

Warlock-Ransomware trifft Wasserversorger über SharePoint-Lücken

Stand 15.10.2026 08:56 · Sendung: – · · Belegstärke: **bestätigt** · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 41 % ■ Wahrscheinlich 15 % ■ Nicht bekannt 44 %

A und B stimmen überein: Die Angriffskette eines Falls ist durch eine einzige Primärquelle (Symantec) gut belegt. Offen sind die Opfer, ihre Länder, die konkret genutzte SharePoint-CVE (ToolShell 2025 oder eine aus 2026), der Treiber des EDR-Killers und jede OT-Auswirkung. Seit dem 05.10.2026 ist keine neue Primärquelle hinzugekommen.

1. Was ist passiert, und warum?

WISSEN

- Symantec (Threat Hunter Team, 01.10.2026): Die Gruppe Longlegs (auch Storm-2603) hat in den letzten zwei Monaten mindestens vier Organisationen angegriffen: einen Wasserversorger, einen Telekommunikationsanbieter, eine regionale Behörde und eine Universität in portugiesisch-/spanischsprachigen Ländern in Europa, Afrika und Lateinamerika. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]
- Symantec nennt die ToolShell-Kette (CVE-2025-49704, -49706, -53770, -53771). Zusätzlich verweist Symantec auf neuere SharePoint-Schwachstellen aus einer CISA-Warnung vom Juli 2026, nennt dazu aber keine CVE-Nummer und ordnet keine davon diesem Fall zu. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]
- Dokumentierte Kette: am 22.07.2026 die Webshell layout2sp.aspx, die die ASP.NET-MachineKeys ausliest. Danach folgten Erkundung, am 28.07. gefälschte signierte __VIEWSTATE-Payloads und Nachladen per msixexec. Am 28./29.07. wurde das getarnte Konto SPSEPRDSetup als lokaler Admin angelegt, mit NetExec das AD ausgekundschaftet und ein VS-Code-Insiders-Tunnel als Persistenz eingerichtet. Am 31.07. liefen der EDR-Killer a.exe und danach Warlock, verteilt über SYSVOL/DFS-Replikation. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]
- Symantec vermutet für den EDR-Killer einen verwundbaren Treiber (BYOVD). Welcher Treiber es in diesem Fall war, ist unbekannt. K7RKScan (CVE-2025-1055) hat die Gruppe in anderen Angriffen genutzt. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]
- Symantec hält beides für möglich: die opportunistische Ausnutzung verwundbarer SharePoint-Server oder eine gezielte Beauftragung. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]
- Microsoft (22.07.2025): Storm-2603 setzt seit dem 18.07.2025 über die SharePoint-Lücken Ransomware ein. Die Herkunft China bewertet Microsoft nur mit mittlerer Sicherheit (moderate confidence), die Ziele des Akteurs kann Microsoft nicht sicher einschätzen. (100 %) [<https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>]
- The Hacker News berichtete im Juli 2025 nach Microsoft, dass Storm-2603 als vermutlich China-basierter Akteur Warlock über ToolShell verteilt. (100 %) [<https://thehackernews.com/2025/07/storm-2603-exploits-sharepoint-flaws-to.html>]
- CISA warnte am 14.07.2026 (zuletzt aktualisiert am 26.08.2026) vor der aktiven Ausnutzung von sechs SharePoint-Schwachstellen (CVE-2026-32201, -45659, -56164, -58644, -50522,

-55040). Warlock oder Storm-2603 werden dort nicht genannt. (100 %)

[<https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations>]

- SecurityWeek (02.10.2026): Das Arsenal der Gruppe könnte („may also include“) diese sechs SharePoint-CVEs aus 2026 umfassen. Eine bestätigte Nutzung durch Warlock wird nicht berichtet. (100 %)

[<https://www.securityweek.com/warlock-expands-sharepoint-exploitation-in-critical-infrastructure-attacks/>]

NICHT BEKANNT

- Namen und Länder der vier Opfer
- Welche SharePoint-Schwachstelle im dokumentierten Fall tatsächlich genutzt wurde (ToolShell 2025 oder eine CVE aus 2026)
- Welcher Treiber beim EDR-Killer in diesem Fall missbraucht wurde
- Ob die Ransomware per GPO/Logon-Skript gestartet wurde
- Ob die Opfer gezielt oder opportunistisch ausgewählt wurden
- Das tatsächliche Motiv, insbesondere ob neben der Erpressung auch Spionage eine Rolle spielt (Symantec nennt keines ausdrücklich)
- Ob Daten abgefließen sind (Double Extortion) und ob die Opfer auf einer Leakseite stehen

