Smarttech
YOUR 24/7 SECURITY PARTNER

DireWolf Ransomware Threat Report

Overview

DireWolf is an active, human-operated ransomware group running a double-extortion model, and it has claimed two significant victims in the past week.

DireWolf's earliest recorded attack dates to 17 April 2025, and the group disclosed its first six victims on a dark web leak site on 26 May 2025. As of 19 August 2026, there were 100 confirmed leak-site victims across 32 countries, with 25 of those disclosed in the past month alone, so this is an accelerating campaign, not a tapering one. It runs a tight core team rather than a broad affiliate programme, and researchers have found no infrastructure or wallet overlap linking it to established groups such as Akira, Fog, Qilin, or SafePay.

DireWolf follows the now-standard double-extortion playbook: encrypt the victim's files, exfiltrate sensitive data beforehand, and threaten public leak on a Tor-hosted site unless a ransom is paid. Ransom notes are victim-specific, containing a hardcoded live-chat room ID and login credentials for direct negotiation. This level of customisation, combined with intrusion dwell times spanning days to weeks, points to methodical, reconnaissance-heavy operators rather than an opportunistic spray-and-pray affiliate crew. Average exfiltration volume observed across incidents is around 265 GB. Typical ransom demands sit around USD $500,000, though this varies by victim size.

Target sectors

DireWolf's victim base skews toward operationally critical, recovery-sensitive sectors. Current standing, out of 100 tracked victims:

Sector	Victim count	Share
Professional Services	17	17%
Manufacturing	16	16%
Healthcare	15	15%
Technology / IT	15	15%
Financial Services	9	9%
Construction & Engineering	recurring, outside the top 5 by volume	–

These sectors share a common weakness DireWolf exploits deliberately: heavy reliance on on-premises backup and database infrastructure.

Recent critical victims

- Arizona State University (ASU), discovered on the group's leak site on 17 August 2026. Reported figures include 1,477 employees, 13,204 users, and 2,831 third-party contractor

credentials, alongside a general exfiltration claim.

Item	Value
Business	**Arizona State University — Learning Enterprise / EdPlus**
Total size	**4.74 GB, 7,925 files/tables, 4 databases, ~5.5 million rows**
Time range	**2017-03 ~ 2026-08**

- TOTVS, a major Brazilian enterprise software and business services provider, claimed on the leak site on 15 August 2026. The listing asserts data exfiltration and, notably, corporate credential exposure: if TOTVS staff or partners reuse exposed passwords elsewhere, those accounts carry immediate takeover risk regardless of whether the underlying ransomware claim is ultimately substantiated. TOTVS has not issued a public confirmation at the time of writing.

Item	Value
Business	**TOTVS Hospitality** (multi-tenant hotel PMS/CRS SaaS for Latin American hotel chains, with a cross-country fiscal e-invoicing suite)
Total size	51.9 GB, 489 files, **15 databases**, **~30.7 million rows**
Time range	2003-10 ~ 2026-08

Technical Profile

DireWolf's encryptor is written in Golang and typically delivered as a UPX-packed binary. Go gives the operators cross-platform portability and a codebase that is comparatively harder for signature-based antivirus to fingerprint; UPX packing adds a layer of obfuscation that slows static analysis and delays detection long enough for the encryption phase to complete. Only Windows variants have been observed to date; no Linux or ESXi encryptor has been documented, which is a gap worth monitoring given how common cross-platform encryptors have become in this space.

DireWolf uses a modern, deliberately efficient hybrid cryptographic design:

1. For each file, the malware generates a random private key and performs a Curve25519 elliptic-curve key exchange against a public key hardcoded in the binary.
2. The resulting shared secret is passed through SHA-256 to derive both the encryption key and the nonce.
3. That key and nonce feed the ChaCha20 stream cipher, chosen for its speed on large, high-volume data sets compared with block ciphers like AES in equivalent software implementations.

This means every encrypted file has its own unique key, so recovering one file's key gives an attacker or defender no path to any other file, and there is no single master key to hunt for.

To maximise throughput across a large estate, DireWolf applies size-based partial encryption: files under 1 MB are encrypted in full, while files over 1 MB have only their first 1 MB segment encrypted. This is enough to destroy the file's structure and render it unusable while sharply cutting the CPU and I/O time needed per file, since encrypting the first megabyte of a 50 GB database file achieves the same practical damage as encrypting all of it. To further accelerate the run, the encryptor waits two seconds after its startup checks, then spins up a worker pool of goroutines sized at eight times the host's logical CPU count, deliberately saturating disk I/O wait time at the cost of a visible CPU and disk-queue spike, a detail defenders can use as a behavioural signal.

