Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

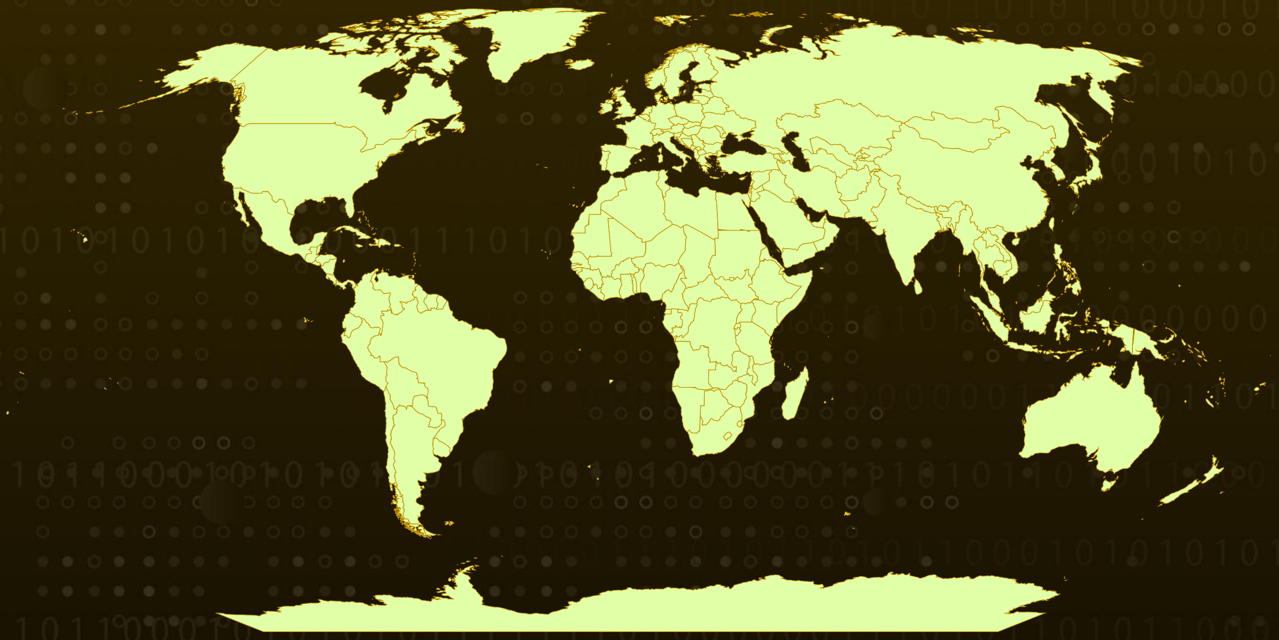
Click, Paste, Compromise: Inside the New FileFix Campaign

Date of Publication	Admiralty Code	TA Number
September 17, 2025	A1	TA2025284

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Malware: StealC
Attack: A new FileFix campaign has taken social engineering to the next level, luring Facebook users with fake "account appeal" pages and tricking them into pasting malicious commands into a file dialog. What looks like a simple PDF path instead launches a stealthy, multi-stage PowerShell chain that hides payloads inside AI-generated images, ultimately dropping the StealC malware to siphon passwords, wallets, and cloud keys. With obfuscation, steganography, and clever hosting on Bitbucket, this attack shows how fast *Fix techniques are evolving from proof-of-concepts into polished, real-world threats.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 A FileFix attack, a new variant of the ClickFix family, has been uncovered. Unlike the original proof of concept published in July 2025, this campaign departs from the reference implementation and demonstrates a significantly more polished operation. The adversary invested heavily in tradecraft, designing a convincing phishing portal, an evasive delivery chain, and a robust supporting infrastructure. Because many of the techniques here are transferable across ClickFix, FileFix, and related “*Fix” methods, this case serves as an important warning for defenders against social engineering and delivery mechanics.

#2 *Fix attacks trick victims into doing the attacker’s work, typically by copying and pasting commands or file paths into the local system. Think of it as a modern pickpocket who politely asks for your keys instead of stealthily lifting your wallet. ClickFix variants commonly bait victims with a fake CAPTCHA that instructs users to run a command via Win+R, while FileFix abuses file upload dialogs so victims paste a path into the File Explorer address bar. The user-facing prompts are deceptively simple, and their very simplicity makes them effective: fatigue and complex anti-bot checks lower suspicion and increase compliance.

#3 In the observed campaign, the lure targeted Facebook accounts. Victims received messages purporting to be from Facebook security, warning of imminent account suspension and offering an “appeal” that required an uploaded incident report. When users opened the file upload window and pasted what they believed was a PDF path, the input instead invoked a payload, a multistage PowerShell chain that downloaded an image, decoded embedded data, decrypted an executable, and ultimately executed additional shellcode.

#4 Technically, the attack was notable for heavy obfuscation and staging. The phishing site’s JavaScript was aggressively minified and fragmented, with randomized identifiers and multilingual translations intended to broaden its reach. Payloads were delivered as single-line, fragmented PowerShell commands, often Base64-obfuscated and XOR-encoded, with the core payload hidden inside seemingly innocuous JPG files. Those images contained compressed, encrypted second-stage scripts and binary payloads that the PowerShell loader extracted, decrypted using RC4 and gzip routines, and executed. The use of steganography and two-stage delivery increased stealth and complicated static detection.

#5 The final stage deployed a loader written in Go, which delivered the StealC infostealer. Its capabilities span information theft, credential harvesting, and dynamic payload loading, with attempts observed to exfiltrate browser data, wallet information, chat app data, cloud keys, and more. This campaign highlights how quickly *Fix techniques can mature from proof of concept into scalable, real-world operations.