WAHRSCHEINLICH (Einschätzung)

- Die Opfer wurden eher opportunistisch über per Internet erreichbare, ungepatchte SharePoint-Server gefunden als gezielt als KRITIS-Betreiber ausgewählt. (55 %) – A und B übereinstimmend: Die gemischte Opferauswahl (Universität, Behörde, Versorger) und die Massenausnutzung bekannter Lücken sprechen dafür. Dagegen sprechen die sprachliche Häufung (portugiesisch/spanisch) und Symantecs ausdrücklicher Hinweis auf eine mögliche Beauftragung.
- Das Motiv war vor allem finanziell, ein zusätzliches Interesse an Spionage ist aber nicht ausgeschlossen. (45 %) – Ransomware mit Lösegeldnotiz und Leakseite spricht für Erpressung. Symantec verknüpft die Gruppe aber mit China-nahen Clustern wie ChamelGang/CamoFei, und Microsoft kann die Ziele nicht einschätzen (widersprüchlich: A 50 % / B 45 %, daher gesenkt).

2. Was ist die Auswirkung?

WISSEN

- In einem Fall lief der EDR-Killer (a.exe) in etwa zwei Stunden auf mindestens 40 Hosts. Danach wurde Warlock auf mindestens 33 Hosts ausgeführt, verteilt über die Domänenfreigabe SYSVOL. Auf drei Hosts zeigt dfsrs.exe als Elternprozess die Auslieferung über die DFS-Replikation. (100 %) [<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]

- The Record und BleepingComputer berichten keine Auswirkungen auf OT oder die Versorgung. Symantec warnt nur allgemein vor „real-world consequences“ bei Angriffen auf essenzielle Dienste. (100 %) [<https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks/>]

- Auch SecurityWeek beschreibt keine OT- oder ICS-Auswirkungen. (100 %)

[<https://www.securityweek.com/warlock-expands-sharepoint-exploitation-in-critical-infrastructure-attacks/>]

NICHT BEKANNT

- Welches der vier Opfer der dokumentierte Fall mit 33 Hosts ist
- Ob die Wasserversorgung, Telekommunikationsdienste, Abrechnung oder Kundenservices beeinträchtigt waren
- Welche Systeme genau verschlüsselt wurden (Verwaltung, Abrechnung, Leitsystem-Server)
- Ob Daten abgefließen sind oder Kunden- bzw. Personaldaten veröffentlicht wurden
- Ob Lösegeld gezahlt wurde

WAHRSCHEINLICH (Einschätzung)

- Der Schaden betraf im Wesentlichen die Büro-IT der Domäne (Verwaltung, Abrechnung, Dokumente), nicht die Steuerung der Wasseraufbereitung. (65 %) – A und B übereinstimmend: Die Kette läuft belegt komplett über AD/SYSVOL der Windows-Domäne, und keine Quelle meldet eine Versorgungsstörung. Ob SCADA- oder OT-Server in derselben Domäne hängen, ist aber

unbekannt.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

- Der dokumentierte Angriff lief vom 22.07.2026 (Webshell) bis zum 31.07.2026 (EDR-Killer und Verschlüsselung), also etwa neun Tage vom Einstieg bis zur Ransomware. (100 %)

[<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]

- American Water entdeckte den Angriff laut 8-K am 03.10.2024 und schaltete Kundenportal und Abrechnung ab. Am 10.10.2024 meldete das Unternehmen, dass die Systeme wieder verbunden werden (widersprüchlich: A 11.10. laut SecurityWeek / B 10.10. laut SEC-Pressemitteilung; die Primärquelle der SEC ist übernommen). Wasser- und Abwasseranlagen bzw. die Wasserqualität waren nach Unternehmensangaben nicht betroffen. (100 %)

[<https://www.sec.gov/Archives/edgar/data/1410636/000141063624000179/ex-991xawkpressreleaseoct1.htm>]

- SecurityWeek berichtete über die schrittweise Wiederinbetriebnahme der Systeme bei American Water. (100 %)

[<https://www.securityweek.com/american-water-bringing-systems-back-online-after-cyberattack/>]

- Bei der Südwestfalen-IT (Akira, Ende Oktober 2023) waren die Online-Dienste für Bürger rund ein dreiviertel Jahr nach dem Angriff wieder vollständig oder nahezu vollständig verfügbar. (100 %) [<https://www.it-daily.net/shortnews/sit-wir-sind-wieder-online>]

NICHT BEKANNT

- Wie lange die Wiederherstellung bei den aktuellen Opfern dauert oder gedauert hat
- Ob Backups verschlüsselt oder gelöscht wurden
- Ob das Active Directory neu aufgebaut werden musste
- Ob Lösegeld gezahlt wurde

