THREAT ADVISORY | 04. SEPTEMBER 2026

Rhysida: Was der Angriff auf Berlin für Ihr Unternehmen bedeutet

Am 4. September 2026 hat die Ransomware-Gruppe Rhysida 5,8 Terabyte Daten aus dem Berliner Landesnetz veröffentlicht. Dieses Advisory beschreibt den Akteur, seine seit 2023 unveränderte Angriffskette und die Maßnahmen, die jetzt Vorrang haben.

Zielgruppe

Regulierte Unternehmen und öffentliche Stellen (DACH), CISO, IT-Leitung, SOC

Regulatorik

NIS2 · DORA · ISO 27001:2022 · KRITIS

Klassifizierung

TLP:CLEAR, Weitergabe erlaubt

Quellen

TIRAS-Datenbestand, CISA, Fortinet, Check Point, Trend Micro, Gen Digital, Microsoft, IBM X-Force, Expel, Senat Berlin

Stand

04. September 2026, 18:00 Uhr

FÜNF SOFORTMASSNAHMEN

1

MFA für jeden Remote-Zugang

VPN, Terminal-Server, RDP-Gateways, Webmail und Dienstleister-Zugänge, ohne Ausnahme für die Domänenanmeldung.

CIS Control 6

2

Kommandozeilen- und PowerShell-Logging

Event 4688 mit Kommandozeile, Script-Block-Logging, Sysmon, zentrale Vorhaltung 180 Tage.

CIS Control 8

3

Volumenalarm am Internet-Uplink

Uploads zu Azure Blob und MEGA nur für definierte Systeme, Alarm bei ungewöhnlichem Ausgangsvolumen.

CIS Control 13

4

SSH auf ESXi abschalten

Management-Netz und Backup-Konsolen vom Client-Netz trennen, Endpoint-Schutz auf Hypervisoren.

CIS Control 4, 12

5

Klartext-Passwörter aufspüren

Fileshares und SharePoint nach Passwortlisten durchsuchen, Passwort-Manager erzwingen, Dienstkonten in Tresore.

CIS Control 5

Management Summary

Was ist passiert?

Zwischen dem 7. und 12. August 2026 flossen 5,79 TB Daten aus zwei Berliner Senatsverwaltungen ab, unbemerkt. Am 14. August wurde der Zugriff entdeckt und die Verbindung zum Landesnetz gekappt. Am 28. August forderte die Ransomware-Gruppe Rhysida 30 Bitcoin. Berlin zahlte nicht. Am 4. September um etwa 16:35 Uhr veröffentlichte Rhysida rund 5,8 TB im Darknet, darunter Personalakten, Verträge, Bundesratsdokumente und Schwachstellenanalysen der Trinkwasserversorgung.

Was bedeutet das?

Rhysida ist seit Mai 2023 aktiv und hat 281 Opfer auf seiner Leak-Site gelistet, 17 davon in DACH. Die Angriffskette ist seit drei Jahren dokumentiert: gültige Zugangsdaten gegen VPN oder Terminal-Server ohne MFA, Aufklärung mit Bordmitteln, Diebstahl der Domänen-Datenbank, PsExec, Exfiltration in Cloud-Speicher, dann Verschlüsselung. Seit 2024 kommen gefälschte Microsoft-Teams-Installer über Suchmaschinen-Anzeigen hinzu. Verwaltung, Gesundheit und Bildung sind die häufigsten Ziele.

Was müssen wir tun?

Sofort: die fünf Maßnahmen oben auf dieser Seite. Jede davon unterbricht eine Phase der Angriffskette, die Rhysida seit 2023 unverändert nutzt. **Diese Woche:** Backup-Wiederherstellung inklusive Hypervisor testen, Isolationsplan mit Stundenziel üben, Fernwartungssoftware auf eine Allowlist setzen, Leak-Site-Monitoring einrichten.

Warum dieses Advisory regulatorisch relevant ist

NIS2 (Art. 21 Abs. 2), DORA (Kapitel II) und ISO 27001:2022 (A.5.7 Threat Intelligence) verlangen den systematischen Umgang mit Bedrohungsinformationen. Dieses Advisory trägt zur Nachweisführung bei. Rhysida greift die Sektoren an, die diese Regelwerke erfassen: Verwaltung, Gesundheit, Wasser, Verkehr

und Finanzen. Der Berliner Fall zeigt zudem, dass eine nicht regulierte Landesverwaltung als Lieferkette zu KRITIS-Betreibern wirkt.

