

THREAT ADVISORY | SEPTEMBER 4, 2026 · VERSION 1.1

Rhysida: What the Attack on Berlin Means for Your Organization

On September 4, 2026, the ransomware group Rhysida published 5.8 terabytes of data from the Berlin state network. This advisory describes the actor, its attack chain, which has remained unchanged since 2023, and the actions that now take priority.

Audience

Regulated companies and public bodies in Germany, Austria and Switzerland, CISOs, heads of IT, SOC

Regulation

NIS2 · DORA · ISO 27001:2022 · KRITIS (German critical infrastructure)

Classification

TLP:CLEAR, sharing permitted

As of

September 7, 2026, version 1.1

Sources

TIRAS data set, BSI, CISA, Fortinet, Check Point, Trend Micro, Gen Digital, Microsoft, IBM X-Force, Expel, Berlin Senate

Changes

Version 1.1 of September 7, 2026. Added: the initial access via the TerminalFix campaign confirmed by the BSI (BITS-B 2026-287419-1032), a sixth immediate action on execution control, three rows in the TTP mapping, the leak site's publication rate and the indicators of the TerminalFix campaign. First version September 4, 2026, 6:00 p.m.

SIX IMMEDIATE ACTIONS

1

MFA for every remote access

VPN, terminal servers, RDP gateways, webmail and service provider access, with no exception for domain login.

CIS Control 6

2

Command line and PowerShell logging

Event 4688 with command line, script block logging, Sysmon, central retention for 180 days.

CIS Control 8

3

Volume alert on the internet uplink

Uploads to Azure Blob and MEGA only for defined systems, alert on unusual outbound volume.

CIS Control 13

4

Disable SSH on ESXi

Separate the management network and backup consoles from the client network, endpoint protection on hypervisors.

CIS Control 4, 12

5

Track down plaintext passwords

Search file shares and SharePoint for password lists, enforce password managers, move service accounts into vaults.

CIS Control 5

6

Restrict PowerShell for standard users

Constrained Language Mode, AppLocker or WDAC, a warning when pasting multi-line commands into Windows Terminal. Awareness: fake captchas.

CIS Control 2, 4, 14 · new in 1.1

Management Summary

What happened?

Between August 7 and 12, 2026, 5.79 TB of data was exfiltrated from two Berlin Senate departments, unnoticed. On August 14, the access was discovered and the connection to the state network was cut. On August 28, the ransomware group Rhysida demanded 30 bitcoin. Berlin did not pay. On September 4 at around 4:35 p.m., Rhysida published around 5.8 TB on the dark web, including personnel files, contracts, Bundesrat documents and vulnerability analyses of the drinking water supply.

What does this mean?

Rhysida has been active since May 2023 and has listed 281 victims on its leak site, 17 of them in Germany, Austria and Switzerland. The attack chain has been documented for three years: initial access via valid credentials against VPN or terminal servers without MFA, since 2024 via fake Teams installers and, as in Berlin, via a command from a fake captcha (TerminalFix). Then reconnaissance with built-in tools, theft of the domain database, PsExec, exfiltration to cloud storage, then encryption. Public administration, healthcare and education are the most frequent targets.

What do we need to do?

Immediately: the six actions above. Each breaks a phase of the attack chain Rhysida has used unchanged since 2023. This week: test backup recovery including the hypervisor, rehearse an isolation plan with a target time in hours, allowlist remote maintenance software, set up leak site monitoring.

Why this advisory matters from a regulatory perspective

NIS2 (Art. 21(2)), DORA (Chapter II) and ISO 27001:2022 (A.5.7 threat intelligence) require the systematic handling of threat information. This advisory contributes to your evidence. Rhysida attacks the sectors these regulations cover: public administration, healthcare, water, transport and finance. The Berlin case also shows that an unregulated state administration acts as part of the supply chain for critical infrastructure operators.

