Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

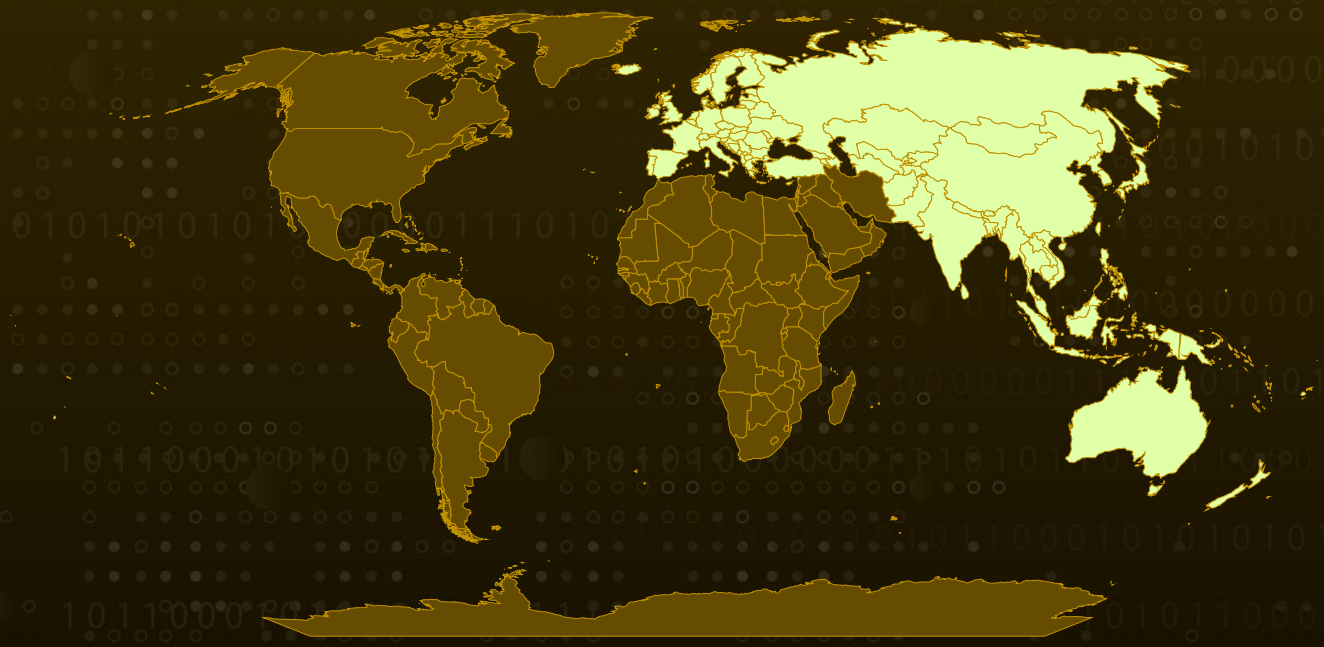
Noodlophile Stealer Advances with Obfuscation, Social Media Deception

Date of Publication	Admiralty Code	TA Number
August 19, 2025	A1	TA2025253

Summary

Attack Discovered: 2025
Targeted Countries: U.S., Europe, Baltic countries, and the Asia-Pacific (APAC) region
Malware: Noodlophile Stealer
Attack: The Noodlophile campaign has steadily matured into a global, multi-layered operation blending social engineering with technical stealth. Posing as urgent copyright infringement notices, attackers trick victims into clicking malicious links or opening disguised files, often delivered through Dropbox. Behind the scenes, they exploit vulnerable applications for DLL side-loading, use obfuscated scripts and portable Python interpreters for persistence, and rely on Telegram-based command-and-control to evade detection. At its core, the Noodlophile Stealer aggressively harvests browser data, credentials, payment details, and system information, while deploying techniques to bypass security defenses and erase its tracks. The campaign's evolving toolkit and AI-driven lures highlight its developers' intent to keep it adaptable, persistent, and increasingly dangerous to enterprises with visible online footprints.

Attack Regions



Attack Details

#1 The Noodlophile campaign, which has quietly persisted and has grown into a far more sophisticated operation. Once limited in scope, it now leans heavily on advanced spear-phishing tactics, most recently masquerading as copyright infringement notices to trick victims into acting quickly. With the use of multilingual lures, AI-powered localization, and a wider global reach, the threat actors have sharpened their approach to deliver the latest variant of the Noodlophile Stealer. Their targeting has expanded across enterprises in the US, Europe, the Baltics, and the Asia-Pacific region.

#2 A notable hallmark of the campaign is its reliance on social media-themed deception. Attackers send tailored phishing emails that impersonate copyright violation warnings for Facebook Pages, exploiting the reputational risks that such claims carry. Using Gmail accounts and carefully crafted details, the messages pressure recipients to open malicious links disguised as “evidence” files.