Die Lage

Der Angriff auf das Berliner Landesnetz ist der größte bekannte Datenabfluss aus einer deutschen Landesverwaltung. Betroffen sind die Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen sowie die Senatsverwaltung für Mobilität, Verkehr, Klimaschutz und Umwelt. Nach Angaben von Digitalstaatssekretär Florian Hauer lief der Abfluss vom 7. bis 12. August, entdeckt wurde er am 14. August. Am 1. September bestätigte Senatssprecherin Christine Richter, dass auch Passwörter abgeflossen sind, die im Klartext in Office-Dateien lagen. Rund 12.000 Systeme des Landes wurden geprüft.

Rhysida behauptet, 1,44 Millionen Dateien erbeutet zu haben: über 46.500 Verträge, über 5.000 Personalakten, Gehaltsabrechnungen, Bußgeldverfahren, vertrauliche Dokumente aus Bundesratsausschüssen, Schwachstellenanalysen zur Berliner Trinkwasserversorgung sowie Klartext-Zugänge zu Verwaltungsdatenbanken und Zahlungsdienstleistern. Der Regierende Bürgermeister Kai Wegner erklärte: „Das Land Berlin wird sich nicht erpressen lassen." Landeskriminalamt und BSI ermitteln. Der Erstzugang wurde nicht bekannt gegeben.

Bereits am 21. Mai 2026 hatte Rhysida die Landeshauptstadt Stuttgart auf seiner Leak-Site gelistet und 5 Bitcoin gefordert, etwa 333.000 Euro. Es kam zu keiner Verschlüsselung; die Stadt erklärte, sie habe keine Hinweise auf einen Cyber-Vorfall. Ein Leak-Site-Eintrag ist eine Behauptung der Täter, kein bestätigter Vorfall. Für Deutschland zählt der TIRAS-Datenbestand neun Rhysida-Einträge seit Juni 2023, für die Schweiz sechs, für Österreich zwei.

Chronologie Berlin

07.–12.08.	Datenabfluss von 5,79 TB, unbemerkt
14.08.	Entdeckung; beide Senatsverwaltungen vom Landesnetz getrennt
17.08.	Öffentliche Bekanntgabe des Vorfalls
24.08.	Systeme wieder angebunden
28.08.	Bekennerschreiben, Forderung 30 BTC (rund 2 Mio. Euro), Sondersitzung des Senats
01.09.	Senat bestätigt Abfluss von Klartext-Passwörtern aus Office-Dateien
04.09. 15:35	Ultimatum abgelaufen; rund eine Stunde später 5,8 TB im Darknet veröffentlicht

Der Akteur

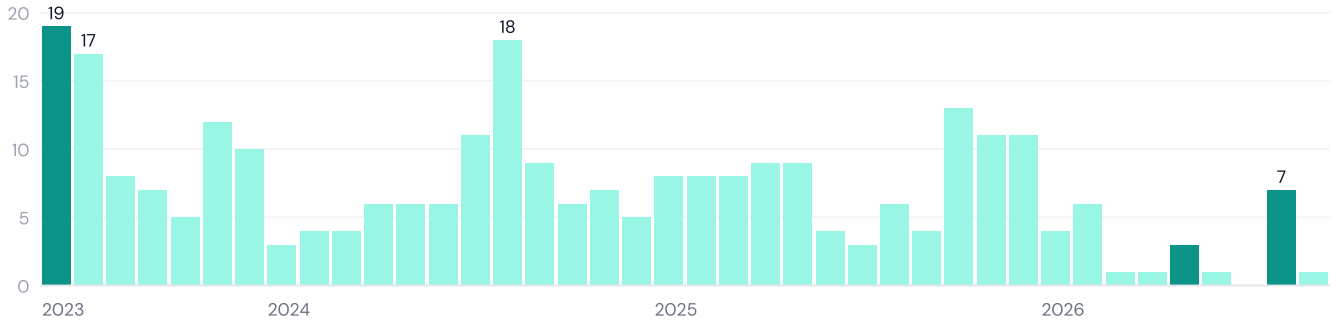
Rhysida ist eine Ransomware-as-a-Service-Operation, die im Mai 2023 auftauchte und seit dem 5. Juni 2023 eine Leak-Site im Tor-Netz betreibt. Die Gruppe stiehlt Daten, verschlüsselt Systeme und versteigert das Diebesgut mit Mindestgebot und siebentägiger Frist. Bleibt die Auktion ohne Käufer, wird ein Großteil veröffentlicht. Die Herkunft ist unbekannt. Microsoft ordnet den aktivsten Affiliate als Vanilla Tempest ein, bei anderen Herstellern als Vice Society oder VICE SPIDER bekannt. IBM X-Force bewertet die seit September 2024 aktive Gruppe Interlock als wahrscheinliche Abspaltung mit geteilter Malware-Basis.

