Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

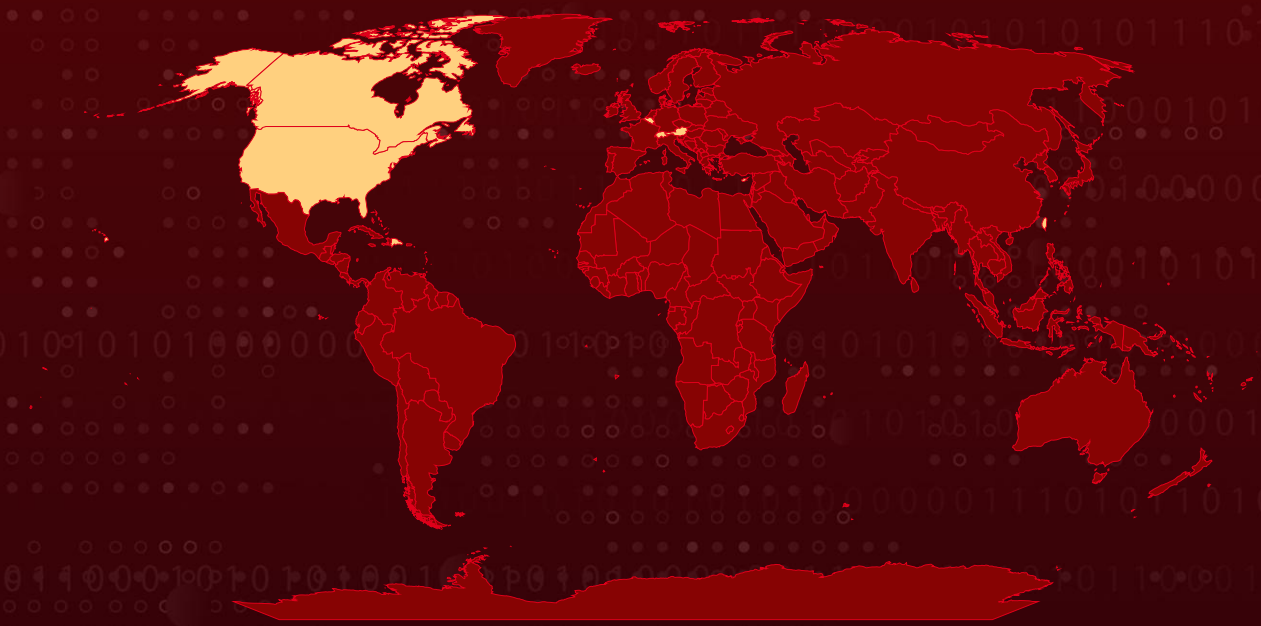
LeakNet Ransomware's Low-Cost High-Scale Infection Strategy

Date of Publication	Admiralty Code	TA Number
March 18, 2026	A1	TA2026074

Summary

First Seen: November 2024
Targeted Regions: Switzerland, Austria, United States, Belgium, Dominican Republic, Cyprus, Taiwan, Mauritius, Canada
Targeted Platform: Windows
Targeted Industries: Charitable Organizations, Manufacturing, Healthcare, Financial Services, Transportation, Business Services & Consulting, Insurance, Sports & Gaming, Education, Energy, Architectural Services, Engineering Services, Logistics
Malware: LeakNet, Deno
Attack: The LeakNet ransomware group has expanded its initial access capabilities by adopting ClickFix social engineering lures delivered through compromised legitimate websites, moving away from its previous reliance on initial access brokers (IABs). It deploys a Deno-based, in-memory loader designed to evade detection by most security tools.

Attack Regions



Attack Details

#1

LeakNet, a ransomware group first seen in November 2024, has shifted how it gains access to victims. Instead of relying on third-party brokers for stolen credentials, it now uses ClickFix social engineering. This method appears on compromised but otherwise legitimate websites, where visitors are shown a fake verification page. The page instructs users to run a command on their system, unknowingly triggering the attack. This approach allows LeakNet to scale its operations, reduce costs, and infect any user who happens to visit the site, regardless of industry.

#2

After execution, a malicious payload installs a second-stage loader built on the Deno runtime, a legitimate developer tool. LeakNet exploits this trust by installing the signed Deno application and running hidden code through it. The malicious script is encoded and never stored as a normal file, making detection difficult. The process is launched through scripts, then gathers system details such as username, device name, memory, and operating system. This data is used to create a unique identifier before connecting to attacker-controlled servers, retrieving further instructions, and maintaining ongoing communication.

#3

Once inside, LeakNet follows a consistent attack pattern. It uses DLL side-loading, placing a harmful file alongside a legitimate program so that trusted processes unknowingly execute it. This helps the activity blend into normal system behavior. The malware then connects to external servers using predictable patterns, which creates a potential point for detection. Before spreading, it checks existing credentials on the system to identify accessible accounts and services.

#4

For lateral movement, LeakNet uses standard administrative tools to move across the network. Stolen data is staged and transferred using cloud storage services, allowing the activity to appear as normal traffic. Each step of the attack relies on trusted tools and services, making detection harder. A similar method was also seen in a separate attempt using phishing through messaging platforms, suggesting either an expansion of tactics or wider adoption of this approach by other threat actors.

Recommendations

Limit PsExec Usage to Authorized Administrators: Create a Group Policy Object (GPO) to restrict PsExec execution to authorized administrator accounts only. LeakNet relies on PsExec for lateral movement, and limiting its availability to a small set of authorized users significantly disrupts the group's ability to propagate through the network.