The largest known data exfiltration from a German state administration

The Senate Department for Urban Development, Building and Housing and the Senate Department for Mobility, Transport, Climate Protection and the Environment are affected. According to Florian Hauer, State Secretary for Digital Affairs, the exfiltration ran from August 7 to 12 and was discovered on August 14. On September 1, Senate spokesperson Christine Richter confirmed that passwords stored in plaintext in Office files had also been exfiltrated. Around 12,000 of the state's systems were checked.

Rhysida claims to have stolen 1.44 million files: more than 46,500 contracts, more than 5,000 personnel files, payroll records, administrative fine proceedings, confidential documents from Bundesrat committees, vulnerability analyses of Berlin's drinking water supply and plaintext access credentials for administrative databases and payment service providers. Governing Mayor Kai Wegner stated: "The State of Berlin will not be blackmailed." The State Criminal Police Office and the BSI are investigating.

The BSI described the initial access on September 4 in warning BITS-B 2026-287419-1032 without naming the affected body; heise linked the warning to the Berlin case on September 7. According to this, the attack did not begin with stolen credentials but with a user: a compromised website displayed a fake Cloudflare captcha, copied a PowerShell command to the clipboard and prompted the user to run it in Windows Terminal. The command downloaded a ZIP archive whose malicious code started via DLL sideloading, established persistence via the registry and an hourly task, scouted Active Directory and backup systems and opened a Python reverse tunnel over TLS on port 443. The BSI calls the campaign TerminalFix, an evolution of ClickFix, and attributes the malware used, LoremIpsumLoader, to the group behind Rhysida.

As early as May 21, 2026, Rhysida had listed the state capital Stuttgart on its leak site and demanded 5 bitcoin, around €333,000. There was no encryption; the city stated that it had no indication of a cyber incident. A leak site entry is a claim by the perpetrators, not a confirmed incident. For Germany, the TIRAS data set counts nine Rhysida entries since June 2023, for Switzerland six and for Austria two.

Chronology

Aug. 7 to 12	Exfiltration of 5.79 TB of data, unnoticed
Aug. 14	Discovery; both Senate departments disconnected from the state network
Aug. 17	Public announcement of the incident
Aug. 21	Disruption of benefit payments, around 50,000 households without housing benefit payments (heise)
Aug. 24	Systems reconnected
Aug. 28	Claim of responsibility, demand of 30 BTC (around €2 million), special session of the Senate
Sept. 1	The Senate confirms the exfiltration of plaintext passwords from Office files
Sept. 4, 3:35 p.m.	Ultimatum expired; around an hour later, 5.8 TB published on the dark web
Sept. 4	BSI publishes warning BITS-B 2026-287419-1032 on the TerminalFix campaign, criticality 2 (Yellow)
Sept. 7	heise links the BSI warning to the Berlin case: initial access via a fake captcha, not via stolen credentials

Rhysida: ransomware as a service with auctions instead of negotiation

Rhysida is a ransomware-as-a-service operation that appeared in May 2023 and has run a leak site on the Tor network since June 5, 2023. The group steals data, encrypts systems and auctions off the loot with a minimum bid and a seven-day deadline. If the auction finds no buyer, a large part is published. Its origin is unknown. Microsoft tracks the most active affiliate as Vanilla Tempest, known to other vendors as Vice Society or VICE SPIDER. The BSI lists the group as Vice Spider (also White Nefas, White Hekate, DEV-O832), active since at least mid-2021 and, since June 2023, almost exclusively with Rhysida. IBM X-Force assesses the group Interlock, active since September 2024, as a likely offshoot with a shared malware base.