281
Opfer auf der Leak-Site seit Juni 2023

17
davon in Deutschland, Österreich, Schweiz

94
Einträge im Jahr 2025, das stärkste Jahr

52
dokumentierte ATT&CK-Techniken in TIRAS



Leak-Site-Einträge pro Monat, Juni 2023 bis September 2026. Jahressummen: 2023 78, 2024 85, 2025 94, 2026 bis 4. September 24. Hervorgehoben: Startmonat sowie die Monate mit Stuttgart und Berlin. Quelle: TIRAS, ransomware.live-Sync vom 2. September 2026.

Typ	Ransomware-as-a-Service, Doppelerpressung (Verschlüsselung plus Auktion gestohlener Daten)
Aktiv seit	Mai 2023; Leak-Site seit 5. Juni 2023; letzte Aktion 4. September 2026
Zielsektoren TIRAS, 168 Einträge mit Sektor	Gesundheitswesen 23 %, öffentliche Verwaltung 18 %, Bildung 12 %, Unternehmensdienstleistungen 12 %, Fertigung 11 %, Technologie 5 %, Transport 5 %, Finanzen 4 %
Zielländer TIRAS, 212 Einträge mit Land	USA 52 %, Kanada 8 %, Großbritannien 5 %, Deutschland 4 %, Australien 4 %, Italien 4 %, Schweiz 3 %
Verwandte Akteure	Vanilla Tempest / Vice Society (Affiliate, Microsoft), Interlock (Abspaltung, IBM X-Force), Initial Access Broker TAG-124 und Gootloader
Bekannte Opfer	Chilenische Armee (05/2023), British Library (10/2023), Insomniac Games (12/2023), Stadt Columbus (07/2024), Port of Seattle (08/2024), Maryland Department of Transportation (09/2025), Landeshauptstadt Stuttgart (05/2026), Land Berlin (08/2026)

Bedrohungsstufe DACH	HOCH. Zwei deutsche Verwaltungen in vier Monaten; der Zieltyp deckt sich mit NIS2- und KRITIS-Kreisen

Fähigkeit mittel, Ressourcen hoch: Rhysida nutzt keine Zero-Day-Schwachstellen. In keinem Incident-Response-Bericht ist eine ausgenutzte CVE belegt; die in Sekundärquellen kursierende Zerologon-Behauptung hat keinen Primärbeleg. Dafür investiert die Gruppe in Infrastruktur: über 40 Code-Signing-Zertifikate in einer einzigen Kampagne 2025, über 200 von Microsoft widerrufene Zertifikate im Oktober 2025.

Die Angriffskette

Zusammengeführt aus der CISA-Warnung AA23-319A, der Incident-Response-Analyse von Fortinet zu einem Vorfall im Juli 2023, Check Point Research, Trend Micro und Microsoft. Die Kette ist über drei Jahre stabil geblieben, nur der Erstzugang hat sich verbreitert.

