Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

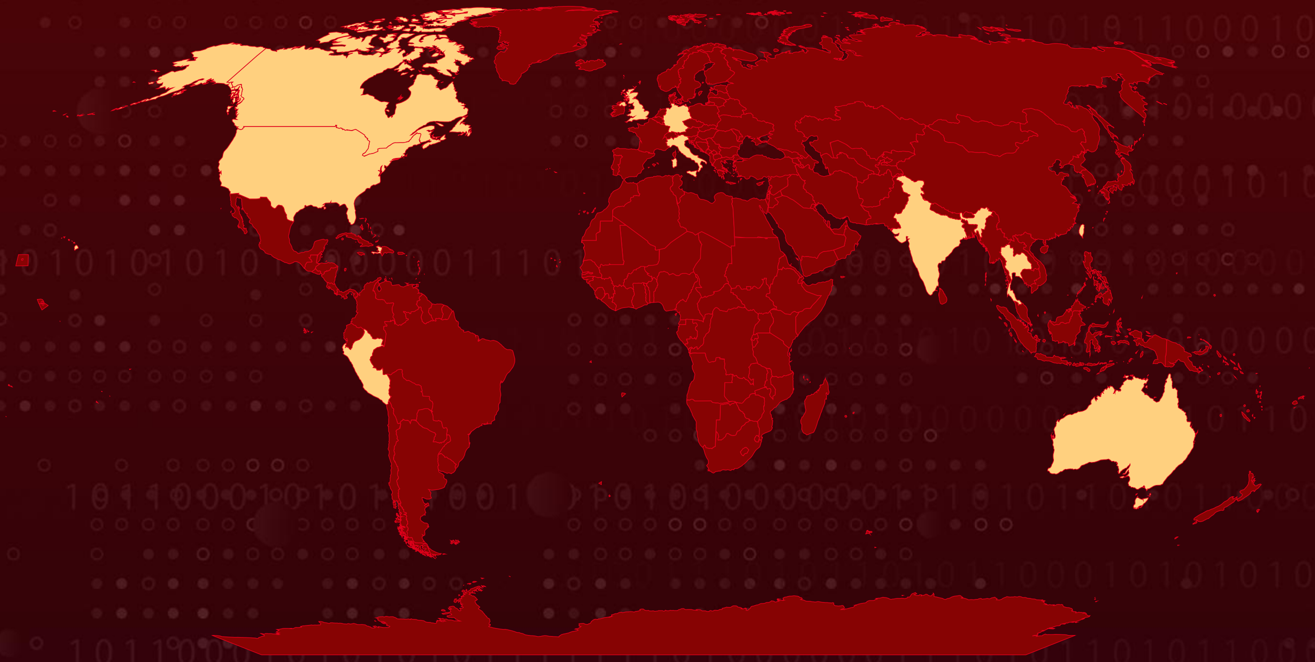
Dire Wolf Ransomware: A New Global Cyber Threat Emerges

Date of Publication	Admiralty Code	TA Number
July 8, 2025	A1	TA2025209

Summary

First Seen: May 2025
Targeted Countries: United States, Thailand, Taiwan, Haiti, Peru, United Kingdom, Germany, India, Canada, Bahrain, Australia, Italy, Singapore
Malware: Dire Wolf Ransomware
Ransom Demand: Around $500,000
Targeted Platforms: Windows (cross-platform capability via Golang)
Targeted Industries: Manufacturing, Technology, Legal Services, Financial Services, Healthcare, Aerospace, Defense, Business Services & Consulting, Real Estate, Transportation, Insurance, Retail, Construction, Consumer Services
Attack: Dire Wolf is a sophisticated ransomware group first identified in May 2025, targeting manufacturing and tech sectors across 13 countries with double extortion tactics. It encrypts and exfiltrates data, demanding ransoms up to $500,000 under threat of public leaks. The malware is written in Golang, packed with UPX, and designed to disable recovery options while using strong encryption. Each attack is customized, with unique ransom notes and negotiation portals, indicating a highly targeted and professional operation.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

Dire Wolf is a newly emerged ransomware group first observed in May 2025, rapidly making an impact by targeting organizations across multiple sectors and countries. The group primarily focuses on the manufacturing and technology sectors, with the United States and Thailand being the most affected nations, followed by Taiwan. As of early July 2025, at least 14 victims have been publicly listed on Dire Wolf's leak site, with attacks spanning 13 countries.

#2

The group employs a double extortion tactic, not only encrypting victims' data but also exfiltrating sensitive files and threatening to release them unless a ransom is paid. This approach significantly raises the stakes for organizations, as the threat extends beyond operational disruption to potential reputational and regulatory consequences. Victims are typically given about a month to pay the ransom, demands have reached up to $500,000, before their stolen data is published on the group's dark web leak site.

#3

Technically, Dire Wolf's ransomware is written in Golang, a language favored by cybercriminals for its cross-platform capabilities and evasion of many antivirus tools. The malware is initially packed with UPX to hinder analysis. Upon execution, it checks for previous infection and ensures only a single instance runs, then disables event logs, terminates security and backup processes, and deletes recovery options to maximize its impact. It uses robust encryption (Curve25519 and ChaCha20), appending the .direwolf extension to affected files while avoiding certain system-critical file types.

