

HiveForce Labs

THREAT ADVISORY

 **ATTACK REPORT**

Operation Hanoi Thief: When Fake CVs Become Cyber Weapons

Date of Publication

December 2, 2025

Admiralty Code

A1

TA Number

TA2025365

Summary

Attack Discovered: November 3, 2025

Targeted Country: Vietnam

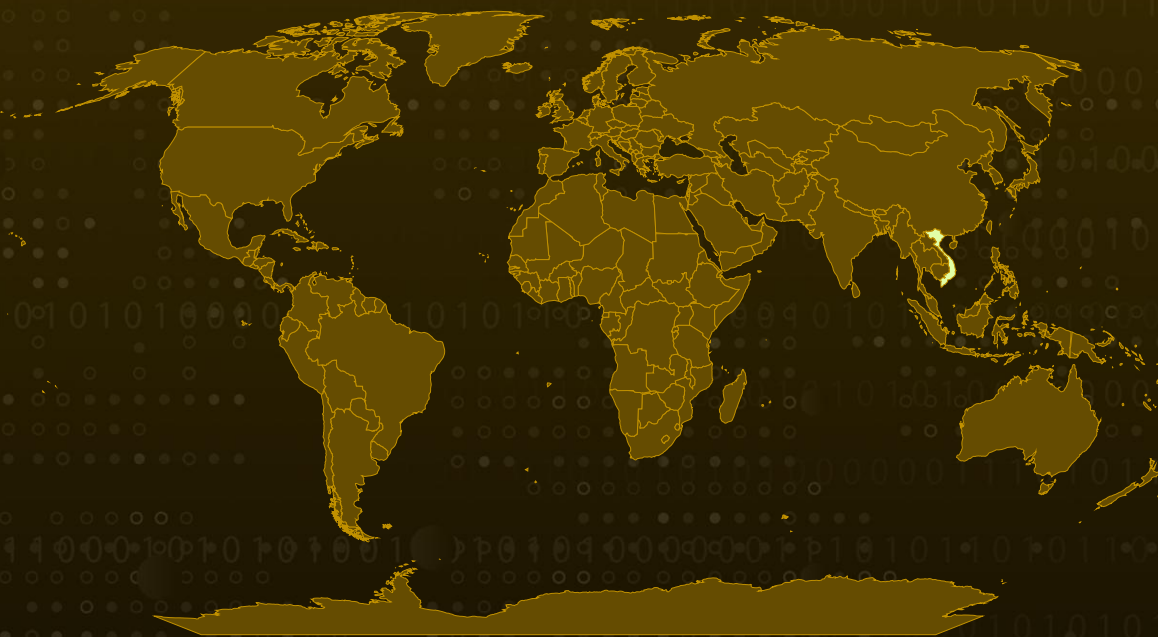
Targeted Industries: Information Technology, Recruitment & HR Firms

Malware: LOTUSHARVEST

Campaign: Operation Hanoi Thief

Attack: Operation Hanoi Thief is a deceptive spear-phishing campaign that hides behind seemingly harmless resumes to infiltrate Vietnamese IT and recruitment teams. By blending clever misdirection like fake GitHub profiles and resume-themed lures, with pseudo-polyglot payloads and abused Windows tools, the attackers quietly execute a malicious DLL implant called LOTUSHARVEST. Once inside, the implant slips past analysis checks, harvests browser credentials and browsing history, and sends the stolen data back to attacker-controlled servers. With its polished social engineering, stealthy execution chain, the campaign makes it a strong reminder that even the most routine HR workflows can become an entry point for sophisticated cyber espionage.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, NavInfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin

Powered by Bing

Attack Details

#1

Operation Hanoi Thief is an emerging spear-phishing campaign that has begun targeting IT teams and HR recruiters across Vietnam. The attackers rely heavily on fake resumes carefully crafted to appear legitimate while embedding pseudo-polyglot payloads designed to camouflage malicious activity. The infection chain begins with a lure-packed ZIP archive delivered through targeted emails. Inside, victims find a convincing resume document and an accompanying LNK shortcut that quietly initiates the intrusion. What follows is the deployment of LOTUSHARVEST, a C++ based DLL implant executed through DLL sideloading.

#2

The first malicious archive publicly identified surfaced on November 3, 2025. It contained an LNK file disguised as a PDF and a pseudo-polyglot lure. Although the resume portrays an applicant for a software developer role, the file name hints at an information-security background, suggesting the attackers tailored the lure to specific technical targets. To make the applicant appear authentic, the adversaries even included a dormant GitHub profile created years earlier, likely fabricated solely to reinforce credibility. Once the victim opens the shortcut file, it silently triggers a chain of commands that abuses a legitimate Windows binary to run embedded batch instructions in the background.

#3

The pseudo-polyglot file itself is engineered to confuse both human reviewers and automated scanners. Some tools read it as plain text; others recognize it as a PDF. A closer look shows malicious scripts placed before the PDF headers, enabling execution without raising suspicion. These scripts misuse trusted binaries to conceal command prompts, rename system files, and manipulate the lure so it appears harmless. They then retrieve, decode, and deploy a malicious DLL named MsCtfMonitor.dll into C:\ProgramData, where a copied version of ctfmon.exe loads it through DLL sideloading. This process ultimately launches the LOTUSHARVEST implant.