Phase	Vorgehen	Beleg
Erstzugang	Gültige Zugangsdaten gegen VPN-Appliances, RDP und Terminal-Server ohne MFA (SonicWall-VPN im Fortinet-Fall, Terminal-Server bei der British Library). Phishing. Seit 2024 gefälschte Microsoft-Teams-Installer über Bing-Anzeigen und SEO-Poisoning, die den OysterLoader ausliefern; seit 2025 zusätzlich Gootloader. Bei Berlin ist der Erstzugang nicht bekannt gegeben.	CISA, Fortinet, British Library, Trend Micro, Expel, Microsoft
Aufklärung	Bordmittel wie `ipconfig`, `whoami`, `nltest`, `net group "domain admins" /domain`, dazu Advanced Port Scanner, PowerView und Cobalt Strike. Ein PowerShell-Skript durchsucht Browser-Verläufe nach Backup- und NAS-Adressen.	CISA, Fortinet
Zugangsdaten	Diebstahl der Active-Directory-Datenbank mit `ntdsutil` oder Impacket, LSASS-Speicherabzug per Task-Manager oder ProcDump, Zugriff auf die SAM-Datenbank über Remote Registry. In Berlin lagen Passwörter im Klartext in Office-Dateien.	CISA, Check Point, Fortinet, Senat Berlin
Seitwärtsbewegung	RDP zum Domänencontroller, PsExec mit SYSTEM-Rechten, WinRM, WMIC. Auf ESXi-Hosts per SSH: eine Linux-Variante wurde mit WinSCP hochgeladen und auf zwei Hypervisoren ohne Endpoint-Schutz ausgeführt, bevor die Windows-Variante folgte.	Fortinet, Check Point
Persistenz	AnyDesk als zweiter Zugang, SOCKS-Backdoor in PowerShell, Go-DLL über rundll32 mit Autostart-Task, PortStarter-Backdoor. Firewall-Regel mit Tarnnamen „Windows Update“.	Fortinet, Check Point
Verschleierung	Löschen der Windows-Event-Logs, des PowerShell-Verlaufs und der RDP-Spuren, PowerShell mit verstecktem Fenster, Tarnung als `conhost.exe`, Skript zum Abschalten von Sicherheitsdiensten, signierte Schadsoftware.	CISA, Check Point, Trend Micro, Expel
Exfiltration	Eigenes Go-Werkzeug mit konfigurierbaren Dateimustern, WinSCP, MegaSync, AZCopy und Storage Explorer in Azure-Blob-Container. British Library: 440 GB in einer Nacht. Berlin: 5,79 TB in fünf Tagen. Beides unbemerkt.	Fortinet, CISA, British Library, Senat Berlin

Wirkung	Löschen der Schattenkopien, Verteilung des Encryptors per Batch-Skript nach `C:\Windows\Temp`. Dateien werden mit AES-256-CTR verschlüsselt, der Schlüssel mit RSA-4096; Dateien über 1 MB nur teilweise, damit es schnell geht. Endung `.rhysida`, Lösegeldnote `CriticalBreachDetected.pdf` in jedem Ordner. Die Note gibt sich als „Cybersecurity Team Rhysida“ aus.	CISA, Gen Digital, Trend Micro, Fortinet
Erpressung	Auktion auf der Tor-Leak-Site mit Mindestgebot und sieben Tagen Frist. Forderungen: Berlin 30 BTC, Stuttgart 5 BTC, Port of Seattle 100 BTC, Insomniac Games 50 BTC. Ein 2024 veröffentlichter Decryptor gilt nur für die damaligen Windows-Varianten.	dpa, heise, Kookmin/KISA

TTP-Mapping und Gegenmaßnahmen

Die zehn Techniken, die in der Kette am frühesten sichtbar und am besten erkennbar sind. Die Spalte Sigma zeigt, wie viele fertige Erkennungsregeln der SigmaHQ-Community in TIRAS für die Technik vorliegen; die Log-Quelle ist die Mindestvoraussetzung. Die CIS-Controls benennen die Maßnahme mit dem größten Hebel.