WAHRSCHEINLICH (Einschätzung)

- Die Kernsysteme laufen nach Tagen bis wenigen Wochen wieder, die vollständige Bereinigung inklusive AD-Neuaufbau dauert Wochen bis Monate. (65 %) – A und B übereinstimmend: Das ist typisch für domänenweite Ransomware mit gestohlenen MachineKeys und Admin-Konten (vergleichbar mit American Water und Südwestfalen-IT). Ein kompromittiertes AD gilt danach in der Regel als nicht vertrauenswürdig. Belege für die konkreten Opfer fehlen.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

- Keine der ausgewerteten Quellen (Symantec, The Record, BleepingComputer, SecurityWeek) berichtet von Auswirkungen auf OT, Leittechnik, Pumpen, Aufbereitung oder andere physische Anlagen. (100 %) [<https://www.bleepingcomputer.com/news/security/warlock-ransomware-breach-sharepoint-in-water-telecom-operator-attacks/>]

NICHT BEKANNT

- Ob beim Wasserversorger OT-Systeme vorsorglich getrennt oder auf Handbetrieb umgestellt wurden
- Ob SCADA-, Historian-, Leitsystem- oder Fernwirk-Server Mitglied der verschlüsselten Windows-Domäne waren
- Zustand der Fernwirktechnik beim Wasserversorger
- Wie die IT/OT-Segmentierung beim Opfer aussieht

WAHRSCHEINLICH (Einschätzung)

- Physische Anlagen wie Pumpen oder Aufbereitung sind nicht beschädigt. (80 %) – A und B übereinstimmend: Warlock ist reine Windows-Ransomware ohne bekannte OT/ICS-Funktionen, und keine Quelle meldet eine Störung. Hardware-Schäden sind bei IT-Ransomware sehr selten und wären bei Versorgern meist öffentlich geworden.
- Mittelbare OT-Auswirkungen sind möglich, z. B. vorsorgliches Trennen, Ausfall der Fernüberwachung oder mitverschlüsselte Windows-/SCADA-Server der Leittechnik in derselben Domäne. (25 %) – Das ist ein bekanntes Muster bei IT-Ransomware in Versorgern (z. B. Colonial

Pipeline). Die domänenweite Verteilung über SYSVOL würde auch Windows-Rechner im OT-Netz erreichen, wenn sie in derselben Domäne hängen. Für diesen Fall gibt es aber keinen Beleg (widersprüchlich: A 30 % / B 25 %, daher gesenkt).

5. Wie viele solcher Ziele gibt es?

WISSEN

- BSI (Stand 03.08.2025): In Deutschland waren noch über 80 On-Premises-SharePoint-Systeme für ToolShell verwundbar, teils mit EOL-Versionen. Auf verwundbaren Servern wurde Ransomware beobachtet. (100 %)

[<https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2025/2025-262781-1032.html>]

- Shadowserver zählte im April 2026 rund 1.370 SharePoint-Server weltweit ohne Patch gegen CVE-2026-32201, USA und Deutschland waren am stärksten betroffen (laut BleepingComputer; von B aus dem Vorstand übernommen und nicht erneut geprüft). (100 %)

[<https://www.bleepingcomputer.com/news/security/over-1-300-microsoft-sharepoint-servers-vulnerable-to-ongoing-attacks/>]

- Bei der ToolShell-Welle 2025 waren laut Berichten (Bloomberg, von The Record zitiert) mindestens 400 Regierungen und Unternehmen betroffen. (100 %)

[<https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks>]

- Laut SecurityWeek waren bei ToolShell 2025 innerhalb weniger Wochen mehr als 400 SharePoint-Server kompromittiert. (100 %)

[<https://www.securityweek.com/warlock-expands-sharepoint-exploitation-in-critical-infrastructure-attacks/>]

- CISA-Alert vom 14.07.2026 (zuletzt geändert am 26.08.2026): Aktiv ausgenutzt werden CVE-2026-32201 (KEV 14.04.), -45659 (KEV 01.07.), -56164 (KEV 14.07.), -58644 (KEV 16.07.), -50522 (KEV 22.07.) und -55040 (KEV 18.08.). Betroffen sind alle unterstützten On-Prem-Versionen (2016, 2019, Subscription Edition). (100 %)

[<https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations>]

- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 142581 gesamt (DNP3 33176, OMRON FINS 22996, ProConOS 16412, EtherNet/IP 15788, Siemens S7 8290, OPC UA 5651) (100 %)