Encrypted files are appended with the .direwolf extension. The encryptor deliberately skips system-critical and already-processed file types (.exe, .dll, .sys, .drv, .bin, .tmp, .iso, .img, .direwolf), keeping the host stable enough to boot and display the ransom note rather than bricking it outright.

Tactics, Techniques, and Procedures

On launch, DireWolf checks for two conditions before doing anything else: the system-wide mutex Global\direwolfAppMutex, and the marker file C:\runfinish.exe. If either is present, the binary logs the event, self-deletes, and exits immediately. This is a single-run safety mechanism: it stops the operators' own tooling from re-encrypting an already-processed host (which would waste time and could corrupt already-encrypted files), and it doubles conveniently as an anti-analysis check against sandboxes that may leave stale artefacts behind. The encryptor takes no configuration file; all behaviour is driven by command-line flags (-d to target a specific directory, -h for help), which minimises artefacts available for reverse engineering.

Once the guardrail checks clear, DireWolf executes a scripted sequence designed to strip out every recovery path before a single file is touched:

- Logging suppression: repeatedly terminates the Windows Event Log service via WMI queries and taskkill, running a persistent "check PID, force close, wait, repeat" loop so the service cannot come back online during the run. It later runs wevtutil cl against the Application, System, Security, and Setup logs to erase what history remains.
- Backup and shadow-copy destruction: issues vssadmin delete shadows /all /quiet and wmic shadowcopy delete /nointeractive to wipe Volume Shadow Copies, then a sequence of wbadmin commands (stop job, disable backup, delete backup -keepVersions:0, delete systemstatebackup, delete catalog) to remove Windows Server Backup jobs and catalogues outright.
- WinRE disablement: runs bcdedit /set {default} recoveryenabled No and bcdedit /set {default} bootstatuspolicy ignoreallfailures, which together prevent the host from booting into Windows Recovery Environment even after a failed boot, closing off the built-in Windows recovery path a responder might otherwise reach for.
- Process and service termination: forcibly kills processes and services that could interfere with encryption or provide a recovery point, including database engines (sqlservr.exe, Oracle), the Volume Shadow Copy service (vss.exe), mail clients (outlook.exe) and servers (Exchange), virtualisation platforms (VMware), backup agents (Veeam, VeeamTransportSvc, BackupExec's BackupExecJobEngine, SQLSERVERAGENT), and security tooling (Symantec, Sophos). Documented runs have terminated as many as 75 services and 59 processes in total.

After the file-encryption pass completes, DireWolf writes its C:\runfinish.exe marker to prevent any future re-run on that host, drops a HowToRecoveryFiles.txt ransom note into every affected directory schedules a forced reboot via shutdown -r -f -t 10, and self-deletes shortly afterward via a delayed timeout and del sequence, removing the executable from disk to complicate forensic recovery.

Tactic	Technique	Observed behaviour
Impact	T1490 – Inhibit System Recovery	VSS, wbadmin, bcdedit destruction chain
Impact	T1489 – Service Stop	Termination of up to 75 services / 59 processes
Impact	T1529 – System Shutdown/Reboot	Forced reboot post-encryption
Defense Evasion	T1070.004 – Indicator Removal: File Deletion	Self-deletion, log clearing
Initial Access (suspected)	T1566.001 – Spearphishing Attachment	Not confirmed, assessed from pattern
Initial Access (suspected)	T1078 – Valid Accounts	Exposed RDP/VPN, credential-based access suspected

No confirmed CVE exploitation has been documented for DireWolf to date. Researchers assess spear-phishing, exposed RDP or VPN services, credential-based attacks, and possible third-party or MSP compromise as the most likely entry vectors.

No new DireWolf-associated file hashes, C2 domains, or infrastructure indicators were identified within the past 30 days at the time of this update (19 August 2026).

General Recommendations

1. Strengthen Preventive Controls

• Enforce phishing-resistant MFA for VPN, VDI, RDP gateways, privileged accounts, backup consoles, and VMware vCenter.
• Disable or tightly restrict internet-facing RDP; route administrative access through hardened jump servers.
• Keep operating systems, VPN appliances, firewalls, hypervisors, backup platforms, and remote access tools fully patched.
• Enable antivirus and EDR protections at all times and ensure tamper protection is enforced.
• Enable vulnerable-driver protection such as Microsoft vulnerable driver blocklist, WDAC, or equivalent controls to reduce BYOVD risk.

