INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:15 UTC

DragonForce Ransomware Abuses Microsoft Teams TURN Relays for C2 Concealment in Multi-Stage BYOVD Attack

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0483
Type	Threat Campaign
CVE ID	CVE-2023-52271, CVE-2025-61155, CVE-2025-1055
Severity	HIGH
CVSS Base Score	9.5
EPSS Score	0.0027 (18th percentile)
Affected Products	Microsoft Teams (TURN relay infrastructure); VirtualBox; DbgView; Huawei HWAuidoOs2Ec.sys driver; Topaz Antifraud wsftprm.sys; Tower of Fantasy GameDriverx64.sys; K7 Security K7RKScan.sys; Palo Alto Networks (spoofed driver); Microsoft SQL Server / MSSQL
Published	2026-06-16T06:18:48
Discovery Source	Rss

Executive Summary

In December 2025, the DragonForce ransomware group executed a sophisticated multi-stage attack against a major U.S. services company, using a novel backdoor that disguises malicious command-and-control traffic as legitimate Microsoft Teams network activity, effectively defeating standard network monitoring and geo-blocking controls. The attack chain combined kernel-level driver exploitation across at least four vulnerable third-party drivers to disable endpoint defenses, followed by data exfiltration and ransomware deployment in a double-extortion pattern. Organizations running Microsoft Teams, MSSQL, or any of the identified vulnerable drivers face elevated risk of undetected compromise; the attack's use of trusted Microsoft infrastructure as a C2 channel represents a significant detection gap for most enterprise security stacks.

Technical Analysis

DragonForce operators deployed Backdoor.Turn, a custom Go-based implant that tunnels C2 traffic over Microsoft Teams' TURN (Traversal Using Relays around NAT) relay infrastructure (T1090.004, T1071.001). By

routing malicious traffic through legitimate Microsoft-owned relay endpoints, the backdoor bypasses geo-blocking, domain-reputation controls, and standard C2 heuristics. The initial access vector was MSSQL exploitation (T1190), followed by credential harvesting (T1552.001) and account abuse (T1078). Defense evasion relied on a multi-driver BYOVD (Bring Your Own Vulnerable Driver) chain (T1574.002, T1562.001) using: Huawei HWAuidoOs2Ec.sys, Topaz Antifraud wsftprm.sys (CVE-2025-1055), Tower of Fantasy GameDriverx64.sys, and K7 Security K7RKScan.sys. A kernel driver with a filename mimicking Palo Alto Networks products was also loaded to impersonate a trusted security vendor (T1036.005). CVE-2023-52271 is associated with the BYOVD kernel exploitation component; CVE-2025-61155 is tentatively linked to a driver or component vulnerability in the chain with NVD enrichment pending (confidence: medium). Kernel-level execution enabled privilege escalation (T1068), EDR/AV disablement (T1562.001), and installation of persistent services (T1543.003). Lateral movement preceded exfiltration (T1041) and ransomware deployment (T1486) in a double-extortion pattern. Relevant CWEs: CWE-506 (embedded malicious code), CWE-668 (resource exposure), CWE-284 (improper access control), CWE-693 (protection mechanism failure), CWE-494 (download of code without integrity check), CWE-269 (improper privilege management). Patch status: CVE-2025-61155 NVD enrichment pending; CVE-2025-1055 and CVE-2023-52271, consult NVD and vendor advisories for current patch availability. No CISA KEV listing as of this report.