#3 Beyond email trickery, the technical execution is equally refined. The attackers leverage legitimate applications vulnerable to DLL side-loading, such as Haihaisoft PDF Reader and Excel converters, to smuggle their payloads. Through recursive stub loading and chained DLL exploits, malicious components are stealthily introduced into the system. Often, these payloads are distributed via Dropbox links, camouflaged as everyday file types like .docx or .png.

#4 After DLL side-loading, an intermediate stage emerges in the form of BAT scripts and portable Python interpreters, which set the groundwork for persistence. Registry modifications ensure the malware survives reboots, while disguised downloads from remote servers continue the compromise. These interpreted scripts serve as short-liners, handing off to further obfuscated components that intensify evasion and prepare for the stealer’s deployment.

#5 Further sophistication comes from the use of obfuscated batch and command scripts, often disguised as document files, which enable dynamic payload delivery. Hosting the final malware on free file-sharing platforms adds resilience against takedowns, while the adoption of Telegram-based command-and-control complicates detection even further.

#6 At the heart of the operation is the Noodlophile Stealer itself, a potent data-harvesting tool that zeroes in on browser-based information. It siphons credentials, cookies, credit card details, system metadata, and security configurations from multiple browsers. In some cases, it deploys a .NET executable to disable monitoring mechanisms. Persistence is maintained via the Startup directory, while self-deletion routines erase forensic traces post-execution. The malware’s unfinished functions hint at rapid development, suggesting its authors are actively preparing for future iterations.

Recommendations

Be cautious with urgent copyright claims: If you or your team receive emails claiming copyright violations, especially on platforms like Facebook, pause before clicking any links. Real copyright notices usually come directly from the platform itself, not through random Gmail accounts. Verify through official channels before taking any action.

Double-check attachments and shared links: The campaign often hides malware inside files that look like harmless documents (.docx) or images (.png). Always scan attachments with updated security tools and avoid downloading files from unknown Dropbox or drive links.

Harden your defenses around browsers: The Noodlophile Stealer specifically targets browser data, passwords, cookies, and credit card details. Encourage users to use password managers instead of storing credentials in browsers and enable multi-factor authentication (MFA) wherever possible to reduce the impact of stolen passwords.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1566.002 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File	T1574 Hijack Execution Flow

T1574.001 DLL	T1036 Masquerading	T1588 Obtain Capabilities	T1588.007 Artificial Intelligence
T1560 Archive Collected Data	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1059.006 Python
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information	T1132 Data Encoding
T1132.001 Standard Encoding	T1113 Screen Capture	T1056 Input Capture	T1056.001 Keylogging
T1057 Process Discovery	T1217 Browser Information Discovery	T1070 Indicator Removal	T1082 System Information Discovery
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1567 Exfiltration Over Web Service	T1071 Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//is[.]gd/PvLoKt, hxxps[:]//paste[.]rs/Gc2BJ, hxxp[:]//196.251.84[.]144/suc/zk2[.]txt, hxxps[:]//t[.]ly/cCEsy, hxxps[:]//tinyurl[.]com/yy2smhn2, hxxps[:]//t2m[.]io/SiemensAG, hxxps[:]//t[.]ly/RossiDoria&Associati, hxxps[:]//t2m[.]io/Ob4WBcu, hxxps[:]//t[.]ly/vqpvk, hxxps[:]//goo[.]su/aSqtBmg, hxxps[:]//tinyurl[.]com/yrnsdpfk, hxxps[:]//tinyurl[.]com/2jaj3kws, hxxps[:]//t2m[.]io/9zPbQxa, hxxps[:]//t[.]ly/EidCollection1112, hxxps[:]//tinyurl[.]com/yz6yy4ta, hxxps[:]//t[.]ly/rsyAl, hxxps[:]//t[.]ly/TimbrGroup,

