TIR-20250924 FileFix - The Latest Social Engineering Tactic Driving Interlock Attacks

9/24/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary

Interlock operators and associated clusters have turned to a phishing-driven campaign known as FileFix (a variant of ClickFix). The activity begins with phishing emails masquerading as Meta/Facebook “incident reports” that pressure victims to address supposed account violations. Links in these messages redirect to compromised but otherwise normal websites, where malicious scripts take over. Instead of dropping malware directly, the sites guide visitors through what appears to be a harmless verification or repair step.

Once the “fix” file is opened, a PowerShell backdoor runs quietly in the background. This backdoor connects to attacker infrastructure, gathers system information, and pulls down further payloads, ranging from credential stealers to remote access tools. If the environment looks promising, operators escalate their activity. They harvest credentials, deploy remote administration software, exfiltrate sensitive files, and in some cases deploy ransomware.

The FileFix phishing campaign is a concern because it lowers the barrier to compromise by mixing

trusted brands like Meta with natural user actions, which leaves traditional security controls less effective. Combined with Interlock's double-extortion model and their targeting across various sectors, the campaign is a risk to businesses of all sizes.

FileFix

What is FileFix?

FileFix is the evolution of ClickFix, a social engineering method first tracked in 2024. While ClickFix convinces users to paste commands into the Windows Run box, FileFix shifts the execution step to opening a file in File Explorer. The change makes the attack chain feel more natural to victims and less detectable by defenders who hardened against clipboard and Run-box abuse last year.

The campaign can start in two ways, but is ty: through phishing emails or SEO poisoning. In the first path, Meta/Facebook-themed phishing emails use official logos and urgent policy language to push recipients into clicking a link. In the second, attackers use SEO poisoning to push malicious links higher in search results, making them appear alongside or above legitimate resources. In both cases, the victim is funneled to a malicious destination. That destination may be a purpose-built site controlled by the threat actor, or in some cases, a legitimate company website that has been quietly compromised.

Once there, a hidden script checks basic details like IP address, browser, or referral source to decide if the visitor should be targeted. If the conditions match, the site presents a "verification" or "repair" step, often framed as a small file download. Opening that file executes a PowerShell loader that retrieves the real payload. Because the process feels like a routine step online (click, download, and run) it lowers suspicion and often bypasses past basic endpoint defenses.