Action Checklist

1. Step 1: Containment. Immediately audit all systems for the presence of the four identified vulnerable drivers: HWAuidoOs2Ec.sys (Huawei), wsftprm.sys (Topaz Antifraud), GameDriverx64.sys (Tower of Fantasy), and K7RKScan.sys (K7 Security). Block loading of these drivers via Windows Defender Application Control (WDAC) or a comparable allowlist policy. Isolate any MSSQL-exposed endpoints from external network access pending verification. Restrict outbound TURN/STUN traffic (UDP 3478, TCP 443 to Microsoft relay ranges). Consult Microsoft documentation (e.g., Office 365 IP addresses and URLs) or your Teams infrastructure vendor for current relay endpoint IP ranges.
2. Step 2: Detection. Query EDR telemetry and Sysmon event logs for driver load events (Event ID 6) involving the four named driver filenames. Obtain driver hashes from published advisories (Northwave, BleepingComputer, NVD, or vendor advisories) and cross-reference multiple sources to ensure completeness. Search for anomalous Go-binary process execution and outbound UDP/TCP connections to Microsoft Teams relay infrastructure from non-Teams processes. Review MSSQL authentication logs for unusual login patterns, enumeration activity (T1087.002), and xp_cmdshell or linked server abuse. Hunt for kernel driver loads with filenames mimicking Palo Alto Networks products from non-standard paths (T1036.005). Reference NIST AU-6 for log review scope and NIST SI-4 for monitoring requirements.
3. Step 3: Eradication. Remove all identified BYOVD driver files from affected hosts and revoke any associated kernel-mode signing certificates where possible. Apply available patches for CVE-2023-52271 and CVE-2025-1055 per NVD and vendor advisories; monitor NVD for CVE-2025-61155 enrichment and apply when available. Rotate all credentials harvested from or accessible on compromised MSSQL instances (NIST IA-5; D3-CRO). Enforce WDAC or Windows Defender Application Control driver allowlisting to block unapproved kernel-mode drivers (CIS 2.3, CIS 4.6). Remove any unauthorized services or scheduled tasks installed for persistence (T1543.003).
4. Step 4: Recovery. Validate that all identified driver files are absent from reimaged or remediated hosts using file integrity monitoring. Confirm WDAC policies are enforced and blocking driver loads outside the approved list. Re-enable EDR/AV solutions and verify protection is active. Monitor MSSQL and authentication logs for 30 days post-remediation for recurrence indicators. Confirm outbound TURN/STUN

traffic originates only from authorized Teams processes. Reference NIST AU-12 for audit record generation requirements during the recovery monitoring period.

5. Step 5: Post-Incident. Conduct a gap assessment against CIS 7.1 (vulnerability management process) and CIS 2.1 (software inventory) to determine whether the vulnerable drivers were tracked. Evaluate whether network monitoring tools can detect C2 over TURN relay infrastructure; if not, engage your SIEM/NDR vendor for updated detection logic. Review MSSQL internet-exposure posture against CIS 4.4 and CIS 4.5 (firewall controls). Implement D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) for all MSSQL and administrative access paths. Document control gaps in your risk register and assign remediation owners with deadlines.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and external IR retainer if memory forensics or MSSQL audit logs confirm successful data exfiltration (DragonForce is a double-extortion operator), if any affected MSSQL instance stores PII, PHI, or PCI-DSS cardholder data triggering state breach notification or HIPAA/PCI reporting obligations, or if the BYOVD driver artifacts confirm active EDR disablement indicating the attacker achieved persistent, undetected kernel access.
Recovery Notes	Before returning any MSSQL instance to production, verify via MSSQL Extended Events that xp_cmdshell is disabled ('EXEC sp_configure "xp_cmdshell", 0; RECONFIGURE;') and confirm no linked-server definitions exist that were not present in the pre-incident configuration baseline. Monitor Sysmon Event ID 6 and Windows CodeIntegrity event logs daily for 30 days for any recurrence of the four named driver files or new spoofed-driver filenames mimicking legitimate vendors, as DragonForce has demonstrated the capability to cycle BYOVD targets. Validate that outbound TURN/STUN flows (UDP 3478, TCP 443) are process-pinned to Teams.exe at the firewall level throughout the monitoring window, since the C2 channel survives reimaging if the firewall ACLs are not enforced.
Forensic Artifacts	Sysmon Event ID 6 (ImageLoad) records from 'Microsoft-Windows-Sysmon/Operational' for HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, K7RKScan.sys, and any driver with a filename mimicking Palo Alto Networks products — these records include SHA256 hashes and the loading process, directly mapping the BYOVD kill-chain sequence. | Windows kernel memory image (WinPmem/DumpIt) analyzed for non-paged pool allocations associated with the BYOVD drivers' Device Objects, IRP hook modifications, and deregistered PsSetCreateProcessNotifyRoutine / ObRegisterCallbacks entries — the specific mechanism DragonForce used to blind EDR sensors. | MSSQL ERRORLOG at '%ProgramFiles%\Microsoft SQL Server\MSSQL\Log\ERRORLOG' and Extended Events trace capturing xp_cmdshell enable/disable audit entries and linked-server query execution — evidence of the initial access and lateral movement stage via CVE-2025-1055 or credential abuse on the internet-exposed MSSQL instance. | Full packet capture (PCAP) of UDP 3478 and TCP 443 traffic from affected hosts to Microsoft Teams TURN relay IP ranges (52.112.0.0/14, 52.122.0.0/15), with STUN binding request dissection to identify non-Teams.exe source processes — the primary artifact demonstrating the DragonForce backdoor's C2 concealment technique. | Registry hive export of 'HKLM\SYSTEM\CurrentControlSet\Services' and 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks' capturing driver service registrations and scheduled task persistence entries installed by the DragonForce multi-stage loader — required to confirm complete eradication before recovery.