TYPE	VALUE
URLs	hxxps[:]//www.dropbox[.]com/scl/fi/e21ecfnbmg49fvqp4ouyd/Prove della violazione delle clausole sul copyright a te destinate[.]zip?rlkey=<key>&dl=1, hxxp[:]//15[.]235[.]172[.]219/vmeo/link/dcaathur[.]txt, hxxp[:]//15[.]235[.]172[.]219/vmeo/getlink?id=dcaathur, hxxp[:]//196[.]251[.]84[.]144/suc/And_st[.]txt, hxxp[:]//160[.]25[.]232[.]62/vmeo/getlink?id=bee02h, hxxp[:]//160[.]25[.]232[.]62/bee/BEE02_H[.]txt, hxxp[:]//196[.]251[.]84[.]144/suc/zk2[.]txt, hxxps[:]//pastebin[.]pl/view/raw/ae4cceca, hxxps[:]//t[.]me/LoneNone, hxxps[:]//0x0[.]st/8fVG[.]txt
SHA256	CE69FA159FB53C9A7375EF66153D94480C9A284E373CE8BF22953268F21B2EB2, FAC94A650CD57B9E8DA397816FA8DDD3217DD568EABA1E46909640CBF2F0A29C, A05CF0002A135ADE9771A1AA48109CC8AA104E7AFA1C56AF998F9ABA2A1E3F05, 2E610C97E5BAE10966811B78FC9E700117123B6A12953BF819CED9B25EB9A507, 0BA36C80167919A98CFFC002CF6819D3F5E117207E901AEBD13E3EA54387E51F, 693789E4B9FB280FA32541E9A548B7FEFD98775B8F075E370464DB3764BB15B9, 69D6582D7550817F792F3287FA91788E7B9252B63D81A380A5E1CA9AA0629150, b3aa210a51e19dd003d35721a18b7fb5c0741dce01dd7725ff610de4adf0a8f2, 95D964EFC32DD04B5AE05BFC251CE470E8C418398EFC97697F41807F33E7390D, C213A15ADD88E8C1CBB06FC4690C02046FA74027848BCB97C7D961FFC21155C6, 9F2205E06231CF53824421AA09E6A43D5A9C5513618E08E4EAACFD94B91C5E61, AF2DFA1FCD055AAF0C818F49C7C4F4370629AC6EECADBCD532A1149A7E01EC11, 707223112E8CED786E7D1ED43224E73606B3E2EFEC615BB3A22FE8CC11D3BB54, 3C3CEE4579E78C9D39B96804815C71C7A2DE17951E08D703197C9C7ED20AB9F3, d0b0551e8988a9f81b80933ec68efabb47cd12acaeffa79c42564863424a376e, 844C2EE464EF5CDC79C2DE52EB544C55E1F9BF7DED2C2F0E44BED263F04DAA42,

TYPE	VALUE
SHA256	5AD456333451FCBD69977A62D4728B1FC8B5BDEBEE763D2B6725226078DAEAF8, 320555e241025b8427e1a3ccfc62f0c5a2347cfd86d29f33709192e2e9cbbac2, a6647dd104487deb71674c64d8a2b03843cd3d32ee2c9a63cc3ea506d8b00552

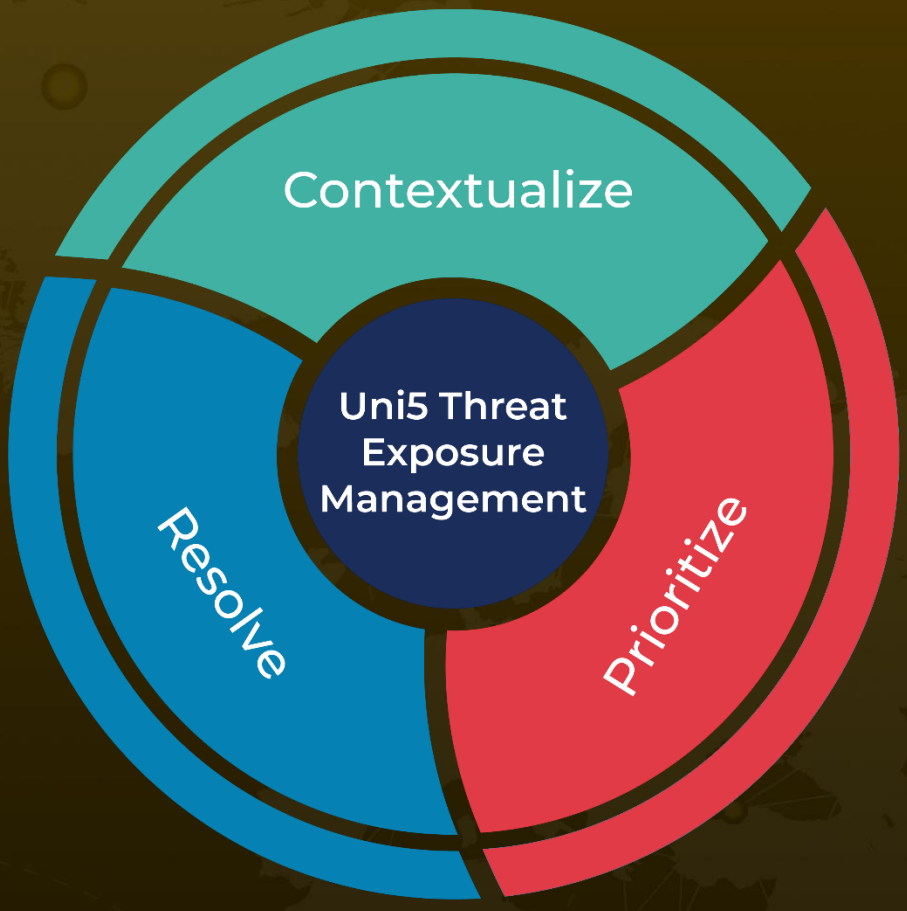
References

https://www.morphisec.com/blog/noodlophile-stealer-evolves-targeted-copyright-phishing-hits-enterprises-with-social-media-footprints/

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

August 19, 2025 • 5:30 AM

More at www.hivepro.com