Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

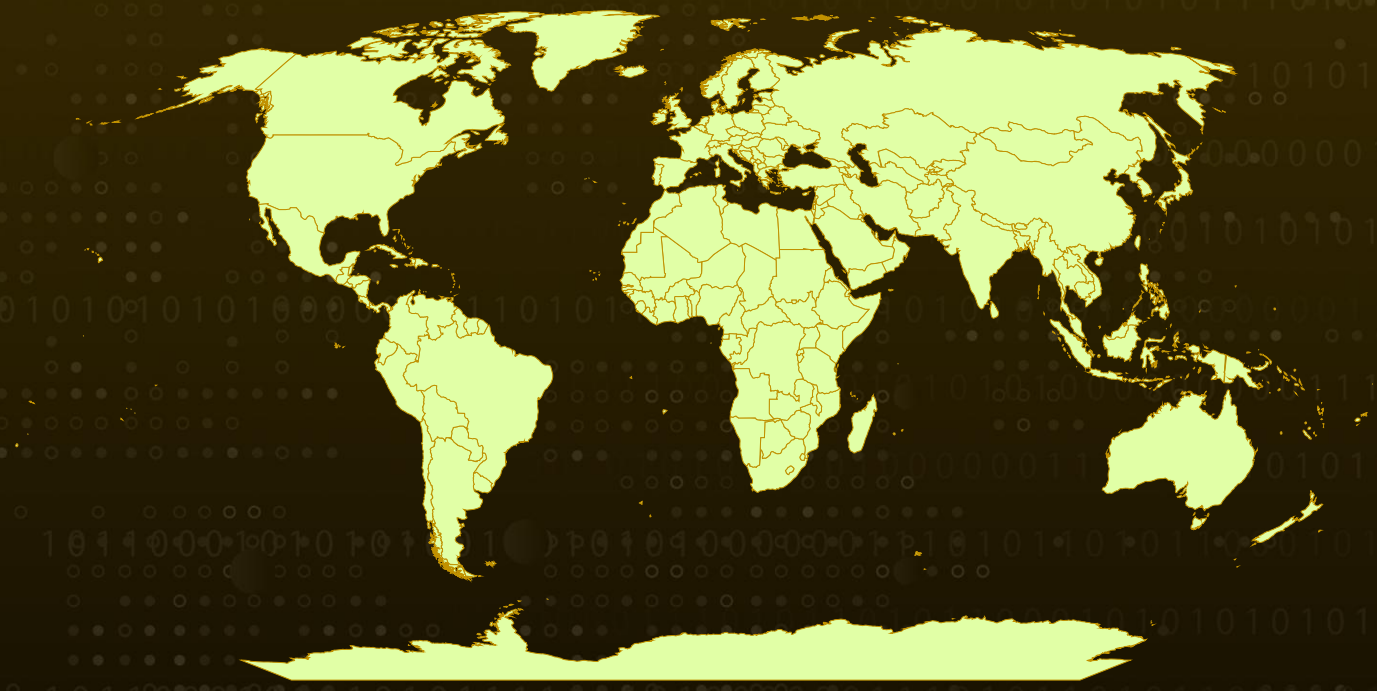
NordDragonScan Turns Simple Lures into Silent Data Heists

Date of Publication	Admiralty Code	TA Number
July 15, 2025	A1	TA2025218

Summary

Attack Commenced: February 2025
Affected Platforms: Microsoft Windows
Targeted Browsers: Chrome, Firefox
Targeted Regions: Worldwide
Malware: NordDragonScan infostealer
Attack: NordDragonScan, a newly identified information-stealing malware, is actively targeting systems through malicious HTA scripts delivered via deceptive shortened links. This .NET based threat is engineered to quietly harvest sensitive data. Leveraging varied decoy documents and persistent delivery mechanisms, it reflects the increasing complexity and precision of targeted cyber-espionage campaigns in 2025.

Attack Regions



Attack Details

#1 A newly identified information-stealing malware, NordDragonScan, is being actively distributed via a malicious website hosting a weaponized HTA script. The infection chain begins with shortened links redirecting to a domain that delivers a RAR archive containing a malicious LNK shortcut.

#2 This shortcut silently launches mshta.exe, executing an HTA payload that downloads decoy content while deploying a hardcoded malicious executable. The malware systematically profiles infected systems, harvesting documents, Chrome and Firefox browser data, capturing screenshots, and exfiltrating the collected data over TLS to a command-and-control (C2) server.

#3 Multiple themed decoys hosted on the attacker's infrastructure use the same payload to broaden infection opportunities and evade detection. NordDragonScan is a .NET executable featuring custom string obfuscation and an embedded PDB path.

#4 It creates a local working directory to stage stolen data and establishes persistence through a registry entry. After retrieving a dynamic C2 endpoint, it conducts local reconnaissance, collects targeted data, and uploads it via a POST request.

#5 This campaign reflects a methodical, opportunistic approach by the threat actor, leveraging diverse lure themes and persistent infrastructure to maximize infection rates while employing basic evasion techniques.

Recommendations

Strengthen Email and Web Gateway Protections: Given that the NordDragonScan campaign relies heavily on shortened URLs, malicious RAR archives, and deceptive shortcut files, organizations should reinforce their email and web filtering systems. Actively monitor for shortened URL services redirecting to unknown or high-risk domains. Implement real-time URL analysis and sandboxing solutions to automatically detonate and inspect attachments and links before delivery to endpoints.

