Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

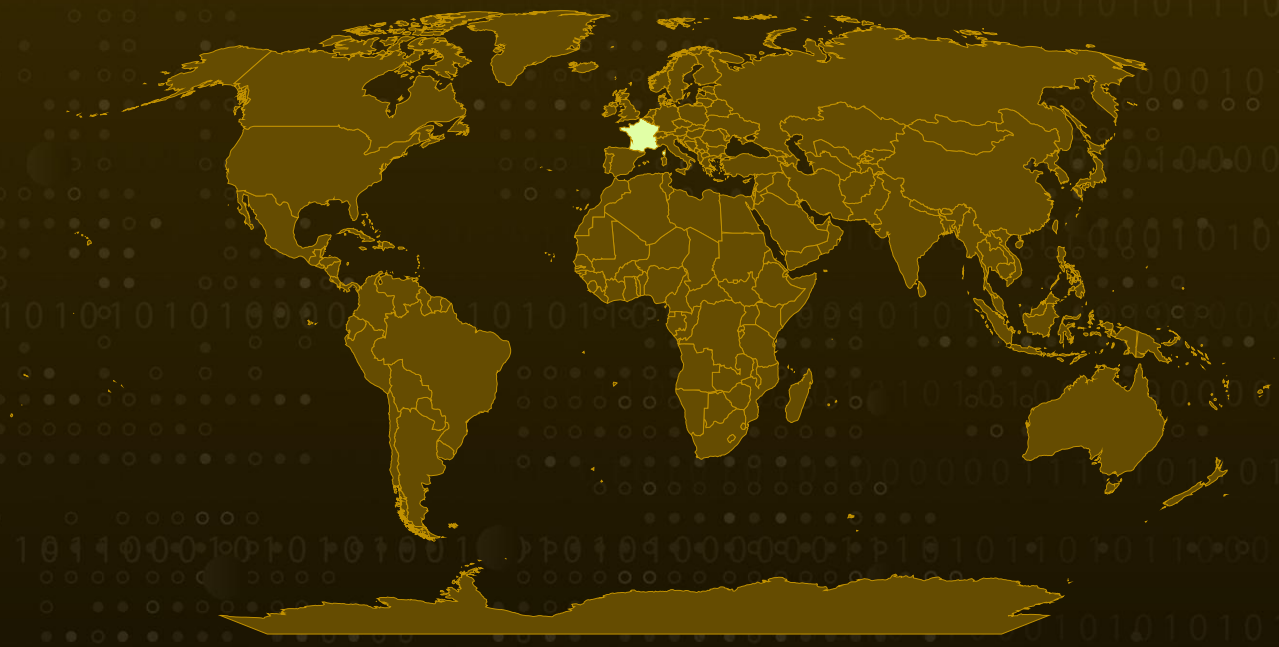
FAUX#ELEVATE: Obfuscated VBS Campaign Targeting Enterprise HR System

Date of Publication	Admiralty Code	TA Number
March 27, 2026	A1	TA2026086

Summary

First Seen: 2025
Targeted Region: France
Targeted Platform: Windows
Targeted Industries: Human Resources / Recruitment Departments
Campaign: FAUX#ELEVATE
Attack: What appears to be a harmless job application quickly unravels into a targeted enterprise compromise under the campaign FAUX#ELEVATE. Aimed at HR teams, the attack leverages a deeply obfuscated VBScript that quietly filters for domain-joined systems, ensuring it lands only on high-value corporate environments. Once executed, it disables key security defenses, establishes a backdoor, siphons credentials from multiple browsers, and deploys a stealthy cryptominer, all while exfiltrating sensitive data over encrypted email channels. The campaign stands out for its precision and discipline, evading sandbox analysis, bypassing low-value targets, and cleaning up its initial traces to leave behind a persistent foothold and a silent monetization pipeline.

Attack Regions



Attack Details

#1 What looks like an ordinary job application quickly turns into a carefully staged compromise. The FAUX#ELEVATE campaign attack begins with a phishing email targeting HR and recruitment teams, carrying a VBScript file. When opened, it displays a convincing French error message suggesting the file is corrupted, while quietly executing malicious code in the background. Beneath this simple lure lies heavy obfuscation; only a tiny fraction of the script's massive 224,000+ lines contains real logic, with the rest padded by meaningless comments. Critical strings are deliberately fragmented and reconstructed at runtime, making analysis and detection significantly harder.

#2 Before deploying its payload, the script performs a series of environment checks to ensure it is running on a valuable target. It avoids reinfecting systems using a mutex mechanism and, more importantly, verifies whether the machine is part of a corporate domain, effectively filtering out home users. Sandbox evasion is built in through timing checks that detect accelerated execution environments. If administrative privileges are missing, the script aggressively loops UAC prompts until elevation is granted. Once elevated, it weakens system defenses by disabling UAC, adding broad Windows Defender exclusions across multiple drives, and removing its own footprint from disk.