Per-Action IR Details

Step 1: Containment — Immediately audit all systems for the presence of the four identified vulnerable drivers: HWAuidoOs2Ec.sys (Huawei), wsftprm.sys (Topaz Antifraud), GameDriverx64.sys (Tower of Fantasy), and K7RKScan.sys (K7 Security). Block loading of these drivers via Windows Defender Application Control (WDAC) or a comparable allowlist policy. Isolate any MSSQL-exposed endpoints from external network access pending verification. Restrict outbound TURN/STUN traffic (UDP 3478, TCP 443 to Microsoft relay ranges) to only authorized Teams clients, using firewall ACLs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST CM-7 — not in knowledge base; omitted, CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Use 'driverquery /v /fo csv > drivers.csv' on each host and diff against known-good baseline to surface HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, and K7RKScan.sys. Block driver loads without WDAC by adding deny rules via Windows Firewall with Advanced Security (netsh advfirewall) to drop UDP 3478 and TCP 443 egress from any process other than Teams.exe. Isolate MSSQL hosts by disabling the NIC via 'Disable-NetAdapter -Name * -Confirm:$false' rather than physical disconnection to preserve volatile state.

Evidence: BEFORE isolating any host or applying ACLs, capture: (1) full RAM image using WinPmem or DumpIt to recover the injected BYOVD driver's in-memory kernel objects and any injected shellcode living only in non-paged pool; (2) 'Get-NetTCPConnection | Where-Object {$_.RemotePort -eq 443 -or $_.RemotePort -eq 3478}' output to document live C2 sessions piggybacking Teams TURN relay IPs; (3) 'netstat -ano' to correlate PIDs of Go-binary processes holding relay connections; (4) running driver list via 'fltMC filters' and 'sc query type= driver state= all' before WDAC blocks flush loaded-but-not-yet-persisted drivers.