281

victims on the leak site since June 2023

17

of them in Germany, Austria, Switzerland

94

entries in 2025, the strongest year

52

documented ATT&CK techniques in TIRAS

Type	Ransomware as a service, double extortion (encryption plus auction of stolen data)
Active since	May 2023; leak site since June 5, 2023; last action September 4, 2026
Publication rate	In 92% of cases, being named on the leak site is followed by publication of the data, after 11 days on average (BSI, citing a commercial service provider). Berlin: 7 days.
Leak site entries per year	2023: 78, 2024: 85, 2025: 94, 2026 through September 4: 24. Source: TIRAS, ransomware.live sync of September 2, 2026.
Target sectors (TIRAS, 168 entries with sector)	Healthcare 23%, public administration 18%, education 12%, business services 12%, manufacturing 11%, technology 5%, transport 5%, finance 4%
Target countries (TIRAS, 212 entries with country)	USA 52%, Canada 8%, United Kingdom 5%, Germany 4%, Australia 4%, Italy 4%, Switzerland 3%
Related actors	Vanilla Tempest / Vice Society (affiliate, Microsoft), Interlock (offshoot, IBM X-Force), initial access broker TAG-124 and Gootloader
Known victims	Chilean Army (05/2023), British Library (10/2023), Insomniac Games (12/2023), City of Columbus (07/2024), Port of Seattle (08/2024), Maryland Department of Transportation (09/2025), state capital Stuttgart (05/2026), State of Berlin (08/2026)
Threat level for Germany, Austria and Switzerland: HIGH	Two German administrations in four months; the target type matches the scope of NIS2 and critical infrastructure.

Moderate capability, high resources: Rhysida does not use zero-day vulnerabilities. No incident response report documents an exploited CVE; the Zerologon claim circulating in secondary sources has no primary evidence. Instead, the group invests in infrastructure: more than 40 code signing certificates in a single campaign in 2025, more than 200 certificates revoked by Microsoft in October 2025.

Stable for three years, only initial access has broadened

Compiled from CISA warning AA23-319A, Fortinet's incident response analysis of an incident in July 2023, Check Point Research, Trend Micro, Microsoft and the BSI warning of September 4, 2026. The chain has remained stable for three years; only initial access has broadened.

Attack flow, simplified

Phase	Approach	Evidence
01 Initial access	Valid credentials against VPN appliances, RDP and terminal servers without MFA (SonicWall VPN in the Fortinet case, terminal server at the British Library). Phishing. Since 2024, fake Microsoft Teams installers via Bing ads and SEO poisoning that deliver OysterLoader; since 2025, also Gootloader. In Berlin, according to the BSI, TerminalFix: a fake captcha on a compromised website, the user runs the copied PowerShell command themselves, without a vulnerability and without stolen credentials.	CISA, Fortinet, British Library, Trend Micro, Expel, Microsoft, BSI
02 Reconnaissance	Built-in tools such as ipconfig, whoami, nltest, net group "domain admins" /domain, plus Advanced Port Scanner, PowerView and Cobalt Strike. A PowerShell script searches browser histories for backup and NAS addresses.	CISA, Fortinet
03 Credentials	Theft of the Active Directory database with ntdsutil or Impacket, LSASS memory dump via Task Manager or ProcDump, access to the SAM database via Remote Registry. In Berlin, passwords were stored in plaintext in Office files.	CISA, Check Point, Fortinet, Berlin Senate
04 Lateral movement	RDP to the domain controller, PsExec with SYSTEM privileges, WinRM, WMIC. On ESXi hosts via SSH: a Linux variant was uploaded with WinSCP and executed on two hypervisors without endpoint protection before the Windows variant followed.	Fortinet, Check Point
05 Persistence	AnyDesk as a second way in, SOCKS backdoor in PowerShell, Go DLL via rundll32 with an autostart task, PortStarter backdoor. Firewall rule with the disguise name "Windows Update". TerminalFix: registry Run entry with a random name, hourly task, hidden directories under ProgramData, Python reverse tunnel over TLS 443 and WebSocket, whose commands, according to the BSI, may not be logged.	Fortinet, Check Point, Microsoft, BSI
06 Defense evasion	Deletion of the Windows event logs, the PowerShell history and RDP traces, PowerShell with a hidden window, disguise as conhost.exe, a script to disable security services, signed malware. TerminalFix: DLL sideloading via the signed LockScreenContentServer.exe, malicious code hidden in PNG images.	CISA, Check Point, Trend Micro, Expel, Microsoft
07 Exfiltration	Custom Go tool with configurable file patterns, WinSCP, MegaSync, AZCopy and Storage Explorer into Azure Blob containers. British Library: 440 GB in one night. Berlin: 5.79 TB in five days. Both went unnoticed.	Fortinet, CISA, British Library, Berlin Senate

