# Noodlophile Stealer evolution - Security Affairs - Against Invaders - Notícia

Data: 2025-08-19 18:42:22

Autor: Inteligência Against Invaders

## Noodlophile Stealer evolution

## Noodlophile malware spreads via copyright phishing, targeting firms in the U.S., Europe, Baltics & APAC with tailored spear-phishing lures.

The Noodlophile malware campaign is expanding globally, using spear-phishing emails disguised as copyright notices. Threat actors tailor lures with details like Facebook Page IDs and company ownership data. Active for over a year, it now targets enterprises in the U.S., Europe, the Baltics, and APAC.

In May, Morphisec researchers observed attackers exploiting AI hype to spread malware via fake AI tools promoted in viral posts and Facebook groups. Users seeking free AI video tools unknowingly download Noodlophile Stealer, a new malware that steals browser credentials, crypto wallets, and may install remote access trojans like XWorm.

At the time, the experts pointed out that Noodlophile Stealer was a previously undocumented malware. Noodlophile is being sold on cybercrime forums as part of malware-as-a-service schemes, often bundled with tools for credential theft. The developer, likely Vietnamese, has been seen actively engaging in related Facebook posts.

Fake AI tools spread via social media and scam websites like “Dream Machine” or “CapCut” bait users into uploading media.

The latest Noodlophile campaign, active for over a year, now leverages advanced spear-phishing emails posing as copyright infringement notices, tailored with reconnaissance-derived details like specific Facebook Page IDs and company ownership information. Unlike its earlier iteration, which used fake AI video generation platforms, this campaign employs multilingual lures (potentially AI-crafted), broader global outreach, and upgraded delivery mechanisms to deploy an enhanced Noodlophile Stealer.

Noodlophile now exploits legit software flaws, uses Telegram for staging, and delivers dynamic payloads via urgent Gmail lures claiming Facebook copyright violations.

*“This campaign capitalizes on enterprises’ reliance on social media by sending highly personalized spear phishing emails that allege copyright violations on specific Facebook Pages.” reads the report published by Morphisec.*

*“These emails, often originating from Gmail accounts to evade suspicion, include precise details such as Page IDs and ownership information, indicating extensive reconnaissance. The urgent tone and legal threats pressure recipients-typically employees or generic contact and marketing inboxes*

*like info@ or support@-to click malicious links disguised as evidence files (e.g., “View Copyright Infringement Evidence.pdf”).”*

The new Noodlophile campaign exploits DLL side-loading in signed apps like Haihaisoft PDF Reader, using recursive stub loading and chained DLL flaws. Attackers often hide payloads in Dropbox archives, Dropbox links are masked by TinyURL. The payloads are disguised as .docx or .png files, enabling covert execution inside trusted processes.

After the side-loading of malicious DLLs, Noodlophile uses an intermediate stage: files disguised as .pptx/.docx are renamed to BAT scripts and Python interpreters. The BAT scripts set persistence via registry keys and, in some cases, fetch more fake “PDF” or “PPTX” files from remote servers. These scripts then run malicious Python code, seamlessly moving to the next obfuscated stage.

Morphisec experts pointed out that in this campaign, threat actors ramp up obfuscation. Malicious scripts disguised as .docx files no longer fetch payloads directly, but instead extract download links hidden in Telegram group descriptions.

*“Instead of directly downloading the next stage, these scripts extract a URL from the description of a Telegram group, enabling dynamic execution of the payload. The final stealer is hosted on free platforms like https://paste[.]rs/Gc2BJ, a tactic that complicates detection and takedown.” continues the report.*

*“This approach builds on the previous campaign’s techniques (e.g., Base64-encoded archives, LOLBin abuse like certutil.exe), but adds layers of evasion through Telegram-based command-and-control and in-memory execution to avoid disk-based detection.“*

The final stealer is then pulled from free hosting sites like Paste.rs, making takedowns harder. Compared to earlier waves, this version adds stronger evasion—leveraging Telegram for staging, in-memory execution, and LOLBin abuse—to stay under the radar.

The Noodlophile Stealer is evolving fast, the malware code includes placeholders for future functions like screenshot capture, keylogging, file exfiltration, and even file encryption. It already targets sensitive browser data, including cookies, credentials, and credit cards, with a strong focus on stealing Facebook cookies.

The malware also gathers system info, checks installed security tools, and ensures persistence while deleting traces to evade detection. Its code suggests rapid expansion, making it a growing threat to enterprises.

*“These unimplemented functions indicate that the stealer’s developers are actively working to expand its capabilities, potentially transforming it into a more versatile and dangerous threat.” concludes the report.*

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking, malware)