Step 2: Detection — Query EDR telemetry and Sysmon event logs for driver load events (Event ID 6) involving the four named driver filenames and their known hashes (obtain from BleepingComputer reporting and Northwave advisory). Search for anomalous Go-binary process execution and outbound UDP/TCP connections to Microsoft Teams relay IP ranges from non-Teams processes. Review MSSQL authentication logs for unusual login patterns, enumeration activity (T1087.002), and xp_cmdshell or linked server abuse. Hunt for spoofed driver filenames mimicking Palo Alto Networks products (T1036.005). Reference NIST AU-6 for log review scope and NIST SI-4 for monitoring requirements.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and enable Event ID 6 (ImageLoad) filtering on driver filename and hash for the four named .sys files. Use this PowerShell query against Sysmon logs: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 6 -and $_.Message -match "HWAuidoOs2Ec|wsftprm|GameDriverx64|K7RKScan"}'. For MSSQL, enable server-side tracing or Extended Events to log xp_cmdshell invocations and linked-server queries. Use Wireshark on the network tap to capture and decode UDP 3478 traffic and identify non-Teams.exe PIDs sourcing STUN binding requests to Microsoft relay ranges.

Evidence: This is an analysis step that does not itself alter live state, but analysts must collect before any downstream containment or eradication actions: (1) Sysmon Event ID 6 records showing ImageLoad of HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, or K7RKScan.sys, including SHA256 hashes for comparison against Northwave advisory IOCs; (2) Sysmon Event ID 1 (Process Create) records for Go-binary executables with parent processes tied to MSSQL (sqlservr.exe) indicating xp_cmdshell lateral staging; (3) Windows Security Event Log Event ID 4625 and 4648 on the MSSQL host for brute-force or pass-the-hash authentication attempts; (4) MSSQL error log at '%ProgramFiles%\Microsoft SQL Server\MSSQL\Log\ERRORLOG' for xp_cmdshell enable/disable audit entries; (5)

Sysmon Event ID 22 (DNS Query) records for Teams relay FQDN resolution (relay.teams.microsoft.com, *.relay.skype.com) initiated by non-Teams.exe processes — the DragonForce backdoor mimics this pattern to blend into relay traffic.

Step 3: Eradication — Remove all identified BYOVD driver files from affected hosts and revoke any associated kernel-mode signing certificates where possible. Apply available patches for CVE-2023-52271 and CVE-2025-1055 per NVD and vendor advisories; monitor NVD for CVE-2025-61155 enrichment and apply when available. Rotate all credentials harvested from or accessible on compromised MSSQL instances (NIST IA-5; D3-CRO). Enforce WDAC or Windows Defender Application Control driver allowlisting to block unapproved kernel-mode drivers (CIS 2.3, CIS 4.6). Remove any unauthorized services or scheduled tasks installed for persistence (T1543.003).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Remove driver files using 'del /f /q C:\Windows\System32\drivers\HWAuidoOs2Ec.sys' (repeat for all four) after booting to WinPE or offline mount if the drivers survive reboot via registry persistence at 'HKLM\SYSTEM\CurrentControlSet\Services'. Audit scheduled tasks with 'schtasks /query /fo LIST /v | findstr /i "TaskName Status Run"' and services with 'sc query type= all state= all' to locate DragonForce persistence mechanisms. For credential rotation without PAM tooling, use Active Directory Users and Computers to force password reset on all MSSQL service accounts and SQL logins, then re-test connectivity before bringing MSSQL back online.

Evidence: BEFORE removing drivers, rotating credentials, or applying patches (all of which alter live state): (1) acquire a complete memory image to preserve the kernel driver's Device Object, IRP hook table modifications, and any EDR callback deregistration artifacts in non-paged pool — use WinPmem targeting the kernel address space; (2) export 'HKLM\SYSTEM\CurrentControlSet\Services' registry hive to capture driver service registration entries for HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, K7RKScan.sys, and any spoofed Palo Alto-named service; (3) collect the full scheduled task XML export via 'Get-ScheduledTask | Export-CliXml tasks-backup.xml' to document persistence mechanisms before removal; (4) export MSSQL server audit logs and sys.server_audit_specification contents before credential rotation clears session tokens; (5) hash all four .sys files on disk (Get-FileHash -Algorithm SHA256) and compare against Northwave advisory IOC list before deletion to confirm identity.