Image 1: FileFix in Action Pathway 1

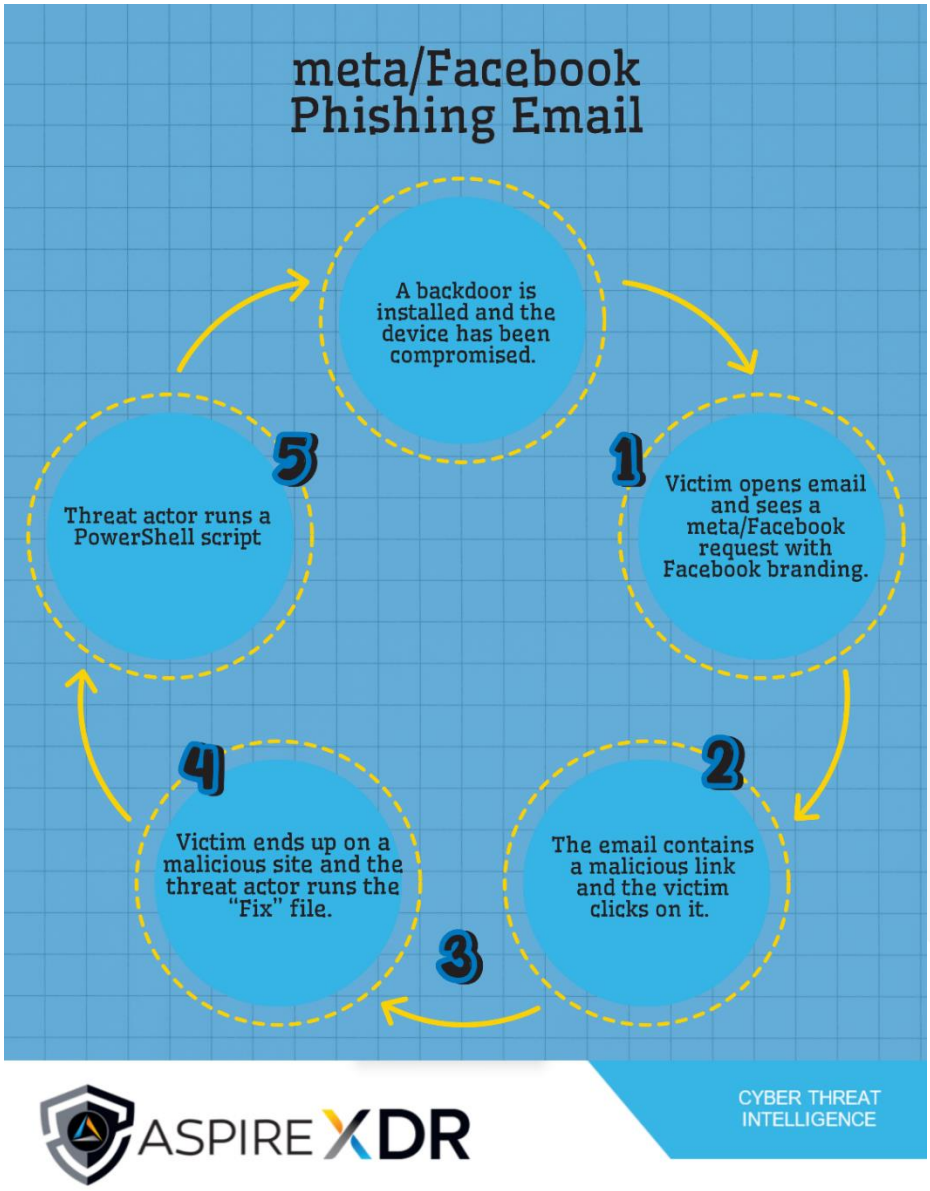