#4

A unique aspect of Dire Wolf's operations is the customization of each attack. The ransomware drops a tailored ransom note for each victim, providing unique credentials to a live chat room for negotiation and sharing a link to a sample of stolen data as proof of exfiltration. This level of personalization, along with the use of custom-built encryptors, suggests a highly targeted approach rather than indiscriminate mass attacks.

Recommendations

Restrict access and patch systems: Grant administrative privileges sparingly and keep all security software up to date. Regularly scan for vulnerabilities and ensure endpoint protection can identify or block unknown malware.

Endpoint and Server Hardening: Use advanced EDR/XDR solutions to detect behaviors linked to Dire Wolf, such as process tampering, disabling of logging services, or termination of backup processes. Configure application controls (e.g., AppLocker or WDAC) to block unauthorized executables. Monitor for encryption indicators like the creation of .direwolf file extensions and rapid deletion of shadow copies.

Network Segmentation and Traffic Control: Segment the internal network to limit lateral movement between endpoints, especially for privileged and critical systems. Apply strict firewall rules and network policies to restrict outbound traffic, particularly to known malicious domains, Tor exit nodes, and suspected command-and-control (C2) infrastructure.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of an Direwolf ransomware attack, up-to-date backups enable recovery without paying the ransom.

Monitor for Exfiltration and Ransom Indicators: Monitor for suspicious activity such as the deletion of shadow copies, disabling of backups, and clearing of event logs. Set up alerts for the use of commands like vssadmin delete shadows, wbadmin delete, bcdedit, and wevtutil cl—all of which are used by Dire Wolf to disrupt recovery and cover tracks.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0002 Execution	TA0005 Defense Evasion	TA0040 Impact
T1059 Command and Scripting Interpreter	T1490 Inhibit System Recovery	T1485 Data Destruction	T1070.001 Clear Windows Event Logs
T1486 Data Encrypted for Impact	T1489 Service Stop	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1027 Obfuscated Files or Information	T1070 Indicator Removal	T1059.001 PowerShell	T1562.002 Disable Windows Event Logging

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3, 8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
SHA1	Ed7c9fbd42605c790660df86b7ec325490f6d827, 4a5852e9f9e20b243d8430b229e41b92949e4d69
MD5	A71dbf2e20c04da134f8be86ca93a619, aa62b3905be9b49551a07bc16eaad2ff
TOX ID	B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2
TOR Address	Hxxp[://]direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd[.]onion
File Name	data345.exe

Recent Breaches

https://gbgroup.com
https://medifarma.com.pe
https://health-insights.com
https://kmp.co.th
https://epc.com
https://iotechworld.com
https://tdmtechservices.com
https://binfaqeeh.com
https://thairunggroup.co.th
https://kiwi86.com
https://lpbwa.org.au
https://smvthailand.com
https://qualitas.pro
https://wilsonuniverse.com

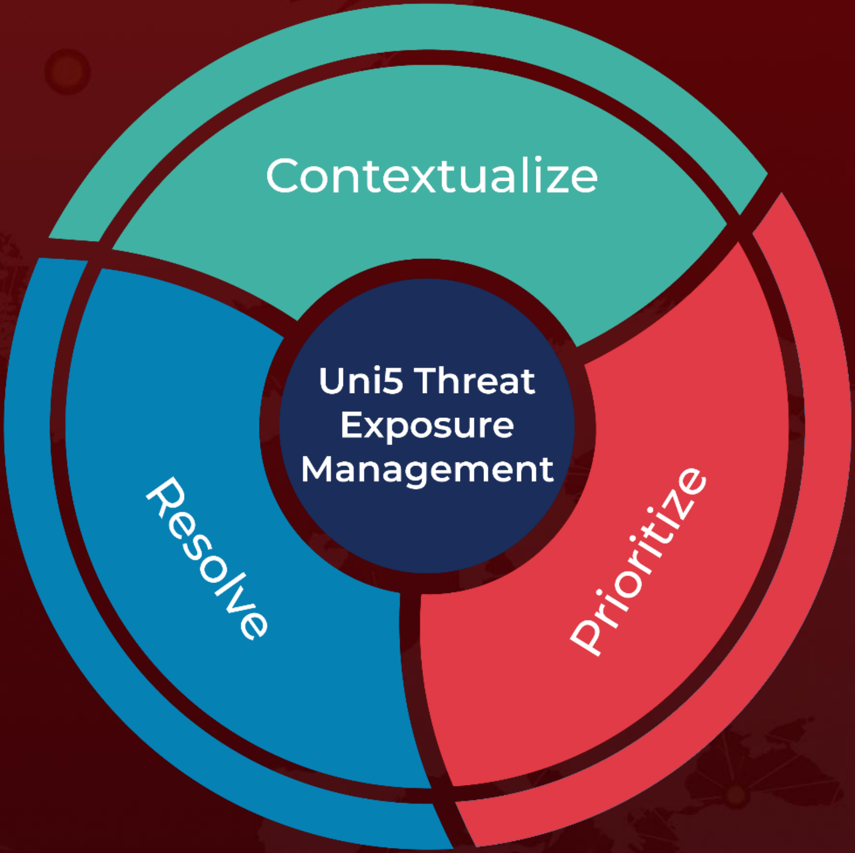
References

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 8, 2025 • 5:30 AM

More at www.hivepro.com