Step 4: Recovery — Validate that all identified driver files are absent from reimaged or remediated hosts using file integrity monitoring. Confirm WDAC policies are enforced and blocking driver loads outside the approved list. Re-enable EDR/AV solutions and verify protection is active. Monitor MSSQL and authentication logs for 30 days post-remediation for recurrence indicators. Confirm outbound TURN/STUN traffic originates only from authorized Teams processes. Reference NIST AU-12 for audit record generation requirements during the recovery monitoring period.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-12 (Audit Record Generation), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use Sysmon Event ID 6 as a continuous canary: configure an alert that fires on ANY driver load not in the WDAC approved list and pipe it to a watched text file reviewed daily by the on-call analyst. Validate WDAC enforcement mode with 'Get-CIPolicy -FilePath ' and confirm 'Enforce' (not 'Audit') mode. For TURN/STUN process validation without NDR tooling, run a daily scheduled PowerShell job: 'Get-NetTCPConnection -RemotePort 443 | ForEach-Object {(Get-Process -Id $_.OwningProcess).Name}' and alert on any process name that is not Teams.exe or update.exe.

Evidence: Recovery validation does not require pre-capture of volatile evidence (host state has been remediated), but the following must be verified before declaring recovery complete: (1) Sysmon Event ID 6 logs show zero loads of HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, or K7RKScan.sys since reimaging; (2) WDAC event log ('Microsoft-Windows-CodeIntegrity/Operational', Event ID 3076 in audit mode or 3077 in enforce mode) shows no block bypasses; (3) MSSQL Extended Events session capturing login failures and xp_cmdshell invocations is active and forwarding to the log aggregator; (4) EDR agent heartbeat confirms tamper-protection is re-enabled and kernel callbacks are re-registered — DragonForce specifically deregistered these via BYOVD, so callback restoration is the proof-of-eradication test.

Step 5: Post-Incident — Conduct a gap assessment against CIS 7.1 (vulnerability management process) and CIS 2.1 (software inventory) to determine whether the vulnerable drivers were tracked. Evaluate whether network monitoring tools can detect C2 over TURN relay infrastructure; if not, engage your SIEM/NDR vendor for updated detection logic. Review MSSQL internet-exposure posture against CIS 4.4 and CIS 4.5 (firewall controls). Implement D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) for all MSSQL and administrative access paths. Document control gaps in your risk register and assign remediation owners with deadlines.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management)

Compensating: For software inventory gap assessment without a CMDB, run 'driverquery /fo csv /v > all_drivers_$(hostname).csv' across all endpoints via PSExec or a PowerShell remoting loop and diff output against a manually maintained approved-driver list. For TURN relay C2 detection without SIEM/NDR, write a Sigma rule targeting Sysmon Event ID 3 (NetworkConnect) where DestinationPort is 3478 or 443 and Image is NOT 'C:\Program Files\Microsoft\Teams\current\Teams.exe' — this directly targets the DragonForce backdoor's relay mimicry behavior. Publish the rule to the team's shared Sigma repository for ongoing use.

Evidence: Post-incident activity does not alter live system state; however, the following artifacts must be preserved from the incident for lessons-learned and threat intelligence sharing: (1) the full timeline of Sysmon Event ID 6 driver load events correlated with EDR callback deregistration timestamps — this documents the precise BYOVD kill-chain sequence for DragonForce's approach; (2) PCAP samples of the Teams-relay-mimicking C2 traffic captured during detection, including STUN binding request headers, for submission to your NDR/SIEM vendor to develop updated detection signatures; (3) the MSSQL Extended Events trace capturing the initial access vector (xp_cmdshell invocations or linked-server abuse) as evidence for the gap assessment finding; (4) exported WDAC audit logs showing which driver loads would have been blocked had enforce mode been active prior to the incident — this quantifies the policy gap for the risk register.