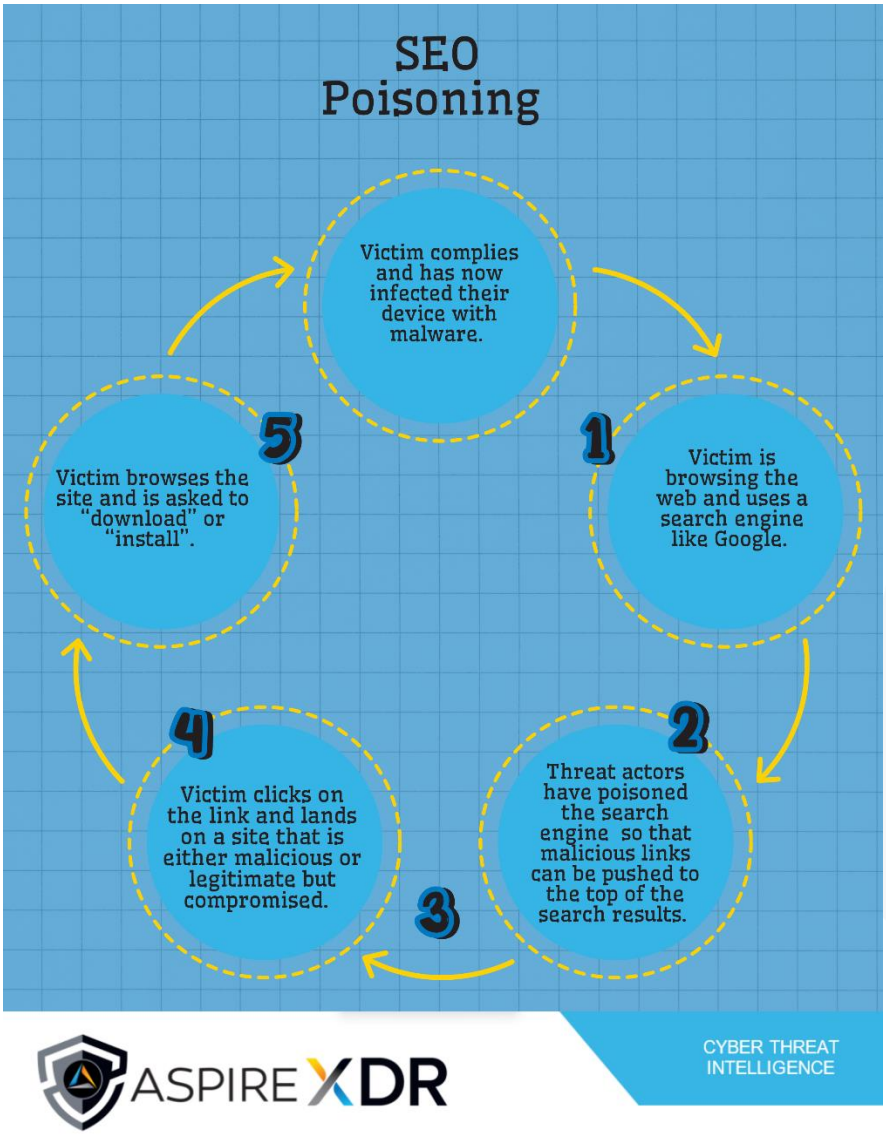
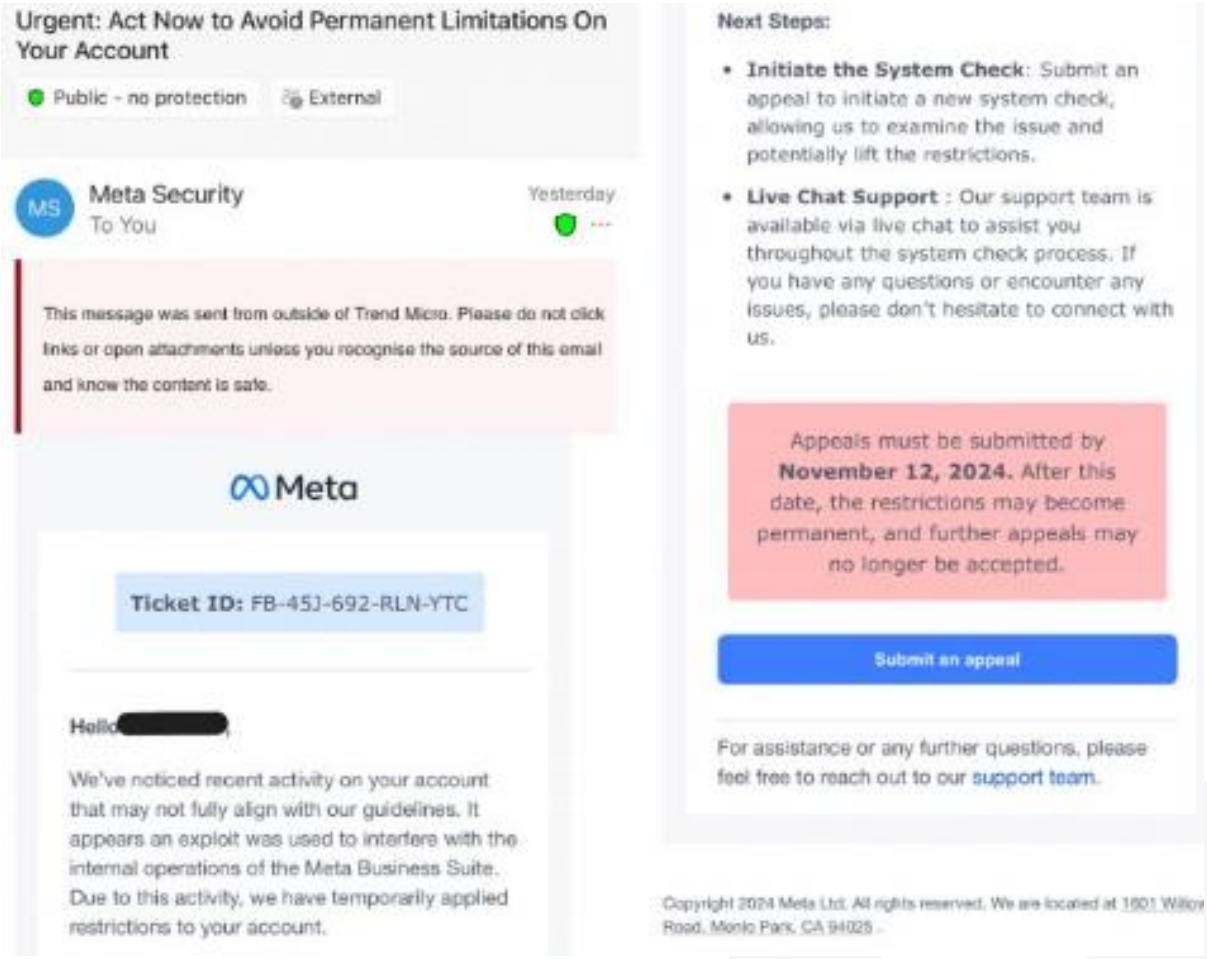