O8 Impact	Deletion of shadow copies, distribution of the encryptor via CISA, Gen Digital, batch script to C:\Windows\Temp. Files are encrypted with Trend Micro, AES-256-CTR and the key with RSA-4096; files over 1 MB are Fortinet only partially encrypted to speed things up. Extension .rhysida, ransom note CriticalBreachDetected.pdf in every folder. The note poses as the "Cybersecurity Team Rhysida".
O9 Extortion	Auction on the Tor leak site with a minimum bid and a seven- dpa, heise, day deadline. Demands: Berlin 30 BTC, Stuttgart 5 BTC, Port of Kookmin/KISA Seattle 100 BTC, Insomniac Games 50 BTC. A decryptor published in 2024 only works for the Windows variants of that time.

The ten techniques that become visible earliest

The thirteen techniques in the chain that become visible earliest and are easiest to detect. The Sigma column shows how many ready-made detection rules from the SigmaHQ community are available in TIRAS for the technique; the log source is the minimum requirement. The CIS Controls name the countermeasure with the greatest leverage.

Technique	Why it matters	Detection and log source	Sigma	Countermeasure
T1078 Valid Accounts	The most common initial access: stolen credentials against VPN and terminal servers without a second factor.	Logons without MFA, new geolocation, known infostealer credentials. Log: VPN gateway, IdP	51	CIS Control 6: phishing-resistant MFA for all remote access

T1024.004 Malicious Copy and Paste	The Berlin PowerShell as a child process 6 initial ac- of WindowsTerminal.exe or ex- cess: the plorer.exe with a download user runs command (iwr, irm, -enc), ZIP the com- extraction to ProgramData. mand from Log: Security 4688 with com- the fake mand line, PowerShell 4104 captcha them- selves. MFA does not help here.	CIS Control 2 / 4: Constrained Language Mode, AppLocker or WDAC, terminal warning when pasting
T1003.003 NTDS	With the ntdsutil "ac i ntds" ifm, se- 24 Active cretdump, ProcDump on Directory lsass, Remote Registry on SAM. database, Log: Sysmon 1/10/11, Security the adver- 4688 sary has every identity in the company.	CIS Control 5: tier- ing of privileged accounts, LSASS protection
T1087.002 / T1482 Account and Domain Trust Discovery	The se- Several discovery commands 36 quence of within 5 minutes from one whoami, host; start of a port scanner. nltest and Log: Security 4688 with com- net group mand line takes a few minutes and does not occur in normal operations.	CIS Control 8: command line au- diting, central logs
T1021.001 / T1569.002 RDP, PsExec	Lateral Service installation PSEXESVC 16 movement or random names, PsExec -i - to the do- s, WMIC remote processes. main con- Log: Security 7045, 4624 type troller and 3 distribu- tion of the encryptor.	CIS Control 12: segmentation, RDP only via jump host

T1685.005 / T1490 Clearing event logs, deleting shadow copies	Both commands immediately precede encryption.	wevtutil cl, event 1102/104, vs-admin Delete Shadows. Log: Security, System, Sysmon 1	8	CIS Control 8 / 11: log forwarding, immutable backups
T1219 Remote Access Tools	AnyDesk as a second way in survives password resets.	Unapproved remote maintenance installation, outbound connections to RMM relays. Log: Sysmon 1/3, proxy	6	CIS Control 2: software allowlist for remote maintenance
T1574.002 / T1027.003 DLL sideloading, steganography	The loader runs under a signed Windows file and fetches its stages as images.	LockScreenContentServer.exe outside System32, dui70.dll next to the EXE, PNG downloaded by PowerShell. Log: Sysmon 1/7/11, EDR	5	CIS Control 10: ASR rules, application control
T1572 / T1547.001 Reverse tunnel, Run key	The tunnel is the persistent access through which the rest of the chain runs.	pythonw.exe from ProgramData with a persistent TLS connection to an unknown domain on 443, new Run key and hourly task. Log: Sysmon 3/13, Security 4698, proxy	24 / 38	CIS Control 13 / 4: outbound only via proxy, no Python runtime without approval
T1567.002 / T1041 Exfiltration	The data outflow takes days, and is the basis for extortion.	Egress to blob.core.windows.net or MEGA, WinSCP/AZCopy from servers, volume anomaly on the uplink. Log: proxy, NetFlow, DNS	5	CIS Control 13: egress filtering, volume alert
T1486 Data Encrypted for Impact	Detection in this phase limits the damage but no longer prevents extortion.	Batch copy to C:\Windows\Temp, mass renaming to .rhysida, CriticalBreachDetected.pdf. Log: Sysmon 1/11, file audit	16	CIS Control 11: tested offline backups including the hypervisor

