July 28, 2025

INTEL471

EMERGING THREATS

FileFix Social Engineering Technique

The FileFix social engineering technique is a sophisticated phishing method that builds upon the previously known (and abused) ClickFix tactic. However unlike ClickFix, which deceives users into executing malicious commands via the Windows Run dialog, FileFix takes a more subtle approach by exploiting the Windows File Explorer's address bar. This technique involves opening a legitimate File Explorer window from a malicious webpage and silently copying a disguised PowerShell command to the user's clipboard. When the user pastes this content into the address bar, the command executes unbeknownst to the user, leading to the download and execution of malware. The payloads delivered through FileFix attacks have included Remote Access Trojans (RATs) and information stealers, which can lead to unauthorized access to sensitive data and systems. Organizations across various sectors, including finance, healthcare, and education, are at risk, as this method bypasses traditional security warnings and relies on user trust in familiar interfaces. Furthermore, in mid-July of 2025, a DFIR report was released covering the abuse of the FileFix technique to deliver a new (and evolved) Interlock RAT Variant being utilized in an active campaign

THREAT SUMMARY

The FileFix social engineering technique is a sophisticated phishing method that builds upon the previously known (and abused) ClickFix tactic. However unlike ClickFix, which deceives users into executing malicious commands via the Windows Run dialog, FileFix takes a more subtle approach by exploiting the Windows File Explorer's address bar. This technique involves opening a legitimate File Explorer window from a malicious webpage and silently copying a disguised PowerShell command to the user's clipboard. When the user pastes this content into the address bar, the command executes unbeknownst to the user, leading to the download and execution of malware. The payloads delivered through FileFix attacks have included Remote Access Trojans (RATs) and information stealers, which can lead to unauthorized access to sensitive data and systems. Organizations across various sectors, including finance, healthcare, and education, are at risk, as this method bypasses traditional security warnings and relies on user trust in familiar interfaces. Furthermore, in mid-July of 2025, a DFIR report was released covering the abuse of the FileFix technique to deliver a new (and evolved) Interlock RAT Variant being utilized in an active campaign.

It is worthy to note that although the paths to execution differ between FileFix and ClickFix techniques, the commands used are likely to be similar or rely on comparable artifacts and methods. The packages included in this collection are based on available reporting related to FileFix at this point in time. Furthermore, attackers may adopt commands similar to those used in ClickFix, as they have with other execution techniques. For reference, here is a link to ClickFix related Hunter Packages.

SYNOPSIS

Research and analysis has found that the FileFix social engineering attack technique leverages the Windows File Explorer's address bar to execute malicious PowerShell commands without raising red flags for the victim. The attack is initiated via a malicious webpage where the HTML element is embedded, and triggers the File Explorer dialog box prompt to interact with it. Simultaneously, JavaScript running on the webpage takes advantage of the navigator.clipboard.writeText() function to automatically copy a malicious PowerShell script to the victim’s clipboard. The clipboard contents appear as an innocuous file path but contain hidden malicious commands. The victim is then tricked into pasting the content from the clipboard into the File Explorer’s address bar, where the PowerShell script is executed, leading to the silent execution of a malicious payload.

Once the script is executed, it downloads and executes a Remote Access Trojan (RAT) such as Interlock RAT or other malware variants that can facilitate further malicious activities. The RATs are designed to establish persistence on the victim's system, enabling attackers to access sensitive data, exfiltrate it, and potentially carry out additional attacks, such as lateral movement within the network or data manipulation. The attacker can then subsequently leverage this access for credential harvesting, system surveillance, and deployment of further malicious payloads. The technique being used alongside Interlock RAT and other instances of its successful use has showcased FileFix's effectiveness in bypassing traditional security defenses. Given its success, FileFix has become a key tool in the arsenal of cybercriminals, significantly impacting organizations worldwide, particularly those in sectors with high-value data such as finance, healthcare, and government.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('332d20d6-5a68-449c-9a01-3cae72d7baac'),touched:!t)

RELATED HUNT PACKAGES

AUTORUN OR ASEP REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/details/use-case/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

MALICIOUS POWERSHELL PROCESS - CONNECT TO INTERNET WITH HIDDEN WINDOW

https://hunter.cyborgsecurity.io/details/use-case/43c8d198-1def-4530-a35a-569e9ebda53e

EXCESSIVE WINDOWS DISCOVERY COMMANDLINE ARGUMENTS - POTENTIAL MALWARE INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/8bb5819f-06a4-4e5d-9099-e43115601999

BROWSER SPAWNING SUSPICIOUS APPLICATIONS - POTENTIAL EXPLOIT OR SOCIAL ENGINEERING

https://hunter.cyborgsecurity.io/details/use-case/59d4df2f-014b-47c0-8008-688d1b41682a

MITRE CONTEXT

- Exploits Vulnerabilities:
    - CVE-2024-38112
- MITRE Tactic Names:
    - Discovery
    - Execution
    - Defense Evasion
    - Persistence
- MITRE Technique Names:
    - Command and Scripting Interpreter
    - System Binary Proxy Execution
    - Remote System Discovery
    - Registry Run Keys / Startup Folder
- MITRE Technique IDs:
    - T1018
    - T1547.001
    - T1059
    - T1218
- Threat Names:
    - Interlock RAT

REFERENCES

1. https://thedfirreport.com/2025/07/14/kongtuke-filefix-leads-to-new-interlock-rat-variant/
2. https://blog.checkpoint.com/research/filefix-the-new-social-engineering-attack-building-on-clickfix-tested-in-the-wild/
3. https://thehackernews.com/2025/06/new-filefix-method-emerges-as-threat.html
4. https://mrd0x.com/filefix-clickfix-alternative/