#3 With defenses lowered, the dropper retrieves additional components. It downloads a renamed 7-Zip utility along with two password-protected archives hosted on Dropbox, extracting them into a public system directory. These archives unpack a full toolkit: a backdoor for remote access, a Monero cryptominer, multiple credential stealers targeting Chromium-based browsers and Firefox, and utilities for harvesting desktop files. Notably, the credential theft mechanism leverages techniques to bypass Chromium's App-Bound Encryption, enabling the extraction of sensitive data such as cookies, saved credentials, and payment information without requiring elevated privileges.

#4 Exfiltration is handled with equal precision. Stolen data is bundled and sent via SMTP over SSL using hardcoded mail.ru accounts, with email subjects tagged by victim geography and data type for easy classification. Meanwhile, the cryptominer fetches its configuration from a compromised website, disguising it as an encoded image file to evade detection, and connects to a mining pool using stealth options that pause activity during user interaction. In parallel, the backdoor establishes persistent command-and-control communication via dynamic DNS infrastructure, ensuring continuous remote access.

#5 To maintain long-term control while minimizing exposure, the malware establishes multiple persistence mechanisms through registry keys and scheduled tasks. Once data theft is complete, it performs a thorough cleanup, removing scripts and tooling associated with the initial infection chain.

Recommendations

Block VBScript Execution via Group Policy: Configure Windows Group Policy to prevent wscript.exe and cscript.exe from executing VBS files downloaded from the internet. This directly mitigates the initial dropper execution vector used in this campaign where a .vbs file disguised as a resume is the entry point.

Monitor C:\Users\Public\ and Subfolders for Suspicious Activity: Deploy endpoint detection rules to alert on file creation, script execution, and binary drops within world-writable directories such as C:\Users\Public\WindowsUpdate\, which was used as the staging directory for the full malware toolkit in this campaign.

Detect Anomalous wscript.exe and cscript.exe Behavior: Create detection rules for wscript.exe or cscript.exe processes that spawn child processes (cmd.exe, powershell.exe, schtasks.exe, netsh.exe), make outbound network connections, modify registry Run keys, or invoke PowerShell with Add-MpPreference -ExclusionPath commands.

Monitor explorer.exe for Unexpected Outbound Connections: Create alerts for explorer.exe establishing network connections to non-Microsoft IPs, particularly on non-standard ports such as 7077 and 62046. In this campaign, the RAT component injected into explorer.exe for persistent C2 beaconing.

Restrict Dropbox and Cloud Storage Access on Endpoints Where Not Required: Where feasible, limit or monitor access to Dropbox CDN URLs from non-browser processes. The campaign uses Dropbox links for payload delivery, and blocking these at the proxy level for non-approved applications can disrupt the delivery mechanism.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1584: Compromise Infrastructure	T1584.004: Server
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1059: Command and Scripting Interpreter	T1059.005: Visual Basic
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
Defense Evasion	T1027: Obfuscated Files or Information	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1070: Indicator Removal	T1070.004: File Deletion
	T1055: Process Injection	
	T1102: Web Service	
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers

Tactic	Technique	Sub-technique
Discovery	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
Exfiltration	T1048: Exfiltration Over Alternative Protocol	T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Impact	T1496: Resource Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	46[.]105[.]76[.]166, 217[.]64[.]148[.]121, 141[.]94[.]96[.]71, 141[.]94[.]96[.]144, 94[.]100[.]180[.]160, 208[.]95[.]112[.]1, 172[.]67[.]69[.]226
Domains	eufr18-166[.]workdns[.]com, pool[.]supportxmr[.]com, pool-fr[.]supportxmr[.]com, lmtop[.]ma, fortrust-cf[.]ma, expressnegoce[.]ma

TYPE	VALUE
URLs	hxxps[:]//www[.]dropbox[.]com/scl/fi/w539fqxeew7p4tooxymd5/gmail2.7z, hxxps[:]//www[.]dropbox[.]com/scl/fi/00v09bc31ppk9tcr1c1fz/gmail_ma.7z, hxxps[:]//lmtop[.]ma/wp-content/uploads/2018/05/1300.png, hxxps[:]//pastebin[.]com/K9rHTWbB
Email Address	olga[.]aitsaid[@]mail[.]ru, 3pw5nd9neeyn[@]mail[.]ru, Vladimirprolitovitch[@]duck[.]com
SMTP Server	smtp[.]mail[.]ru[:]465
Monero Wallet	42VXdAiAeFvEsma3tjqbJ9P8o21fCE3f6fzDDVDRNmi4EK4iMKaFtoodb76rYobsn3WBAPZrXWCnsPf8JuNbNYHQ6C3Kypi, 47V66mBWCNsGrxS4jnevMbCzfaKW5mAaH5d9L8jem3SXFRcRKBFBMFRQpETVJdMPNUVDvAwzE8zi1HhQjnxED6vTFoo2yWu
SHA256	f33586a516e58b2f349dfd7743702f43f5e0ece769ed46088d3400d1b0f0b10b, 0863bd3878d0a0e6b809eccacffe83fa5b2ccccbef7830f956accd306a81298e, 24a1eacb0fbed9efb819567b7e25151384825d353254b31ec9d875694f7f53d4, 3c03ca8fb96c8e1c61e58a5c65d9eeda0f5bbe5c2faf4c021e7b704fe5917f29, 63bae4929da48baa903251966e3e6bc3b46c4c9fd70b4e8b171bde3218484362, 7578a9ff2b432f3fa9582d2adeb281eca73ce7ff73a48f8dbdc29c54e616c1de, 7a76eb82b564837c1bf43883a1d93ff7a2e9a56ecb0f093447593329e5200492, 7eb7c1d6b03522109517b94779019aedbf93d7e441883dfd09eb90e0709dc2ca, 7f48b81c923002827ffed90fd5ebb9bf98f38c00ca78b4921dab057d89fb1705, 7fc00bf9c5ca44e7708a0d1d56221fc564859ec3aa7f299c7f3c698cb4d580da, a1c56fc63d58c613115c298baca7da311f021e451c4394b08323b95572c2ecb6, a33bf25ece3360c4d75127aa032f20f5093fc2cd20fcb709f0370369fcf0b9dc,