#4

Once active, LOTUSHARVEST operates as a stealthy information stealer equipped with multiple layers of anti-analysis safeguards. It checks for virtual environments, debugger presence, and even generates fake exceptions to confuse analysts and disrupt sandboxing. When running on a real machine, the implant collects browser-stored credentials, recently visited URLs, and local system identifiers such as the computer name and username. Using the WinINet API, it exfiltrates this information over HTTPS to attacker-controlled domains, many of them randomly generated subdomains hosted on services like Pipedream and RequestRepo.

#5

While attribution remains ongoing, the campaign's TTPs echo previous activity linked to likely Chinese threat groups that have historically used fake CVs, niche lure themes, and similar C2 infrastructure. However, the LOTUSHARVEST implant stands out from more familiar Chinese-linked tooling such as PlugX, calling for measured judgment. Operation Hanoi Thief underscores how threat actors continue to exploit everyday workflows like recruiting and resume screening to infiltrate high-value environments with quietly innovative techniques.

Recommendations



Treat Unexpected Resumes with Caution: If you receive a CV from an unknown sender, especially in ZIP format, pause before opening it. Verify the sender on LinkedIn or through official company channels. If anything feels off, flag it to your security team.



Disable Risky File Types For HR and IT Teams: Block or restrict formats like .lnk, .bat, and .exe from reaching inboxes. Most HR teams don't need these file types, and removing them cuts off a major attack path used in this campaign.



Use a Safe, Isolated System for Reviewing Attachments: Encourage HR or recruitment teams to open resumes in a protected environment, like a sandbox or a virtual machine, so suspicious files cannot reach the main corporate network.



Strengthen Browser and Credential Protections: Since LOTUSHARVEST steals browser credentials, encourage employees to avoid storing passwords in browsers. Move to a secure password manager and enable MFA wherever possible.



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	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1587 Develop Capabilities	T1587.001 Malware
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File

<u>T1218</u> System Binary Proxy Execution	<u>T1036</u> Masquerading	<u>T1036.007</u> Double File Extension	<u>T1140</u> Deobfuscate/Decode Files or Information
<u>T1574</u> Hijack Execution Flow	<u>T1574.001</u> DLL	<u>T1082</u> System Information Discovery	<u>T1083</u> File and Directory Discovery
<u>T1217</u> Browser Information Discovery	<u>T1555</u> Credentials from Password Stores	<u>T1555.003</u> Credentials from Web Browsers	<u>T1005</u> Data from Local System
<u>T1041</u> Exfiltration Over C2 Channel	<u>T1071</u> Application Layer Protocol	<u>T1071.001</u> Web Protocols	<u>T1059</u> Command and Scripting Interpreter

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1beb8fb1b6283dc7fffedcc2f058836d895d92b2fb2c37d982714af648994fed, 77373ee9869b492de0db2462efd5d3eff910b227e53d238fae16ad011826388a, 693ea9f0837c9e0c0413da6198b6316a6ca6dfd9f4d3db71664d2270a65bcf38, 48e18db10bf9fa0033affaed849f053bd20c59b32b71855d1cc72f613d0cac4b

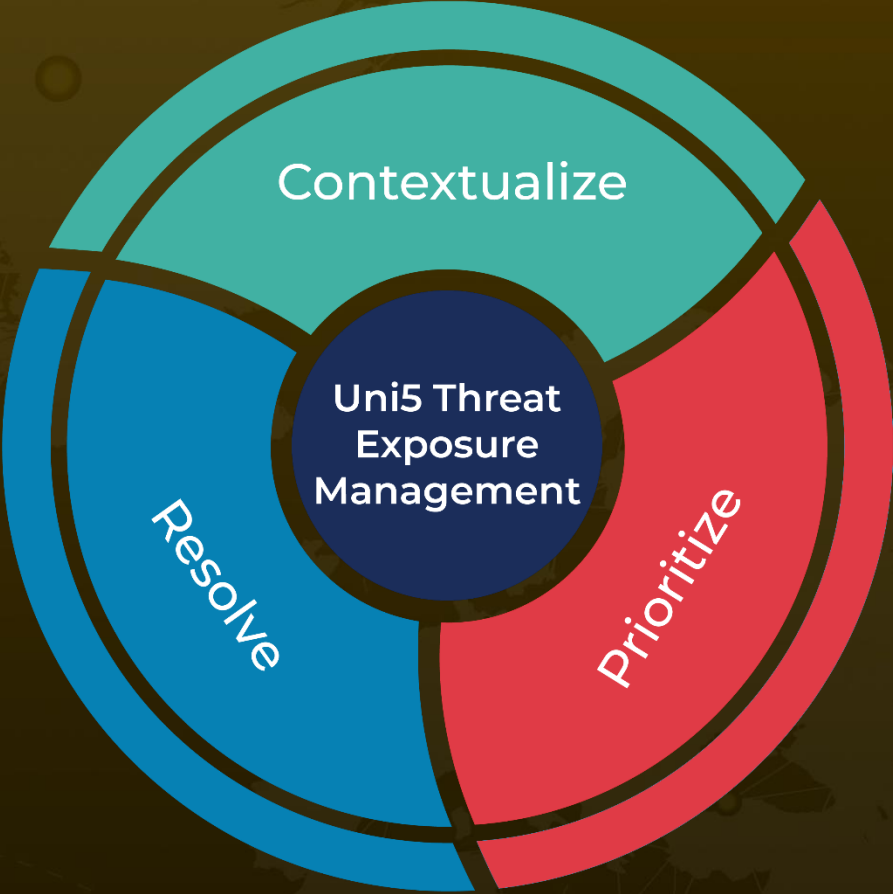
✂ References

<https://www.segrite.com/blog/9479-2/>

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

December 2, 2025 • 8:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com