• Block unauthorized remote management tools such as AnyDesk, Atera, ScreenConnect, Splashtop, TeamViewer, MeshAgent, and Remotely unless explicitly approved.
• Restrict application execution using allowlisting or application control to prevent execution from temporary folders, user profiles, downloads, and SMB shares.
• Limit administrative privileges and ensure employees operate with standard user

accounts wherever possible.
• Remove standing domain administrator access and use just-in-time privileged access for administrative tasks.
• Restrict PsExec, remote service creation, and administrative share abuse to reduce ransomware propagation.
• Segment critical environments including Active Directory, backup infrastructure, VMware ESXi/vCenter, file servers, production systems, and user networks.
• Restrict use of personal or unmanaged devices on corporate networks unless strong device posture, EDR, encryption, and access controls are enforced.
• Monitor and restrict high-risk file-transfer tools such as Cyberduck, WinSCP, Rclone, MEGAsync, FileZilla, and s5cmd.

2. Build a Resilient Recovery Strategy

• Develop and regularly update the ransomware response plan covering credential compromise, RMM abuse, data exfiltration, ESXi targeting, backup disruption, and encryption.
• Maintain offline, encrypted, and immutable backups for critical systems and data.
• Test restoration procedures frequently to confirm that backups are usable and clean
• Keep backup infrastructure isolated from standard domain credentials and user networks.
• Maintain clean golden images for critical servers, endpoints, domain controllers, and recovery systems.
• Define clear recovery priorities for crown-jewel assets such as identity systems, backup platforms, ERP, EHR, file shares, VMware infrastructure, and production systems.
• Ensure backup administrators, domain administrators, and virtualization administrators use separate accounts and separate access paths.
• Monitor for backup deletion, failed backup jobs, VSS deletion, disabled backup agents, and suspicious backup-console logins.
• Preserve critical logs outside the compromised domain, including EDR, VPN, DNS, proxy, firewall, Active Directory, backup, and vCenter logs.
• Maintain an up-to-date emergency contact directory for executives, IT, security, legal, communications, cyber insurance, external incident response vendors, law enforcement, regulators, and key suppliers.
• Pre-approve crisis communication templates for employees, customers, regulators, partners, and media.
• Establish clear ransom decision-making authority, including legal, sanctions, insurance, executive, and board-level escalation.

3. Empower with Risk Awareness & Preparedness

• Conduct routine tabletop exercises simulating Qilin-style ransomware scenarios, including VPN compromise, unauthorized RMM deployment, data theft, ESXi encryption, and backup disruption.
• Train employees to recognize phishing attempts, suspicious links, fake CAPTCHA pages, malicious installers, MFA fatigue attempts, and unusual system behavior.
• Train helpdesk teams to detect social engineering attempts related to password resets, MFA resets, remote access enrollment, and account recovery.
• Maintain an accurate asset inventory covering endpoints, servers, cloud assets,

VMware infrastructure, backup systems, privileged accounts, remote access tools, and critical applications.

• Maintain network flow inventories to understand how critical systems communicate and where segmentation is required.
• Identify and document crown-jewel data locations, including HR, finance, legal, customer data, patient data, source code, intellectual property, and regulated information.
• Review third-party and MSP access regularly, ensuring vendors use MFA, named accounts, least privilege, session logging, and time-bound access.
• Review ransomware readiness metrics with executive leadership, including MFA coverage, EDR health, backup restore success, privileged account count, patching SLA compliance, and RMM exceptions.

References

https://asec.ahnlab.com/en/89944/
https://www.levelblue.com/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors
https://www.darkreading.com/threat-intelligence/dire-wolf-ransomware-manufacturing-technology
https://gbhackers.com/dire-wolf-ransomware/
https://securityonline.info/direwolf-the-new-ransomware-group-targeting-global-businesses/
https://socradar.io/blog/dark-web-profile-dire-wolf-ransomware/
https://www.dexpose.io/direwolf-targets-brazilian-business-leader-totvs/
https://blog.rankiteo.com/ari1787092238-arizona-state-university-breach-august-2026/
https://www.cisa.gov/stopransomware/ransomware-guide

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com