Technik	Warum relevant	Erkennung	Log-Quelle	Sigma	Gegenmaßnahme
T1078 Valid Accounts	Der häufigste Erstzugang: gestohlene Zugangsdaten gegen VPN und Terminal-Server ohne zweiten Faktor.	Anmeldungen ohne MFA, neue Geolokation, bekannte Infostealer-Credentials	VPN-Gateway, IdP	51	CIS Control 6: Phishing-resistente MFA für alle Remote-Zugänge
T1003.003 NTDS	Mit der Active-Directory-Datenbank hat der Angreifer jede Identität im Unternehmen.	`ntdsutil "ac i ntds" ifm`, secretsdump, ProcDump auf lsass, Remote-Registry auf SAM	Sysmon 1/10/11, Security 4688	24	CIS Control 5: Tiering privilegierter Konten, LSASS-Schutz
T1087.002 / T1482 Account und Domain Trust Discovery	Die Abfolge aus `whoami, nltest, net group` dauert wenige Minuten und kommt im Normalbetrieb nicht vor.	Mehrere Discovery-Befehle in unter 5 Minuten von einem Host; Start eines Portscanners	Security 4688 mit Kommandozeile	36	CIS Control 8: Kommandozeilen-Auditing, zentrale Logs
T1021.001 / T1569.002 RDP, PsExec	Seitwärtsbewegung zum Domänencontroller und Verteilung des Encryptors.	Dienstinstallation PSEXESVC oder Zufallsnamen, `PsExec -i -s`, WMIC-Remote-Prozesse	Security 7045, 4624 Typ 3	16	CIS Control 12: Segmentierung, RDP nur über Jump-Host
T1685.005 / T1490 Event-Logs löschen, Schattenkopien löschen	Beide Befehle gehen der Verschlüsselung unmittelbar voraus.	`wevtutil cl`, Event 1102/104, `vssadmin Delete Shadows`	Security, System, Sysmon 1	8	CIS Control 8 / 11: Log-Forwarding, unveränderliche Backups
T1219 Remote Access Tools	AnyDesk als zweiter Zugang überlebt Passwort-Resets.	Nicht freigegebene Fernwartungs-Installation, Outbound zu RMM-Relays	Sysmon 1/3, Proxy	6	CIS Control 2: Software-Allowlist für Fernwartung
T1567.002 / T1041 Exfiltration	Der Datenabfluss dauert Tage und ist die Grundlage der Erpressung.	Egress zu blob.core.windows.net oder MEGA, WinSCP/AZCopy von Servern, Volumenanomalie am Uplink	Proxy, NetFlow, DNS	5	CIS Control 13: Egress-Filter, Volumenalarm
T1486 Data Encrypted for Impact	Erkennung in dieser Phase begrenzt den Schaden, verhindert die Erpressung aber nicht mehr.	Batch-Kopie nach C:\Windows\Temp, Massenumbenennung auf .rhysida, CriticalBreachDetected.pdf	Sysmon 1/11, Datei-Audit	16	CIS Control 11: Getestete Offline-Backups inklusive Hypervisor
T1189 / T1553.002 Malvertising, Code Signing	Seit 2024 zweiter Erstzugang: signierte, gefälschte Teams-Installer aus Suchmaschinen-Anzeigen.	Installer für Teams, PuTTY oder Zoom aus Nicht-Hersteller-Domänen nach Werbeklick	Proxy, EDR	–	CIS Control 9 / 14: Download-Beschränkung, Werbefilter, Awareness

T1021.004 SSH auf ESXi	Hypervisor-Verschlüsselung trifft alle VMs auf einmal.	SSH-Sitzungen zu ESXi von Workstations, Datei-Uploads auf Hypervisoren	ESXi-Auth-Log, Sysmon 3	5 CIS Control 4 / 12: SSH auf ESXi deaktivieren, Management-Netz trennen

Ohne Kommandozeilen-Auditing (Event 4688 mit Prozess-Kommandozeile) sind die Erkennungen für Credential Dumping, Aufklärung und Verschlüsselung blind. Im Fortinet-Fall verhinderte fehlendes Script-Block-Logging die Rekonstruktion der PowerShell-Aktivität.

Was das für Ihr Unternehmen bedeutet

Thema	Bewertung
Verwaltung ist Lieferkette	Die Berliner Landesverwaltung unterliegt nicht der BSI-KritisV. Trotzdem lagen dort Schwachstellenanalysen der Wasserversorgung, Bundesratsdokumente und Zahlungszugänge. Wer Daten mit Behörden, Dienstleistern oder Verbänden teilt, muss deren Sicherheitsniveau in die eigene Risikobewertung einbeziehen (NIS2 Art. 21 Abs. 2 lit. d, ISO 27001 A.5.19 bis A.5.22).
Verweildauer ist das Problem, nicht die Verschlüsselung	In Berlin blieb der Abfluss fünf Tage unbemerkt, bei der British Library flossen 440 GB in einer Nacht ab. Rhysida verschlüsselt erst, nachdem die Daten weg sind. Eine Erkennung in der Aufklärungs- oder Exfiltrationsphase verhindert die Erpressung; eine Erkennung bei der Verschlüsselung nicht mehr.
MFA-Lücken auf der Domäne	Die British Library hatte MFA für Cloud-Dienste, aber nicht für den Terminal-Server auf der Domäne. Über diesen Server kam der Angreifer hinein. Prüfen Sie jeden Remote-Zugang, der direkt in das Active Directory führt: VPN, RDP-Gateways, Citrix, Terminal-Server, Wartungszugänge von Dienstleistern.
Hypervisoren sind Ziel	Rhysida verschlüsselt ESXi-Hosts per SSH, bevor Windows-Systeme an der Reihe sind. Im Fortinet-Fall verhinderten restriktive vSphere- und Veeam-Berechtigungen die flächendeckende Verschlüsselung. Management-Netz, SSH-Zugang und Backup-Konsolen gehören vom Client-Netz getrennt.
Gefälschte Software aus Suchmaschinen	Seit 2024 kommt der Erstzugang auch über Bing- und Google-Anzeigen für gefälschte Teams-, PuTTY- und Zoom-Installer, gültig signiert. Wer Mitarbeitenden erlaubt, Software selbst herunterzuladen, braucht Download-Beschränkungen und Werbefilter.
Leak-Site vor Incident	Bei Stuttgart und Columbus erschien der Leak-Site-Eintrag, bevor der Vorfall intern erkannt oder bestätigt war. Leak-Site-Monitoring liefert oft den ersten Hinweis.