Monitor for Anomalous Deno Runtime Execution: Deploy behavioral detection rules to alert on Deno.exe execution outside of designated development environments. Focus on suspicious command-line arguments (particularly base64-encoded data URLs), unexpected parent-child process chains (e.g., msiexec spawning PowerShell or VBS scripts leading to Deno), and outbound network connections from Deno processes to unrecognized infrastructure.

Detect DLL Side-Loading in Non-Standard Directories: Create detection rules for jli.dll being loaded from C:\ProgramData\USOShared or other non-standard directories. A legitimate Java process loading jli.dll from a Windows Update-associated directory is anomalous and should trigger an alert for immediate investigation.

Detect Credential Enumeration via klist: Alert on the execution of "cmd.exe /c klist" on endpoints, as this built-in Windows command is used by LeakNet to enumerate active authentication credentials prior to lateral movement. While klist has legitimate uses, its execution in combination with other post-exploitation indicators should be investigated immediately.

Monitor Outbound Connections to S3 Buckets: Implement network monitoring to detect unexpected outbound connections to Amazon S3 bucket URLs from systems that do not have a legitimate business need for cloud storage access. LeakNet uses S3 for payload staging and data exfiltration, leveraging the appearance of normal cloud traffic to evade detection.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.001: PowerShell
		T1059.005: Visual Basic
Defense Evasion	T1218: System Binary Proxy Execution	T1218.007: Msiexec
	T1574: Hijack Execution Flow	T1574.001: DLL
	T1620: Reflective Code Loading	
Discovery	T1087: Account Discovery	
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Collection	T1560: Archive Collected Data	
Impact	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	apiclofront[.]com, sendtokenscf[.]com, binclloudapp[.]com, neremedysoft[.]com, ndibstersoft[.]com, windowallclean[.]com, cnoocim[.]com, delhedghogeggs[.]com, serialmenot[.]com, crahdhduf[.]com, weaplink[.]com, okobojirent[.]com, mshealthmetrics[.]com, verify-safeguard[.]top, fastdlvrss[.]s3[.]us-east-1[.]amazonaws[.]com, backupdailyawss[.]s3[.]us-east-1[.]amazonaws[.]com, tools[.]usersway[.]net
IPv4	144[.]31[.]2[.]161, 87[.]121[.]79[.]6, 87[.]121[.]79[.]25, 144[.]31[.]54[.]243, 144[.]31[.]224[.]98, 194[.]31[.]223[.]42
File Path	C:\ProgramData\USOShared\jli.dll
File Name	Romeo*.ps1, Juliet*.vbs
URL	hxxps[:]//[DOMAIN]/*/intake/organizations/events?channel=app
TOR Address	nleakk6sejx45jxtk7x6iyt65hwvfrkifc5v7ertdlwm3gttbpvlvxqd[.]onion

Recent Breaches

https://www.cisf.ch/
https://www.hb-brantner.at/de/
https://www.sunnydayssunshinecenter.com/
https://www.sandhaccounting.com/
https://www.barryequipment.com/
https://rmga.be/
https://www.nthconsultants.com/
https://www.alpinelumber.com/
https://www.bancovimenca.com/
https://www.bococ.org.cy/
https://sirioamericas.com/

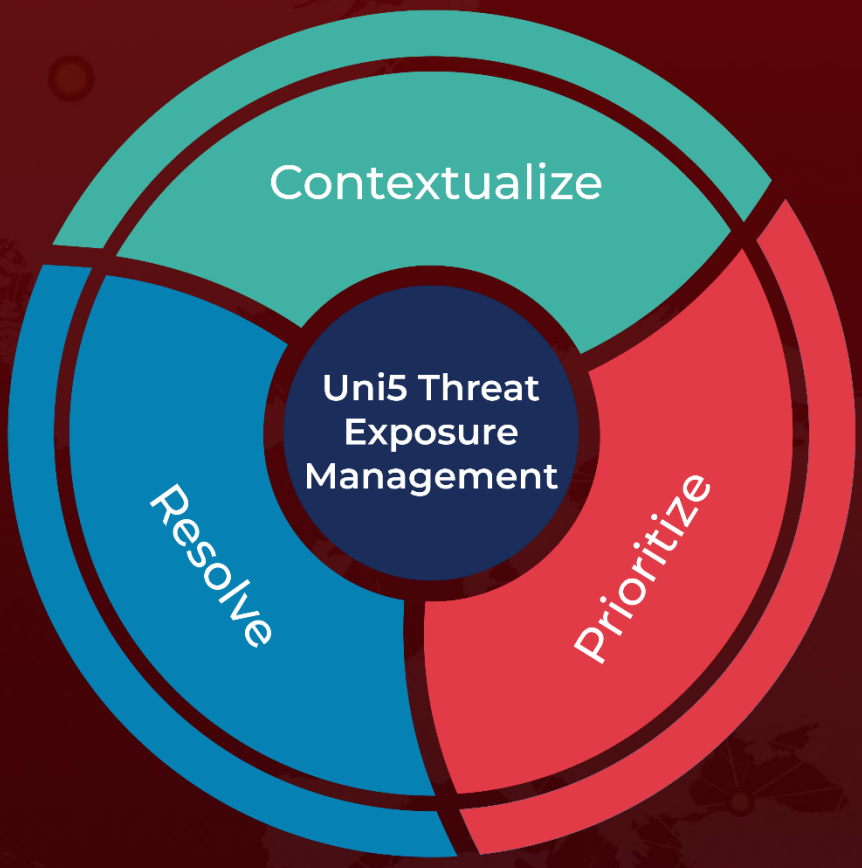
References

https://reliaquest.com/blog/threat-spotlight-casting-a-wider-net-clickfix-deno-and-leaknets-scaling-threat

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

March 18, 2026 • 06:00 AM

More at www.hivepro.com