both bear directly on this campaign. The note on [CVE-2026-45659: SharePoint RCE Under Active Exploitation](#) covers a deserialization flaw in on-premises SharePoint added to CISA's KEV catalog, and its guidance to treat the federal remediation window as the practical deadline for all organizations applies equally to the ToolShell family [5]. The companion note on [CVE-2026-58644](#) addresses a later SharePoint zero-day under an accelerated remediation mandate [6]. Read together with the Warlock reporting, the three suggest that on-premises SharePoint has been a recurring entry point across consecutive years and not an isolated 2025 event; this is our inference from the pattern and not a finding stated in any single source.

For the defense-evasion stage, CSA's [GentleKiller: Inside the Gentlemen RaaS EDR-Killer Suite](#) is the closest match. It describes a separate ransomware operation that uses BYOVD techniques to terminate security processes, and it recommends prioritizing Hypervisor-Protected Code Integrity (HVCI) and

Windows Defender Application Control policies over sole reliance on EDR process monitoring, since BYOVD attacks operate below the layer that user-space agents can observe [7]. That guidance reinforces the driver-blocking and agent-health recommendations above.

For the post-compromise portion of the chain, CSA's [Zero Trust Guidance for Critical Infrastructure](#) is the most specific resource. Its emphasis on segmentation and limiting implicit trust between IT and operational environments corresponds to the tiered-administration and isolation measures recommended above [8]. As a topical fallback for control mapping, the [AI Controls Matrix \(AICM\) v1.1](#) provides controls in its Threat and Vulnerability Management and related domains that organizations can use to document patch, key-rotation, and tamper-protection practices [9].

References

- [1] The Hacker News. "[Warlock Exploits SharePoint Flaws to Disable Security Tools and Deploy Ransomware.](#)" The Hacker News, October 2026 (reporting on Symantec and Carbon Black Threat Hunter Team research).
- [2] Microsoft Threat Intelligence. "[Disrupting active exploitation of on-premises SharePoint vulnerabilities.](#)" Microsoft Security Blog, July 22, 2025 (updated July 23, 2025).
- [3] Security Affairs. "[Warlock Ransomware Still Exploits Year-Old SharePoint Flaws to Hit Critical Infrastructure.](#)" Security Affairs, October 2026.
- [4] NIST National Vulnerability Database. "[CVE-2025-1055 Detail.](#)" NVD, accessed October 5, 2026.
- [5] Cloud Security Alliance AI Safety Initiative. "[CVE-2026-45659: SharePoint RCE Under Active Exploitation.](#)" CSA Labs, July 3, 2026.
- [6] Cloud Security Alliance AI Safety Initiative. "[SharePoint Zero-Day CVE-2026-58644 Joins CISA KEV Under 3-Day Mandate.](#)" CSA Labs, July 2026.
- [7] Cloud Security Alliance AI Safety Initiative. "[GentleKiller: Inside the Gentlemen RaaS EDR-Killer Suite.](#)" CSA Labs, June 22, 2026.
- [8] Cloud Security Alliance. "[Zero Trust Guidance for Critical Infrastructure.](#)" Cloud Security Alliance, 2025.
- [9] Cloud Security Alliance. "[AI Controls Matrix v1.1.](#)" Cloud Security Alliance, 2025.