Konkrete Gegenmaßnahmen, sofort umsetzbar

Rhysida nutzt keine Zero-Days. Die Gruppe nutzt fehlende MFA, fehlendes Logging, ungeschützte Hypervisoren und Passwörter in Word-Dateien. Das sind lösbare Probleme, wenn man weiß, wo man anfangen muss.

Maßnahme	CIS Control	Umsetzung	Verhindert
MFA für alle Remote-Zugänge	Control 6	Phishing-resistente MFA (FIDO2/WebAuthn) für VPN, Terminal-Server, RDP-Gateways, Webmail und Dienstleister-Zugänge. Conditional-Access-Regeln. Keine Ausnahme für die Domänenanmeldung.	Erstzugang
Kommandozeilen- und PowerShell-Logging	Control 8	Event 4688 mit Kommandozeile, PowerShell Modul-, Script-Block- und Transkriptions-Logging, Sysmon. Zentrale Vorhaltung 180 Tage. Ohne diese Logs sind sechs der zehn Erkennungen aus Abschnitt 4 blind.	Unentdeckte Aufklärung
Fernwartung auf Allowlist	Control 2	Nur freigegebene, signierte Fernwartungssoftware. AnyDesk, TeamViewer und ähnliche Werkzeuge ohne Freigabe blockieren, Outbound zu RMM-Relays überwachen.	Persistenz
Egress-Kontrolle und Volumenalarm	Control 13	Uploads zu Cloud-Speichern (Azure Blob, MEGA) nur für definierte Systeme. Alarm bei ungewöhnlichem Ausgangsvolumen am Internet-Uplink, besonders nachts und am Wochenende.	Exfiltration
Hypervisor härten	Control 4 / 12	SSH auf ESXi deaktivieren oder auf Management-Netz beschränken. vSphere- und Backup-Konsolen nur über Jump-Host. Endpoint-Schutz auch auf Hypervisoren.	Verschlüsselung aller VMs
Klartext-Passwörter beseitigen	Control 5	Fileshares und SharePoint nach Passwortlisten durchsuchen, Passwort-Manager erzwingen, Dienstkonten in Tresore überführen.	Ausweitung nach Erstzugang
Backup-Strategie testen	Control 11	Offline- oder unveränderliche Backups, Wiederherstellung inklusive Hypervisor und Domänencontroller testen. Die British Library konnte Daten nicht zurückspielen, weil Server zerstört und Altanwendungen nicht neu installierbar waren.	Ausfalldauer
Isolationsplan mit Stundenziel	Control 17	Wer darf welche Netzsegmente trennen, in welcher Zeit, mit welcher Freigabe. Tabletop-Übung mit dem Berlin-Szenario: Verdacht auf Abfluss, keine Verschlüsselung, Entscheidung in unter zwei Stunden.	Verweildauer

Downloads und Werbung filtern	Control 9 / 14	Software nur aus Hersteller-Domänen oder dem Software-Portal. Werbefilter oder DNS-Filter im Browser. Awareness-Hinweis: gefälschte Teams-Installer.	Malvertising-Zugang
Leak-Site-Monitoring	Control 17	Eigene Organisation, Tochtergesellschaften und wichtige Dienstleister auf Ransomware-Leak-Sites beobachten. Ein Eintrag erscheint oft, bevor der Vorfall intern bekannt ist.	Späte Erkennung

Anhang A: Indikatoren

Auswahl aus CISA AA23-319A, Fortinet und ransomware.live. Host-Artefakte sind stabiler als Hashes und IP-Adressen; die Encryptor-Binaries werden pro Opfer neu gebaut, die IP-Adressen stammen aus dem Sommer 2023.