TYPE	VALUE
SHA256	b25a969eb9bec5945cff6ebbfc76c3630635662c607e298645db3a4f26fd0665, b72a1fb2d8032fac898285e37085c6283eb2322d3c49aa35e6dac64836c1335e, c3ff6d497e1ffc65a56577afdc64984f61542faeeed6beb0a957539e48ee86ef, ee42c62af657c8ebe6096a8d4f8e2baf17a37648288ada7e903cdbf83c146560, 3c68e3d7a1eaf38cf4b4de68444cc005e03cba7ee86a76209f87efcf952d8211, 1ecaef416cc63d931eada6cf373cf24a4a405750b626ef29f7b031503b1f6270, 47d70838cbedc8b0e0634e51bde8a72035922bddc1177cc9210fa0adb967d6a2, 936583f5116bb46703ba8a4998157fbaa2af5a2d29f240ddda92be312403e940, 45eddd42646074db6ac073119c87df0d2a597666fa75f33580fa611724adadf2, fa58dced1d951f4f308248336aefb15727ea0dd09749ce5643d37c515733f8ee, 11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5, 866a0803d06c7941e9ae87cbe83c6d85267c43299b09b9edabf030d54bee2676, 853d8001c173520a7f459be73ac6bb7f0363db3beb7632f0a6059fb88b288b6a

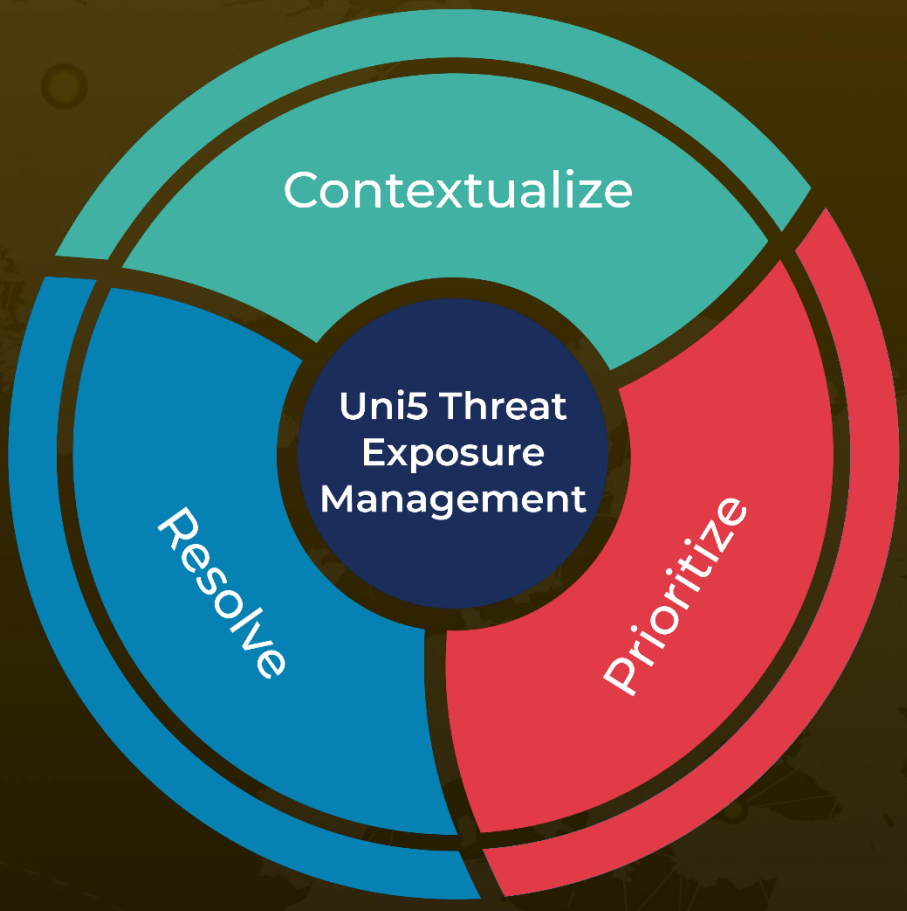
References

https://www.securonix.com/blog/faux-elevate-threat-actors-crypto-miners-and-infostealers/

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 27, 2026 • 8:00 AM

More at www.hivepro.com