# FileFix – Fortinet-Themed Variant Uses Cache Smuggling to Evade Detection

*A new FileFix variant is using cache smuggling to deliver malware onto systems without any visible download. A fake Fortinet VPN "Compliance Checker" page instructs users to paste what looks like a normal path into File Explorer, but when entered, a hidden PowerShell command extracts and runs a malicious ZIP from Chrome's cache.*

*This is a more advanced, harder-to-detect version of the FileFix technique the Cyber Threat Intelligence (CTI) team covered in a recent Threat Intelligence Report.*

## Overview

A new FileFix variant was recently discovered that's harder to spot. It uses cache smuggling to place a malicious ZIP in Chrome's cache and runs it without any obvious download or network traffic.

The campaign presents a fake Fortinet VPN "Compliance Checker" page and tells users to paste what appears to be a normal file path into File Explorer. That pasted text contains a space-padded PowerShell command. When the user hits Enter, PowerShell extracts a ZIP file from the browser cache and runs it, bypassing controls that monitor for downloads or web requests.

### Affected Products

- Google Chrome browser (local cache used as payload storage)
- Windows operating systems where PowerShell and File Explorer are available
- Any endpoint that allows unmonitored script execution from user space

The Aspire CTI Team recently released a Threat Intelligence Report on FileFix and its link to Interlock ransomware. This new activity builds directly on that attack chain but introduces a more advanced delivery method capable of evading endpoint detection and response (EDR) systems. When the victim visits the phishing page, JavaScript instructs the browser to fetch a fake image file.

Although the response header labels it as "image/jpeg," the file actually contains a ZIP archive. The image is cached locally by Chrome as normal behavior. That command retrieves a ZIP from Chrome's cache and runs FortiClientComplianceChecker.exe, which executes the payload. This new method removes the need for visible downloads or network fetches, allowing the malware to bypass many antivirus and EDR detection layers.

If exploited, attackers gain quiet control of the device because the payload runs from the browser cache with no download or network alerts. From that foothold an attacker will steal browser-saved credentials and use them to access other systems, often followed by data exfiltration or ransomware (Interlock has been observed in similar chains). See Aspire's recommendations below.

## Aspire Protects

- Instruct staff **NEVER** to copy or paste commands or file paths from a web page into File Explorer, Command Prompt, or the Run box.
- Monitor for `explorer.exe` or `conhost.exe` spawning PowerShell with long or encoded command strings.
- Security teams should search for creation of `%LOCALAPPDATA%\FortiClient\compliance` or `.zip files` extracted from Chrome's cache directory.
- Reset passwords used on devices where suspicious PowerShell activity is observed.
- Block access to domains serving fake Fortinet VPN pages or any resources mislabeled as "image/jpeg" with large binary content.

### TTPs to Watch

Initial Access

- Drive-by Compromise [T1189] – Attacker may deliver the FileFix lure through a malicious or SEO-poisoned webpage.
- User Execution: User-initiated [T1204.004] – Attacker may convince a user to paste a padded path into File Explorer to trigger PowerShell execution.

Execution

- Command and Scripting Interpreter: PowerShell [T1059.001] – Attacker may execute hidden PowerShell commands to extract and launch payloads from the browser cache.

Defense Evasion

- Masquerading: Match Legitimate Resource Name or Location [T1036.005] – Attacker may disguise the payload as a Fortinet compliance utility.
- Obfuscated Files or Information [T1027] – Attacker may hide commands with space padding and encoding to avoid detection.

Credential Access

- Credentials from Web Browsers [T1555.001] – Attacker may steal saved credentials from browser profiles after local execution.
- Valid Accounts [T1078] – Attacker may use stolen credentials to regain or expand access.

Command and Control / Tool Transfer

- Ingress Tool Transfer [T1105] – Attacker may stage the malicious ZIP in the browser cache for local execution, avoiding external downloads.

Exfiltration and Impact

- Exfiltration to Cloud Storage [T1567.002] – Attacker may upload stolen data to cloud platforms before encryption.
- Data Encrypted for Impact [T1486] – Attacker may encrypt files to demand ransom following data theft.

**IoCs**

Active (Cache-Smuggling Variant)

- %LOCALAPPDATA%\FortiClient\compliance
- FortiClientComplianceChecker.exe
- ComplianceChecker.zip
- bTgQcBpv / mX6o0lBw markers
- Explorer > conhost > PowerShell execution chain
- “image/jpeg” payloads containing ZIP data

Historical (from prior FileFix and Interlock attack chain)

- File hashes and IPs/domains are listed in September’s Cyber Threat Intelligence Report: FileFix – The Latest Social Engineering Tactic Driving Interlock Attacks

***Note**: For more details on how we can help protect your organization, contact Aspire’s Customer Success Management team.*

**Targeted Industries**

The new FileFix cache-smuggling variant can impact any organization that allows users to access the web.

- Public Sector
- Education
- Finance
- Healthcare
- Legal
- Manufacturing
- Retail

## Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Supporting Documentation

Cache smuggling: When a picture isn't a thousand words | Expel

The ClickFix Factory: First Exposure of IUAM ClickFix Generator

New FileFix attack uses cache smuggling to evade security software

Customer Service - FileFix - The Latest Social Engineering Tactic Driving Interlock Attacks - Customer Support