T1189 / T1553.002 Malvertising, code signing	Second initial access vector since 2024: signed, fake Teams installers from search engine ads.	Installers for Teams, PuTTY or Zoom from non-vendor domains after an ad click. Log: proxy, EDR	CIS Control 9 / 14: download restrictions, ad filters, awareness
T1021.004 SSH on ESXi	Hypervisor encryption hits all VMs at once.	SSH sessions to ESXi from 5 workstations, file uploads to hypervisors. Log: ESXi auth log, Sysmon 3	CIS Control 4 / 12: disable SSH on ESXi, separate the management network

Without command line auditing (event 4688 with the process command line), the detections for credential dumping, reconnaissance and encryption are blind. In the Fortinet case, missing script block logging prevented the reconstruction of the PowerShell activity.

Six lessons from Berlin, Stuttgart and the British Library

Public administration is part of the supply chain

The Berlin state administration is not subject to the German critical infrastructure ordinance (BSI-KritisV). Nevertheless, it held vulnerability analyses of the water supply, Bundesrat documents and payment credentials. Anyone who shares data with authorities, service providers or associations must include their security level in their own risk assessment (NIS2 Art. 21(2)(d), ISO 27001 A.5.19 to A.5.22).

Dwell time is the problem, not encryption

In Berlin, the exfiltration went unnoticed for five days; at the British Library, 440 GB left in one night. Rhysida only encrypts after the data is gone. Detection in the reconnaissance or exfiltration phase prevents extortion; detection at encryption no longer does.

MFA gaps on the domain

The British Library had MFA for cloud services but not for the terminal server on the domain. That server is how the adversary got in. Check every remote access that leads directly into Active Directory: VPN, RDP gateways, Citrix, terminal servers, service provider maintenance access.

The user is the initial access

In Berlin, there was neither a vulnerability nor a stolen password. An employee ran a command that a website presented to them. MFA and patch levels do not help against this. What helps: standard users are not allowed to run arbitrary PowerShell commands, Windows Terminal warns when multi-line commands are pasted, and awareness training shows fake captchas, not just fake invoices.

Hypervisors are a target	Rhysida encrypts ESXi hosts via SSH before Windows systems are next. In the Fortinet case, restrictive vSphere and Veeam permissions prevented widespread encryption. The management network, SSH access and backup consoles belong separated from the client network.
Fake software from search engines	Since 2024, initial access has also come via Bing and Google ads for fake Teams, PuTTY and Zoom installers with valid signatures. If you allow employees to download software themselves, you need download restrictions and ad filters.
Leak site before incident	In Stuttgart and Columbus, the leak site entry appeared before the incident had been detected or confirmed internally. Leak site monitoring often provides the first indication.

Implementable immediately, because Rhysida needs no zero-days

Rhysida does not use zero-days. The group exploits missing MFA, missing logging, unprotected hypervisors, passwords in Word files and users who are allowed to run any command. These are solvable problems if you know where to start.