Detection Guidance

Primary detection focus areas: (1) Driver load telemetry. Enable Sysmon Event ID 6 (driver loaded) and alert on any load of HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, K7RKScan.sys, or any driver with a filename pattern mimicking Palo Alto Networks products from non-standard paths. Cross-reference driver hashes against published advisories (Northwave, BleepingComputer, NVD). (2) TURN relay C2. Hunt for non-Teams processes (by process name and parent process lineage) establishing outbound connections to Microsoft Teams TURN relay infrastructure (UDP 3478, TCP 443). Consult Microsoft's Office 365 IP address list or Teams technical documentation for the current set of relay endpoint IP ranges. Legitimate Teams traffic originates from the Teams client process; any other originating process is anomalous. (3) MSSQL abuse. Review SQL Server error

logs and Windows Security Event logs for enumeration patterns (large volumes of SELECT queries against sys.syslogins or similar), xp_cmdshell execution, unusual stored procedure calls, and logons from unexpected source IPs. (4) Privilege escalation and EDR tampering. Alert on Windows Security Event ID 4697 (service installed) and 7045 (new service) for kernel-mode driver services. Monitor for EDR process termination events or protection disablement sequences preceding these driver loads. (5) Go binary execution. Hunt for unsigned or anomalously signed Go-compiled executables (identifiable by Go runtime strings in binary metadata) spawning network connections. Behavioral IOCs: outbound connections to Microsoft relay infrastructure from non-Teams parent processes; kernel-mode driver loads from user-writable directories; MSSQL spawning cmd.exe or PowerShell child processes. Confidence on CVE-to-exploit mapping for CVE-2025-61155 is medium pending NVD enrichment; adjust detection priority accordingly.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[see BleepingComputer reporting and Northwave advisory for verified driver hashes]`	Kernel-mode drivers used in BYOVD chain: HWAuidoOs2Ec.sys, wsftprm.sys, GameDriverx64.sys, K7RKScan.sys — obtain confirmed hashes from linked reporting	MEDIUM
DOMAIN	`relay.teams.microsoft.com (relay infrastructure ranges)`	Microsoft Teams TURN relay endpoints abused by Backdoor.Turn for C2 tunneling — flag connections from non-Teams processes	HIGH
HASH	`[spoofed Palo Alto Networks driver — hash pending vendor or researcher disclosure]`	Spoofed driver impersonating a Palo Alto Networks product, used for defense evasion (T1036.005)	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1068** — Exploitation for Privilege Escalation
- **T1105** — Ingress Tool Transfer
- **T1078** — Valid Accounts
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1552.001** — Credentials In Files
- **T1543.003** — Windows Service
- **T1190** — Exploit Public-Facing Application
- **T1090.004** — Domain Fronting
- **T1071.001** — Web Protocols
- **T1574.002** — DLL Side-Loading

- **T1543** — Create or Modify System Process
- **T1486** — Data Encrypted for Impact
- **T1087.002** — Domain Account
- **T1027** — Obfuscated Files or Information
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-3** — Access Enforcement
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1105	Ingress Tool Transfer	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1552.001	Credentials In Files	Credential-Access
T1543.003	Windows Service	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1090.004	Domain Fronting	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1574.002	DLL Side-Loading	Persistence
T1543	Create or Modify System Process	Persistence

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1087.002	Domain Account	Discovery
T1027	Obfuscated Files or Information	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/ransomware-gang-abus.. .	T3
CVE-2025-61155 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-61155	T1
CVE-2025-61155 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2025-61155	T3
BYOVD research use cases featuring vulnerable driver ... - GitHub	https://github.com/BlackSnufkin/BYOVD	T3
Vulnerability Notice Topaz Antifraud - Northwave Cyber Security	https://northwave-cybersecurity.com/vulnerability-notice-topaz-anti...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2023-52271, CVE-2025-61155, CV...	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5227...	T1

Generated 2026-06-16 19:15 UTC by TJS Security Command Center