Image 2: FileFix in Action Pathway 2



Also, researchers tracking FileFix have connected it to the KongTuke/LandUpdate808 cluster, which had already been linked to fake CAPTCHA and web-inject campaigns. Researchers have also found PHP-based RATs in these operations; the same type of malware tied to FileFix. Seeing the same malware in both places gives stronger grounds to connect these campaigns back to Interlock.

Image 3: Meta/Phishing Email Example



Source: Trend Micro

INTERLOCK RANSOMWARE

Interlock was first spotted in September 2024 and is assessed to be financially motivated. Unlike many groups that sell access through a RaaS model, Interlock runs closed operations and publishes stolen data on its own leak site, the *Worldwide Secrets Blog*. Analysts place its operators in Eastern Europe based on hosting and infrastructure patterns. The group has gone after high-value targets in North America

and Western Europe, with healthcare, education, manufacturing, and local government hit hardest.

Known Interlock Victims

- DaVita – U.S. healthcare provider, ransom demand of $2.5 million, ~1 TB of data threatened.
- Kettering Health – U.S. hospital network, ransom demand of $3 million, ~850 GB of data published.
- City of Saint Paul, Minnesota – local government breach, 43 GB of data leaked after refusal to pay.
- Additional education and manufacturing victims have been listed on the *Worldwide Secrets Blog*, with ransom asks generally in the low-to-mid millions and data sets ranging from 100 GB to over 1 TB.

TTPs

Over the past year, Interlock has shifted from pushing fake browser updates, to using ClickFix, and now to FileFix. Each version looks different on the surface, but the sequence underneath is consistent, which includes a small PowerShell script, a lightweight backdoor, and an open path for follow-on actions. What has changed is the group's delivery. ClickFix leaned on the Run box, but FileFix delivers a small file that looks like a repair tool. Opening it feels ordinary to most users, which makes it harder to flag and bypasses many of the defenses.

Once inside, the operators run system checks, steal credentials with keyloggers or info-stealers, take screen shots, and move across the network with tools like RDP or AnyDesk. Data theft comes first, with encryption used later.

Interlock's operations tie directly to the KongTuke (also known as LandUpdate808) malware, which uses compromised websites and injected JavaScript to deliver prompts that lead into the FileFix chain. Analysts have linked both NodeJS- and PHP-based RATs to these campaigns. The NodeJS variant is hardened with anti-VM checks, XOR+gzip network framing, and SOCKS proxy capability, while the PHP variant emphasizes fast system profiling and tasking flexibility. The use of both shows Interlock's willingness to adapt tools to the victim environment.

Recent security incidents show Interlock pushing beyond the healthcare industry. The St. Paul attack in July 2025 forced the Minnesota National Guard to deploy cyber units, while other victims in Europe and North America have reported thefts of terabytes of data. In each case, the fallout has been operational disruption and data leaks.

Importantly, Interlock continues to experiment with loaders and backdoors. Reports from Sekoia TDR note use of LummaStealer and BerserkStealer in early 2025. These overlaps, along with shared infrastructure, tie FileFix activity firmly back to Interlock.

Observed TTPs include:

- Initial Access – T1189 Drive-By Compromise; T1204.004 User Execution (FileFix/ClickFix)
- Execution – T1059.001 PowerShell; T1059.007 JavaScript; T1218 Signed Binary Proxy Execution
- Persistence – T1547.001 Run Keys/Startup; T1053.005 Scheduled Task
- Privilege Escalation & Lateral Movement – T1078 Valid Accounts; T1021.001 RDP; T1558.003 Kerberoasting
- Discovery – T1082 System Information; T1057 Process Discovery; T1007 Service Discovery; T1016 Network Config
- Command & Control – T1105 Ingress Tool Transfer; T1090 Proxy; T1071.001 Web (via temporary tunnels, raw TCP 443 fallbacks)
- Exfiltration & Impact – T1567.002 Exfil to Cloud Storage; T1486 Encryption; T1070.004 File Deletion/Self-remove

How FileFix Links to ClickFix

ClickFix and FileFix are very similar. Both depend on convincing the user to take an action that feels harmless but runs attacker code. With ClickFix, the step was pasting a command into Windows+R. FileFix streamlines it by offering a downloadable “fix” file that opens in File Explorer.

At first glance, swapping the Run-box for a file might seem like a small change. In practice, it makes the lure feel ordinary. Open the file, and the same PowerShell stage runs in the background, giving attackers a view of the system and the choice to escalate.