Action	CIS Control	Implementation	Prevents
MFA for all remote access	Control 6	Phishing-resistant MFA (FIDO2/WebAuthn) for VPN, terminal servers, RDP gateways, webmail and service provider access. Conditional access rules. No exception for domain login.	Initial access
Command line and PowerShell logging	Control 8	Event 4688 with command line, PowerShell module, script block and transcription logging, Sysmon. Central retention for 180 days. Without these logs, seven of the thirteen detections from the TTP mapping are blind.	Undetected reconnaissance
Restrict PowerShell and execution	Control 2 / 4	Constrained Language Mode for standard users, AppLocker or Windows Defender Application Control, ASR rules against script downloads, Windows Terminal warning when pasting multi-line commands. Separate accounts and workstations for administrators.	TerminalFix initial access
Remote maintenance on an allowlist	Control 2	Only approved, signed remote maintenance software. Block AnyDesk, TeamViewer and similar tools without approval, monitor outbound connections to RMM relays.	Persistence

Egress control and volume alert	Control 13	Uploads to cloud storage (Azure Blob, MEGA) only for defined systems. Alert on unusual outbound volume on the internet uplink, especially at night and on weekends.	Exfiltration
Harden the hypervisor	Control 4 / 12	Disable SSH on ESXi or restrict it to the management network. vSphere and backup consoles only via jump host. Endpoint protection on hypervisors as well.	Encryption of all VMs
Eliminate plaintext passwords	Control 5	Search file shares and SharePoint for password lists, enforce password managers, move service accounts into vaults.	Escalation after initial access
Test the backup strategy	Control 11	Offline or immutable backups, test recovery including the hypervisor and domain controller. The British Library could not restore data because servers were destroyed and legacy applications could not be reinstalled.	Duration of the outage
Isolation plan with a target time in hours	Control 17	Who may disconnect which network segments, within what time, with which approval. Tabletop exercise with the Berlin scenario: suspected exfiltration, no encryption, decision in under two hours.	Dwell time
Filter downloads and ads	Control 9 / 14	Software only from vendor domains or the software portal. Ad filters or DNS filters in the browser. Awareness note: fake Teams installers.	Malvertising access
Leak site monitoring	Control 17	Monitor your own organization, subsidiaries and important service providers on ransomware leak sites. An entry often appears before the incident is known internally.	Late detection

Indicators

Selection from CISA AA23-319A, Fortinet, ransomware.live and Microsoft (TerminalFix, August 28, 2026). Host artifacts are more stable than hashes and IP addresses; the encryptor binaries are rebuilt for each victim, and the IP addresses date from summer 2023.

Indicator	Meaning	Source
*.rhysida	Extension of encrypted files	all

CriticalBreachDetected.pdf	Ransom note in every all directory
C:\Users\Public\bg.jpg	Wallpaper set by the attack- Talos ers' tool
C:\Windows\Temp*.exe · S_1.bat · S_2.bat	Staging and distribution of CISA the encryptor
C:\in · C:\out · C:\out\PSTools.zip	Exfiltration staging and tool CISA storage
temp_logs	Backup path of the NTDS Check Point dump, identical to Vice Society
C:\Users\Public\main.dll · iii.bat · Task "System" ONS TART	Go backdoor with Fortinet persistence
ad.ps1 · w.ps1 · DataGrabber1.exe · dob.exe · fury.exe · 67	Backdoor, reconnaissance, Fortinet exfiltration, Windows encryp- tor, Linux encryptor
conhost.exe SHA-256 6633fa85bb234a75927b23417313e51a4c 155e12f71da3959e168851a600b010	Rhysida binary disguised as CISA conhost
1.ps1 SHA-256 4e34b9442f825a16d7f6557193426ae7a18899ed 46d3b896f6e4357367276183	Cleanup and execution script CISA
-d <path> -sr	Encryptor call with self- CISA deletion
cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet	Child process of the encrypt- Fortinet tor on servers
rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7c ad[.]onion	Leak site, active ransomware.live
rhysidaeverywhere@onionmail[.]org · rhysidaofficial@on ionmail[.]org	Negotiation addresses CISA
776c5589[.]schedule[.]newhomessection[.]com	Gootloader domain CISA 04/2025
oij89jiiuguygh.blob.core.windows[.]net · e57thgdfge.bl ob.core.windows[.]net	Azure Blob exfiltration targets 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 and exfiltration, Fortinet, Check July/August 2023 Point
verify_pkg.zip SHA-256 18c2090e8a0ae0568af9b87e59eaf82 70f23d2909600ed9db91a9444fd8b278f	TerminalFix: ZIP archive from Microsoft the captcha command 08/2026