Indikator	Bedeutung	Quelle
`*.rhysida`	Endung verschlüsselter Dateien	alle
`CriticalBreachDetected.pdf`	Lösegeldnote in jedem Verzeichnis	alle
`C:\Users\Public\bg.jpg`	Gesetztes Wallpaper	Talos
`C:\Windows\Temp\*.exe · S_1.bat · S_2.bat`	Staging und Verteilung des Encryptors	CISA
`C:\in · C:\out · C:\out\PSTools.zip`	Exfiltrations-Staging und Werkzeugablage	CISA
`temp_l0gs`	Sicherungspfad des NTDS-Dumps, identisch mit Vice Society	Check Point
`C:\Users\Public\main.dll · iii.bat · Task „System“ ONSTART`	Go-Backdoor mit Persistenz	Fortinet
`ad.ps1 · w.ps1 · DataGrabber1.exe · dob.exe · fury.exe · 67`	Backdoor, Aufklärung, Exfiltration, Encryptor Windows, Encryptor Linux	Fortinet
`conhost.exe SHA-256 6633fa85bb234a75927b23417313e51a4c155e12f71da3959e168851a600b010`	Als conhost getarntes Rhysida-Binary	CISA
`1.ps1 SHA-256 4e34b9442f825a16d7f6557193426ae7a18899ed46d3b896f6e4357367276183`	Bereinigungs- und Ausführungsskript	CISA
`-d <pfad> -sr`	Encryptor-Aufruf mit Selbstlöschung	CISA
`cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet`	Kindprozess des Encryptors auf Servern	Fortinet
`rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad[.]onion`	Leak-Site, aktiv	ransomware.live
`rhysidaeverywhere@onionmail[.]org · rhysidaofficial@onionmail[.]org`	Verhandlungsadressen	CISA
`776c5589[.]schedule[.]newhomessection[.]com`	Gootloader-Domäne	CISA 04/2025
`oij89jiiuguygh.blob.core.windows[.]net · e57thgdfge.blob.core.windows[.]net`	Azure-Blob-Exfiltrationsziele	CISA 04/2025
`5.255.113[.]37:4001 · 5.255.127[.]20:443 · 23.108.57[.]83:443 · 5.255.103[.]7 · 5.226.141[.]196`	C2 und Exfiltration, Juli/August 2023	Fortinet, Check Point

Vollständige Hash-Listen: CISA AA23-319A (über 40 SHA-256) und Cisco Talos. Für die Malvertising-Kampagne pflegt Expel eine Indikatorliste auf GitHub.

Anhang B: Ökosystem und Verbindungen

Vanilla Tempest / Vice Society. Microsoft führt Vanilla Tempest (früher DEV-0832, bei anderen Herstellern VICE SPIDER oder Vice Society) als finanziell motivierten Akteur, der primär Rhysida einsetzt, daneben INC Ransomware. Check Point fand im August 2023 identische Artefakte: den NTDS-Sicherungspfad temp_l0gs, gleiche Firewall-Regelnamen und die PortStarter-Backdoor, während Vice Society seit dem 21. Juni 2023 keine Opfer mehr veröffentlichte. Die CISA-Warnung nennt die Überschneidung ausdrücklich.

Interlock. IBM X-Force bewertet Interlock, aktiv seit September 2024, als wahrscheinliche Abspaltung aus dem Rhysida-Umfeld. Beide nutzen die Supper-Backdoor mit unterschiedlichen Cryptern und teilen Code-Strukturen zwischen NodeSnake, InterlockRAT und Supper.

Zugangsbeschaffung. Der Initial Access Broker TAG-124 lieferte im Mai 2024 den Loader Broomstick für Rhysida und wechselte im September 2024 zu Interlock. Gootloader verschafft beiden Gruppen Zugang. Die Malvertising-Kampagnen liefen Mai bis September 2024 mit sieben Zertifikaten und ab Juni 2025 mit über vierzig; Microsoft erkannte sie Ende September 2025, ordnete sie Vanilla Tempest zu und widerrief Anfang Oktober über 200 Zertifikate, ausgestellt über Microsoft Trusted Signing, SSL.com, DigiCert und GlobalSign.