Recommendations

Train people to spot "copy-paste traps": Employees should be warned that attackers are now asking victims to paste commands or file paths into system dialogs. No legitimate security or account service will ever ask users to paste code into Run, File Explorer, or a terminal. Simple awareness can stop these attacks at the very first step.

Lock down risky tools like PowerShell: Where possible, restrict or monitor the use of PowerShell and command-line tools. Many of these *Fix attacks rely on hidden PowerShell commands to deliver malware. Application control and script-blocking policies can drastically reduce risk.

Detect the unusual, not just the obvious: Monitor for suspicious behavior like images being downloaded and immediately executed, or large encoded strings in PowerShell logs. Attackers are hiding payloads inside JPG files to sneak past traditional filters, so behavioral monitoring is key.

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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link
T1027 Obfuscated Files or Information	T1027.003 Steganography	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1497 Virtualization/Sandbox Evasion	T1217 Browser Information Discovery	T1140 Deobfuscate/Decode Files or Information	T1204 User Execution

T1204.004 Malicious Copy and Paste	T1132 Data Encoding	T1071 Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	70AE293EB1C023D40A8A48D6109A1BF792E1877A72433BCC89613461CFFC7B61, 06471E1F500612F44C828E5D3453E7846F70C2D83B24C08AC9193E791F1A8130, 08FD6813F58DA707282915139DB973B2DBE79C11DF22AD25C99EC5C8406B234A, 2654D6F8D6C93C7AF7B7B31A89EBF58348A349AA943332EBB39CE552DDE81FC8, FD30A2C90384BDB266971A81F97D80A2C42B4CEC5762854224E1BC5C006D007A, 1D9543F7C0039F6F44C714FE8D8FD0A3F6D52FCAE2A70B4BC442F38E01E14072, 1801DA172FAE83CEE2CC7C02F63E52D71F892D78E547A13718F146D5365F047C, 7022F91F0534D980A4D77DF20BEA1AE53EE02F7C490EFBFAE605961F5170A580, B3CE10CC997CD60A48A01677A152E21D4AA36AB5B2FD3718C04EDEF62662CEA1
IPv4	77[.]90[.]153[.]225
Domains	facebook[.]meta-software-worldwide[.]com, facebook[.]windows-software-downloads[.]com, facebook[.]windows-software-updates[.]cc, facebook[.]windows-software-updates[.]com, elprogresofood[.]com, mastercompu[.]com, thanjainatural[.]com, Bitbucket[.]org/pibejiloiza/, Bitbucket[.]org/brubroddagrofe/, Bitbucket[.]org/creyaucuronna-4413/, Grabify[.]link/5M6TOW

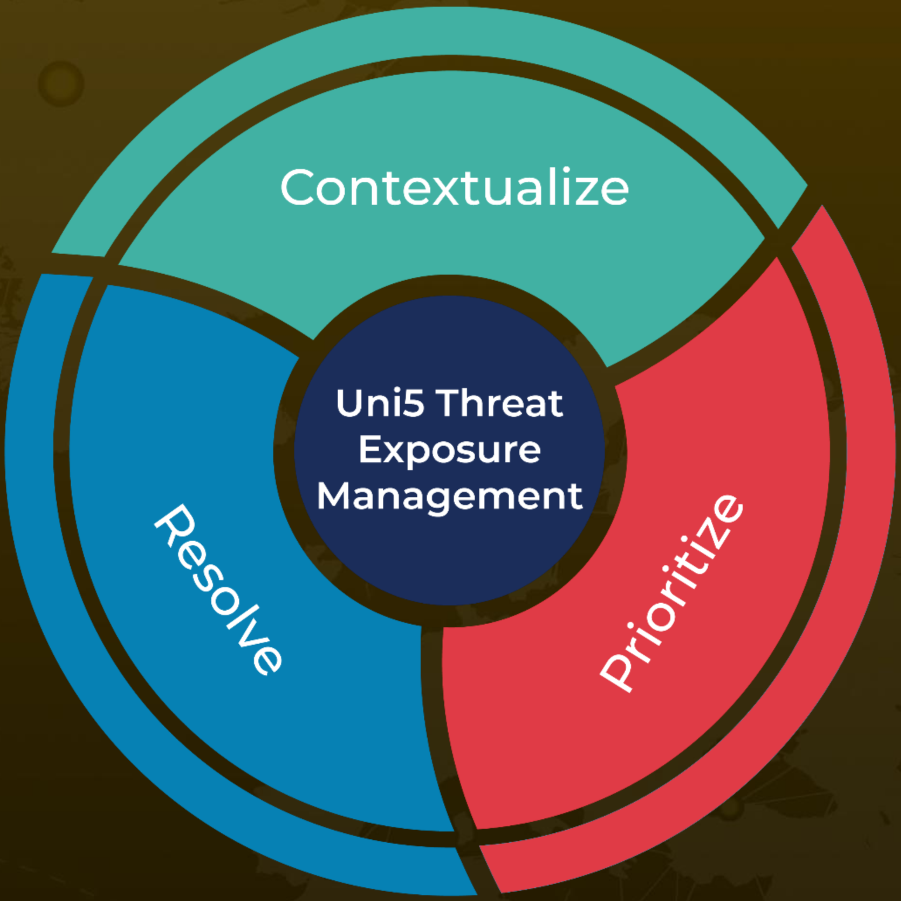
References

https://www.acronis.com/en/tru/posts/filefix-in-the-wild-new-filefix-campaign-goes-beyond-poc-and-leverages-steganography/

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

September 17, 2025 • 5:00 AM

More at www.hivepro.com