C:\ProgramData\f47f2a8c21c9df4e · 1.bat · LockScreenContentServer.exe outside System32 · dui70.dll SHA-256 b a77feed86bcd49308746421bdc684a432dd5d68c363975b2a3c6831bda3f07	TerminalFix: staging, batch Microsoft start and sideloading DLL	08/2026
client.py SHA-256 b8d107800403b9197e5b7609ceacd8e4cac1 b0f9a1d156e6dacd6c3f7794b36a · pythonw.exe	TerminalFix: Python reverse tunnel	Microsoft 08/2026
gitnow[.]dev:443 · bestsocialmedianewspapper[.]com · o fflineupdater[.]com	TerminalFix: tunnel C2, PNG hosting, failover	Microsoft 08/2026

Complete hash lists: CISA AA23-319A (more than 40 SHA-256 hashes) and Cisco Talos. For the malvertising campaign, Expel maintains an indicator list on GitHub.

Ecosystem and connections

Vanilla Tempest / Vice Society	Microsoft tracks Vanilla Tempest (formerly DEV-0832, known to other vendors as VICE SPIDER or Vice Society) as a financially motivated actor that primarily uses Rhysida, alongside INC Ransomware. In August 2023, Check Point found identical artifacts: the NTDS backup path temp_I0gs, identical firewall rule names and the PortStarter backdoor, while Vice Society had stopped publishing victims after June 21, 2023. The CISA warning explicitly mentions the overlap.
Interlock	IBM X-Force assesses Interlock, active since September 2024, as a likely offshoot from the Rhysida environment. Both use the Supper backdoor with different crypters and share code structures between NodeSnake, InterlockRAT and Supper.
Access brokering	In May 2024, the initial access broker TAG-124 supplied the Broomstick loader for Rhysida and switched to Interlock in September 2024. Gootloader provides access to both groups. The malvertising campaigns ran from May to September 2024 with seven certificates and from June 2025 with more than forty; Microsoft detected them at the end of September 2025, attributed them to Vanilla Tempest and re-voked more than 200 certificates in early October, issued via Microsoft Trusted Signing, SSL.com, DigiCert and GlobalSign. In August 2026, Microsoft described the TerminalFix campaign without attributing it to an actor; the BSI attributes the malware used in it, LoremIpsumLoader (also AxolotLoader), which BlueVoyant had previously found in trojanized Teams installers, to the same group that operates Rhysida.

What this advisory is based on

BSI, BITS-B 2026-287419-1032, German institutions compromised via TerminalFix campaign (September 4, 2026, German); Microsoft, TerminalFix campaign deploys a reverse tunnel through multi-stage intrusion (August 28, 2026); BlueVoyant, Lorem Ipsum Malware (2026); heise, BSI explains first

attack vector against Berlin authorities (September 7, 2026, German); MITRE ATT&CK T1204.004; CISA/FBI/MS-ISAC AA23-319A (November 15, 2023, updated 04/2025); Fortinet FortiGuard, Analyzing Rhysida Ransomware Intrusion (11/2023) and Ransomware Roundup Rhysida (08/2023); Check Point Research (08/2023); Trend Micro (08/2023); Gen Digital, Rhysida Ransomware Technical Analysis (October 26, 2023); Kim et al., Kookmin University / KISA (02/2024); British Library, Cyber Incident Review (March 8, 2024); Microsoft Threat Intelligence (10/2025); Expel, Certified OysterLoader (10/2025); IBM X-Force, Interlock and Rhysida within the ransomware ecosystem; ransomware.live (September 4, 2026); Berlin Senate via heise (September 1, 2026) and dpa (August 28 and September 4, 2026); heise on Stuttgart (05/2026). All information is based on publicly available sources and the TIRAS data set. Leak site entries are claims by the perpetrators. Victim data only in aggregated form.