NICHT BEKANNT

- Aktuelle Zahl verwundbarer SharePoint-Server in DE, AT und CH (Stand Oktober 2026)
- Wie viele davon Wasser-, Energie- oder Industriebetreibern gehören
- Ob es weitere, noch nicht öffentliche Opfer dieser Welle gibt

WAHRSCHEINLICH (Einschätzung)

- In DACH, vor allem in Deutschland, ist weiterhin eine dreistellige Zahl von On-Prem-SharePoint-Servern aus dem Internet erreichbar und nicht vollständig gegen die 2026 aktiv ausgenutzten Lücken gepatcht. (55 %) – Das BSI meldete 2025 über 80 verwundbare Systeme, und laut Shadowserver lag Deutschland im April 2026 weit vorn. Die Patchquoten steigen aber, und neuere Zählungen fehlen (widersprüchlich: A 55 % für DACH / B 60 % für Deutschland, daher gesenkt).

6. Kann das wieder passieren?

WISSEN

- Laut Symantec nutzt die Gruppe auch ein Jahr nach den Patches noch die ToolShell-Lücken aus 2025. The Record schreibt, dass einige der ausgenutzten Lücken zum Angriffszeitpunkt seit über einem Jahr gepatcht waren. (100 %)

[<https://www.security.com/threat-intelligence/warlock-ransomware-critical-infrastructure>]

- The Record: Einige der ausgenutzten Lücken waren zum Angriffszeitpunkt seit über einem Jahr gepatcht. (100 %) [<https://therecord.media/warlock-ransomware-used-in-critical-infrastructure-attacks>]

- CISA meldet die aktive Ausnutzung von sechs SharePoint-Schwachstellen aus 2026 in allen unterstützten On-Prem-Versionen. Empfohlen wird, SharePoint nicht direkt ins Internet zu stellen (sonst ein Layer-7-Reverse-Proxy mit Authentifizierung), AMSI im Full Mode zu betreiben, Patches einzuspielen und zu prüfen und die Central Administration extern zu sperren. Vor der Rotation

der MachineKeys sollen zuerst Eindringlingsspuren gesucht und entfernt werden, damit die Schlüssel nicht erneut gestohlen werden. (100 %)

[<https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations>]

• Beazley: Ein ausgenutzter Pfad sollte erst mit dem Microsoft-Release im August 2026 geschlossen werden, die Juli-Updates reichen daher eventuell nicht. (100 %) [<https://beazley.security/alerts-advisories/sharepoint-vulnerabilities-under-active-exploitation-cisa-urges-sharepoint-hardening>]

• Festnahmen oder Anklagen gegen die Gruppe sind nicht bekannt. Die Kampagne wird als aktuell (letzte zwei Monate) beschrieben. (100 %) [<https://www.bleepingcomputer.com/news/security/warlock-ransomware-breach-sharepoint-in-water-telecom-operator-attacks/>]

NICHT BEKANNT

- Ob die Gruppe weitere Opfer angreift (keine Berichte nach dem 05.10.2026)
- Ob die Gruppe ihr Zielgebiet auf DACH ausweitet
- Ob gepatchte, aber nicht bereinigte Server (alte MachineKeys) noch offen sind
- Ob es eine Warnung von BSI, NCSC oder WaterISAC speziell zu dieser Welle gibt (nicht gefunden)

WAHRSCHEINLICH (Einschätzung)

- Die Gruppe wird weiter verwundbare On-Prem-SharePoint-Server ausnutzen, auch bei KRITIS-nahen Organisationen und in Europa. (75 %) – A und B übereinstimmend: Die Gruppe nutzt seit Juni/Juli 2025 durchgehend SharePoint, 2026 kamen immer neue SharePoint-CVEs in den KEV-Katalog, viele Server sind nicht bereinigt, und es gibt keine Hinweise auf eine Zerschlagung.
- Ein DACH-Opfer (z. B. ein Versorger) wird über genau diesen Weg in den nächsten Monaten öffentlich bekannt. (20 %) – Der aktuelle Fokus liegt laut Symantec auf portugiesisch-/spanischsprachigen Ländern, Deutschland hat aber viele verwundbare Server (widersprüchlich: A 25 % / B 20 %, daher gesenkt).