Key differences

- **User action** — ClickFix = paste into Run; FileFix = open a “fix” file in Windows File Explorer (the file manager where you see folders, documents, and drives)

- **First security signal** — Click Fix = Clipboard/Run activity vs. FileFix = file execution > PowerShell
- **Detection** — ClickFix = Run-box rules vs. FileFix = routine file-open behavior
- **User mindset** — FileFix borrows the familiar “download and run a helper” pattern seen across the web

Aspire Case Study

A customer in the education sector escalated an endpoint alert tied to PowerShell shortly after a staff member visited a well-known hobby website. Unknown to the user, the site had been modified to deliver a short, randomized JavaScript file that only appeared for selected visitors. The page displayed a simple verification step that looked routine, and the user was prompted to run a helper file, a sequence that blends FakeCaptcha-style lures with FileFix-style execution.

Minutes later, telemetry captured powershell.exe executing an encoded command. The command wrote a script into the user profile, ran it, and then deleted it. This self-cleaning behavior left no obvious dropper behind, but DNS logs recorded visits to both the compromised hobby site and a barebones “it works”-style domain later tied to malicious activity.

The SOC quickly contained the incident. EDR killed the PowerShell process on behavior, the endpoint was isolated, and global DNS blocklists were updated with the malicious domains. Because the helper deleted itself, analysts recommended a full reimage of the device rather than relying on cleanup tools. Credentials for the impacted user and any accounts accessed during the activity window were rotated to close off possible re-entry.

FileFix or FakeCaptcha?

Lining up the activity against recent reporting showed clear FileFix characteristics:

- Short injected script > user prompt > PowerShell staging that quickly reached out to disposable infrastructure.

What complicates the picture is the lure itself. The “verification” step looked more like FakeCaptcha, which means the operators are recycling familiar tactics on the front end

while keeping FileFix on the back end. The presence of KongTuke-linked infrastructure tied it even closer to campaigns where we've seen that blending of old and new delivery methods.

This makes the case an example of a hybrid attack chain. What we saw was a front end that carried the look and feel of FakeCaptcha, a verification step designed to lower suspicion and get the user to take action. But once the user followed the prompt, the activity lined up with FileFix, which involves PowerShell staging in the user profile, quick callbacks to temporary infrastructure, and a helper that cleaned itself up.

The threat actor seemed to borrow Fake Captcha's social engineering style, but the execution chain underneath was FileFix. That mix is consistent with how Interlock-aligned operators are evolving their delivery. The group borrows lures that feel familiar to users while modernizing the execution to avoid security defenses.

Access Broker Connection

One of the clearest markers of FileFix is how fast it pivots into credential theft. With almost no exploits involved, a single user action can hand over the keys an attacker needs to explore a domain. That fits the business model of initial-access brokers, who either sell those footholds or pass them directly to ransomware gangs.

For Interlock, it's not always clear if they're buying access or running the campaigns themselves, and by the time an alert shows up, stolen credentials may already be in use. Shutting down the process isn't enough if those credentials are left active, the attacker can just log back in later. The safer approach is to cut off any outbound tunnels and rotate credentials used on the machine during that window.

A Global Problem for Small Teams

Another idea to consider is that FileFix campaigns are designed to scale. Operators can reuse the same script on a compromised site, change only the language shown to visitors, and keep reaching new victims without altering how the attack works. That's why these chains have shown up in more than a dozen languages, from English and Spanish to Polish and Vietnamese.

For smaller organizations, this makes the threat harder to spot. There's no targeted spear-phish to block and no software vulnerability to patch. Instead, any staff member browsing a normal-looking website (vendor page, manual, even a hobby forum) can be funneled into the same "fix" step if they meet the checks. The infection chain doesn't care whether the endpoint is fully patched or sitting behind a firewall.

The Defenders shouldn't waste time chasing every new domain. What stays consistent are the patterns, such as short injected JavaScript with random names and a user-led "fix" file. Those are the behaviors that small teams can reliably look for and block, no matter the language used.

Conclusion

FileFix is a small shift with big impact: moving the paste target to File Explorer bypasses many controls and turns routine browsing into a foothold. Interlock has adapted quickly and now runs a steady script: stage quietly, persist, steal, and encrypt. The case study shows how fast this can start and how containment plus a clean rebuild cuts it off. The controls below focus on this exact gap.