Primary sources online

- BSI: Cyber security warning BITS-B 2026-287419-1032, German institutions compromised via TerminalFix campaign (September 4, 2026, German)
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-287419-1032.pdf?__blob=publicationFile&v=2
- Microsoft Security Blog: TerminalFix campaign deploys a reverse tunnel through multistage intrusion (August 28, 2026)
<https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/>
- heise online: BSI explains first attack vector against Berlin authorities (September 7, 2026, German)
<https://www.heise.de/news/BSI-erklaert-ersten-Angriffsvektor-auf-Berliner-Behoerden-11444072.html>
- MITRE ATT&CK: T1204.004 Malicious Copy and Paste
<https://attack.mitre.org/techniques/T1204/004/>
- CISA/FBI/MS-ISAC: Joint Advisory AA23-319A, #StopRansomware: Rhysida Ransomware
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a>
- Check Point Research: The Rhysida Ransomware, Activity Analysis and Ties to Vice Society (08/2023)
<https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/>
- Trend Micro: An Overview of the New Rhysida Ransomware (08/2023)
https://www.trendmicro.com/en_us/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
- Fortinet FortiGuard Labs: Ransomware Roundup, Rhysida (08/2023)
<https://www.fortinet.com/blog/threat-research/ransomware-roundup-rhysida>
- Gen Digital: Rhysida Ransomware Technical Analysis (10/2023)
<https://www.gendigital.com/blog/insights/research/rhysida-ransomware-technical-analysis>
- Gen Digital (Avast): Decrypted Rhysida Ransomware (02/2024)
<https://www.gendigital.com/blog/insights/research/decrypted-rhysida-ransomware>
- British Library: Learning Lessons from the Cyber-Attack, Cyber Incident Review (March 8, 2024)
<https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf>

- Expel: Certified OysterLoader, Rhysida activity via code signing certificates (10/2025)
<https://expel.com/blog/certified-oysterloader-tracking-rhysida-ransomware-gang-activity-via-code-signing-certificates/>
- ransomware.live: Rhysida, leak site entries
<https://www.ransomware.live/group/rhysida>

How we can support you with implementation

This advisory shows how Rhysida operates and which actions take priority. Implementation requires an individual assessment of your infrastructure, your existing security measures and your regulatory requirements.

We work with you to check which of your log sources cover the critical detections, where the gaps are and which action has the greatest leverage, and we implement the immediate actions together with your team before you invest in costly penetration tests.

Contact us for an initial conversation.

kontakt@threat-informed.de | www.threat-informed.de

This advisory is part of our threat briefings for companies under NIS2, DORA and critical infrastructure rules in Germany, Austria and Switzerland. TLP:CLEAR, sharing permitted. As of: September 7, 2026, version 1.1.

Glossary

Term	Meaning
ATT&CK	MITRE knowledge base of adversary tactics and techniques; T numbers denote techniques
C2	Command and control: infrastructure for remotely controlling compromised systems
ClickFix TerminalFix	/ Social engineering technique: a website gets the user to run a copied command themselves in the Run dialog (ClickFix) or in Windows Terminal (TerminalFix)
CIS Controls	Center for Internet Security Controls: prioritized catalog of IT security measures
ESXi	VMware hypervisor on which virtual machines run
FIDO2	Phishing-resistant authentication standard
IdP	Identity provider: central sign-in service, such as Entra ID
IOC	Indicator of compromise: technical characteristic of an attack

Leak site	Tor website on which extortion groups name victims and publish data
LOLBin	Living off the land binary: legitimate system tool that adversaries misuse
MFA	Multi-factor authentication
NTDS	Active Directory database with all accounts and password hashes
RaaS	Ransomware as a service: the operator provides malware and infrastructure, affiliates carry out attacks
RMM	Remote monitoring and management: remote maintenance software such as AnyDesk
Sigma	Vendor-neutral format for detection rules; SigmaHQ is the community collection
TLP	Traffic Light Protocol: marking that indicates how widely information may be shared
WDAC	Windows Defender Application Control: allows only approved programs and scripts
TTP	Tactics, techniques, procedures: the methods adversaries use