Lage

Laut Symantec (Threat Hunter Team, Bericht vom 01.10.2026) hat die China-nahe Gruppe Longlegs (Microsoft: Storm-2603) in rund zwei Monaten mindestens vier Organisationen mit Warlock-Ransomware angegriffen: einen Wasserversorger, einen Telekommunikationsanbieter, eine regionale Behörde und eine Universität. Die Opfer liegen in portugiesisch- und spanischsprachigen Ländern in Europa, Afrika und Lateinamerika. Der Einstieg lief über ungepatchte On-Premises-SharePoint-Server. Danach folgten eine Webshell, gestohlene ASP.NET-MachineKeys, ein getarntes Admin-Konto und Persistenz über einen Tunnel. Ein EDR-Killer lief in etwa zwei Stunden auf mindestens 40 Hosts, anschließend wurde die Ransomware über SYSVOL/DFS-Replikation auf mindestens 33 Hosts verteilt. Im dokumentierten Fall vergingen vom Ablegen der Webshell (22.07.2026) bis zur Verschlüsselung (31.07.2026) etwa neun Tage. Opfernamen, Länder und Folgen für OT oder die Wasserversorgung sind auch 14 Tage nach dem Bericht nicht öffentlich. Ein DACH-Opfer ist nicht belegt, und seit dem 05.10.2026 gibt es keine neue Primärquelle.

Angriff	Ransomware-Kampagne (Warlock) über On-Premises-SharePoint: Webshell, Diebstahl von ASP.NET-MachineKeys, gefälschte __VIEWSTATE-Payloads, getarntes Admin-Konto, Tunnel-Persistenz (VS Code Insiders), EDR-Killer (vermutlich BYOVD), Verteilung über SYSVOL/DFSR
Wann / Status	Kampagne laut Symantec in den zwei Monaten vor dem 01.10.2026; dokumentierter Fall vom 22.07.2026 (Webshell) bis 31.07.2026 (EDR-Killer und Verschlüsselung) ·
Täter	unbekannt – unbekannt

Früherer Stand: Erstmeldung (03.10.2026 07:24)

Wissen 43 % · wahrscheinlich 18 % · nicht bekannt 39 %

Laut Symantec Threat Hunter Team (Bericht vom 01.10.2026) hat die China-nahe Gruppe Longlegs (Storm-2603) in rund zwei Monaten mindestens vier Organisationen in portugiesisch- und spanischsprachigen Ländern angegriffen: einen Wasserversorger, einen Telekom-Anbieter, eine regionale Behörde und eine Universität. Die Angreifer kamen über ungepatchte On-Premises-SharePoint-Server (ToolShell 2025, laut Medien auch neuere Lücken aus 2026) hinein. In einem Fall schalteten sie auf mindestens 40 Hosts in etwa zwei Stunden die Schutzsoftware ab und verschlüsselten danach über SYSVOL mindestens 33 Hosts. Die Opfer sind nicht genannt, Auswirkungen auf OT oder die Wasserversorgung sind nicht berichtet, und in DACH ist kein Opfer bekannt.

Früherer Stand: Nach 24 Stunden (03.10.2026 07:34)

Wissen 44 % · wahrscheinlich 18 % · nicht bekannt 38 %

Laut Symantec (Bericht vom 01.10.2026) hat die China-nahe Gruppe Longlegs, auch Storm-2603 genannt, in rund zwei Monaten mindestens vier Organisationen in portugiesisch- und spanischsprachigen Ländern angegriffen: einen Wasserversorger, einen Telekommunikationsanbieter, eine regionale Behörde und eine Universität. Die Angreifer kamen über ungepatchte On-Premises-SharePoint-Server hinein. In einem dokumentierten Fall schalteten sie die Schutzsoftware auf mindestens 40 Hosts ab und verteilten Warlock danach über SYSVOL auf mindestens 33 Hosts. Die Opfer sind bis heute nicht genannt. Keine Quelle berichtet bisher von Auswirkungen auf OT, Leittechnik oder die Wasserversorgung, und in DACH ist kein Opfer bekannt.

Früherer Stand: Nach 72 Stunden (04.10.2026 08:06)

Wissen 47 % · wahrscheinlich 18 % · nicht bekannt 35 %

Symantec meldete am 01.10.2026, dass die China-nahe Gruppe Longlegs (Storm-2603, auch Gold Salem) in rund zwei Monaten mindestens vier Organisationen mit Warlock-Ransomware angegriffen hat: einen Wasserversorger, einen Telekommunikationsanbieter, eine regionale Behörde und eine Universität in portugiesisch- und spanischsprachigen Ländern. Die Angreifer kamen über ungepatchte On-Premises-SharePoint-Server hinein, schalteten dann die Schutzsoftware aus und verteilten die Ransomware über das Active Directory (SYSVOL). Bis heute (04.10.2026) sind weder die Namen der Opfer noch Auswirkungen auf OT oder die Wasserversorgung öffentlich, und in DACH ist kein Opfer bekannt.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.