Recommendations

FileFix works because it blends in with what looks like normal user behavior. The best defense is a mix of simple user rules and a few behind-the-scenes security measures that security teams can set up:

- **User awareness** – Staff should know the two biggest red flags: (1) never paste commands from a web page into Windows Run or a browser console, and (2) never open a "fix" or "verification" file offered by a website. These are not normal IT practices and should always raise suspicion.
- **Quick isolation over cleanup** – If a device shows signs of running one of these chains (Windows Explorer launching PowerShell, suspicious prompts, or sudden outbound connections), the safest step is to isolate and reimage. In-place cleanup often leaves gaps that attackers can use to return.

- **Credential hygiene** – Treat any login used on a suspicious device as exposed. Rotate the user's password right away, and reset admin credentials that may have been active on the machine. This cuts off one of the fastest ways attackers come back after initial access.
- **Blocking common tunnels** – Interlock often leans on disposable Cloudflare tunnels. Security teams should consider default blocking of new trycloudflare.com subdomains unless there's a business reason to allow them.
- **Watch for unusual cloud use** – Many incidents now involve data theft before encryption. Keep an eye out for first-time use of tools like AzCopy or bulk file transfers to cloud storage, especially from accounts that don't normally handle backups. This can catch the theft stage early.
- **Incident response playbooks** – Update response guides to reflect this threat class. The steps are: isolate first, reimage rather than attempt cleanup, block related domains, rotate credentials, and check for remote tool use (like RDP or AnyDesk) that may signal lateral movement.

MITRE MAP

Interlock and FileFix

Initial Access	T1189 - Drive-By Compromise
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Persistence	T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Privilege Escalation	T1068 - Exploitation for Privilege Escalation T1078 - Valid Accounts
Defense Evasion	T1036.005 - Masquerading: Match Legitimate Resource Name or Location T147.001 - Steal or Forge Kerberos Tickets: Kerberoasting
Credential Access	T1003 - Credentials from Web Browsers

Discovery	T1082 - System Information T1033 - Account/User
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols T1105 - Ingress Tool Transfer
Impact	T1486 - Data Encrypted for Impact T1657 - Financial Extortion / Double-Extortion

ASPIRE PROTECTS

- **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 cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

- Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **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.

Indicators of Compromise (IoCs)

MD5

- 3344a2d675911a0136199004cf8ec059

SHA1

- c2423a732cbbc194edfc0f17145896309598ac37

SHA256

- 70ae293eb1c023d40a8a48d6109a1bf792e1877a72433bcc89613461cffc7b61

IPv4

- 77[.]90[.]153[.]225
- 144[.]31[.]221[.]37

Domain

- Elprogresofood[.]com
- Mastercompu[.]com
- Math1st[.]com
- Kovels[.]com

Hostname

- Facebook[.]meta-software-worldwide[.]com
- Facebook[.]windows-software-downloads[.]com
- Facebook[.]windows-software-updates[.]cc
- Facebook[.]windows-software-updates[.]com

SUPPORTING DOCUMENTATION

FileFix in the wild! New FileFix campaign goes beyond POC and leverages steganography

New FileFix attack uses steganography to drop StealC malware

Interlock ransomware adopts new FileFix attack to push malware

FileFix: The New Social Engineering Attack Building on ClickFix Tested in the Wild - Check Point Blog

FileFix in the Wild: Steganographic JPGs and StealC Delivered via File Explorer Trickery - LevelBlue - Open Threat Exchange

FileFix Explained: New Paths to Exploitation and Defense in Windows | CyberMaxx

New FileFix attack weaponizes Windows File Explorer for stealthy commands

KongTuke FileFix Leads to New Interlock RAT Variant – The DFIR Report

FileFix In The Wild: Phishing Campaign Hides Malware Inside Photographs

#StopRansomware: Interlock | CISA

Unwrapping the emerging Interlock ransomware attack

Message from Wolf Bot

US agencies warn of Interlock ransomware targeting critical infrastructure in North America, Europe - Industrial Cyber

INTERLOCK Ransomware

The Rise of Interlock Ransomware Group

The Interlock Ransomware Problem Security Teams Can't Ignore | BlackFog

Saint Paul cyberattack linked to Interlock ransomware gang

Dark Web Profile: Interlock Ransomware - SOCRadar® Cyber Intelligence Inc.

KongTuke Campaign Deploys Modified Interlock RAT Using FileFix Method Against Windows Environments

KongTuke (Malware Family)

Yet Another NodeJS Backdoor (YaNB): A Modern Challenge

Interlock ransomware evolving under the radar - Sekoia.io Blog

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.