Prioritize Browser Data Protection and Session Isolation: The malware targets browser profiles from Chrome and Firefox to steal sensitive session data, credentials, and browsing histories, organizations should enforce secure browser configurations. Encourage the use of password managers that isolate credentials from browser stores.

Monitor Outbound Connections: Track encrypted POST requests and outbound traffic to unknown or suspicious domains, as NordDragonScan uses TLS to exfiltrate data to dynamic C2 servers. Implement DNS filtering, anomaly detection, and firewall rules to block unexpected connections. Configure SIEM and network monitoring tools to alert on unusual data transfers from user directories or unauthorized processes.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1204** User Execution	**T1059** Command and Scripting Interpreter	**T1112** Modify Registry
T1204.002 Malicious File	**T1204.001** Malicious Link	**T1047** Windows Management Instrumentation	**T1059.001** PowerShell
T1547.001 Registry Run Keys / Startup Folder	**T1036** Masquerading	**T1027** Obfuscated Files or Information	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1113** Screen Capture	**T1119** Automated Collection	**T1041** Exfiltration Over C2 Channel
T1056 Input Capture	**T1074** Data Staged	**T1074.001** Local Data Staging	**T1568.003** DNS Calculation
T1218.005 Mshta			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	secfileshare[.]com, kpuszkiev[.]com
SHA256	2102c2178000f8c63d01fd9199400885d1449501337c4f9f51b7e444aa6fbf50, e07b33b5560bbef2e4ae055a062fdf5b6a7e5b097283a77a0ec87edb7a354725, 3f3e367d673cac778f3f562d0792e4829a919766460ae948ab2594d922a0edae, f8403e30dd495561dc0674a3b1aedaea5d6839808428069d98e30e19bd6dc045, fbffe681c61f9bba4c7abcb6e8fe09ef4d28166a10bfeb73281f874d84f69b3d, 39c68962a6b0963b56085a0f1a2af25c7974a167b650cf99eb1acd433ecb772b, 9d1f587b1bd2cce1a14a1423a77eb746d126e1982a0a794f6b870a2d7178bd2c, 7b2b757e09fa36f817568787f9eae8ca732dd372853bf13ea50649dbb62f0c5b, f4f6beea11f21a053d27d719dab711a482ba0e2e42d160cefdbdad7a958b93d0
Filename	Укрспецзв_Акт_30_05_25_ДР25_2313_13 від 26_02_2025.rar, Act300525.doc, adblocker.exe, SPicture.png
File Path	C:\Users\Public\Documents\install.exe, %USERPROFILE%\AppData\Local\Temp\adblocker.exe, C:\Users\NordDragon\Documents\visual studio
User-Agent	RTYUghjNM

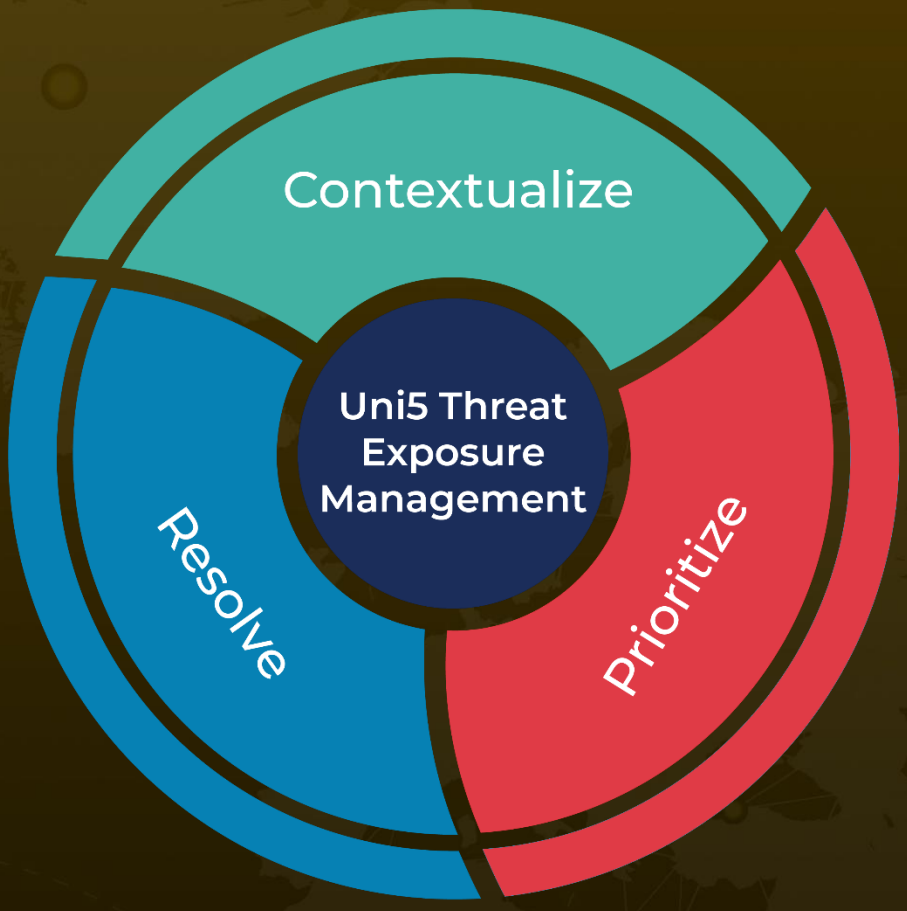
References

https://www.fortinet.com/blog/threat-research/norddragonscan-quiet-data-harvester-on-windows

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 15, 2025 • 4:00 AM

More at www.hivepro.com