Wie wir Sie bei der Umsetzung unterstützen können

Dieses Advisory zeigt, wie Rhysida vorgeht und welche Maßnahmen Priorität haben. Die Umsetzung erfordert eine individuelle Bewertung Ihrer Infrastruktur, Ihrer bestehenden Sicherheitsmaßnahmen und Ihrer regulatorischen Anforderungen.

TIRAS: Threat-Informed Resilience & Advisory System

TIRAS übersetzt aktuelle Bedrohungsintelligenz in priorisierte, umsetzbare Maßnahmen, zugeschnitten auf Ihr Unternehmensprofil. Die 52 Rhysida-Techniken in diesem Advisory sind dort mit Erkennungsregeln, Log-Quellen und ISO-27001-Controls verknüpft. Sie sehen, welche Ihrer Log-Quellen die kritischen Erkennungen abdecken, wo Lücken sind und welche Maßnahme den größten Hebel hat.

Bevor Sie in kostenintensive Penetrationstests investieren, hilft TIRAS Ihnen dabei, Ihre Ressourcen gezielt dort einzusetzen, wo die reale Bedrohungslage es erfordert.

Interesse? Kontaktieren Sie uns für ein erstes Gespräch.
kontakt@threat-informed.de | www.threat-informed.de

Quellen: CISA/FBI/MS-ISAC AA23-319A (15.11.2023, aktualisiert 04/2025); Fortinet FortiGuard, Analyzing Rhysida Ransomware Intrusion (11/2023) und Ransomware Roundup Rhysida (08/2023); Check Point Research (08/2023); Trend Micro (08/2023); Gen Digital, Rhysida Ransomware Technical Analysis (26.10.2023); Kim et al., Kookmin University / KISA (02/2024); British Library, Cyber Incident Review (08.03.2024); Microsoft Threat Intelligence (10/2025); Expel, Certified OysterLoader (10/2025); IBM X-Force, Interlock and Rhysida within the ransomware ecosystem; ransomware.live (04.09.2026); Senat Berlin via heise (01.09.2026) und dpa (28.08. und 04.09.2026); heise zu Stuttgart (05/2026). Alle Informationen basieren auf öffentlich verfügbaren Quellen und dem TIRAS-Datenbestand. Leak-Site-Einträge sind Behauptungen der Täter. Opferdaten nur aggregiert.

Dieses Advisory ist Teil unserer Threat Briefings für Unternehmen unter NIS2, DORA und KRITIS in der DACH-Region. TLP:CLEAR, Weitergabe erlaubt.

Glossar

Abkürzung	Bedeutung
ATT&CK	MITRE-Wissensbasis für Angreifertaktiken und -techniken; T-Nummern bezeichnen Techniken

C2	Command and Control: Infrastruktur zur Fernsteuerung kompromittierter Systeme
CIS Controls	Center for Internet Security Controls: priorisierter Maßnahmenkatalog für IT-Sicherheit
ESXi	VMware-Hypervisor, auf dem virtuelle Maschinen laufen
FIDO2	Phishing-resistenter Authentifizierungsstandard
IdP	Identity Provider: zentraler Anmeldedienst, etwa Entra ID
IOC	Indicator of Compromise: technisches Merkmal eines Angriffs
Leak-Site	Tor-Webseite, auf der Erpressergruppen Opfer nennen und Daten veröffentlichen
LOLBin	Living off the Land Binary: legitimes Systemwerkzeug, das Angreifer zweckentfremden
MFA	Multi-Faktor-Authentifizierung
NTDS	Datenbank des Active Directory mit allen Konten und Passwort-Hashes
RaaS	Ransomware-as-a-Service: Betreiber stellt Schadsoftware und Infrastruktur, Affiliates führen Angriffe aus
RMM	Remote Monitoring and Management: Fernwartungssoftware wie AnyDesk
Sigma	Herstellerneutrales Format für Erkennungsregeln; SigmaHQ ist die Community-Sammlung
TLP	Traffic Light Protocol: Kennzeichnung, wie weit Informationen geteilt werden dürfen
TTP	Tactics, Techniques, Procedures: Vorgehensweisen von Angreifern