مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

ClickFix: New Social Engineering Tactic Infects Windows Systems

Tracking #:432317256

Date:13-05-2025

TLP: WHITE

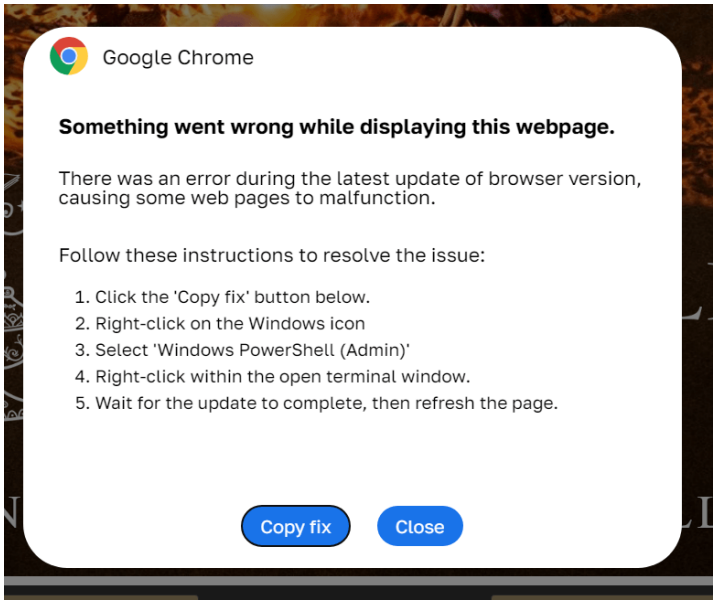
EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a newly observed social engineering technique dubbed ClickFix is being actively exploited by threat actors to compromise Windows systems without exploiting software vulnerabilities.

TECHNICAL DETAILS:

A newly observed social engineering technique dubbed **ClickFix** is being actively exploited by threat actors to compromise Windows systems without exploiting software vulnerabilities. First detected in early 2024, ClickFix campaigns have escalated throughout 2025. This technique manipulates users into executing PowerShell scripts themselves by mimicking legitimate troubleshooting steps—effectively bypassing traditional security defenses.

The attack commonly leverages fake pop-ups, phony error messages, or CAPTCHA verifications on malicious or compromised websites. These messages urge the user to "fix" a problem by copying and running a script via the Windows Run dialog (Win + R) or search bar. Once executed, the PowerShell script typically downloads and runs malware on the user's machine under current user privileges.



An example of instructions for confirming that you're not a robot.

Attack Details: How ClickFix Works

ClickFix exploits human trust and urgency by presenting a fabricated technical problem and offering a scripted "fix." The process typically unfolds in four manipulated steps:

1. **User Clicks a "Fix" or "How to Fix" Button**
   - A webpage displays an error message or fake system notification (e.g., plugin missing, CAPTCHA failed, document cannot be opened).
   - The "Fix" button silently copies a PowerShell script to the clipboard.
2. **User Is Told to Press [Win + R] or Open Windows Search Bar**
   - Instructions guide the user to open the Run dialog or search bar.
3. **User Pastes the Script**
   - Using [Ctrl + V], the copied PowerShell command is pasted into the prompt.
4. **User Presses [Enter] to Execute Script**
   - The malicious script is executed with the user's privileges, often downloading further malware or opening a remote access channel.

Key Variants of the ClickFix Deception:

- **Browser Update Needed**: Fake prompts ask users to "install" a browser fix.
- **Document Preview Error**: Prompts for missing plugins to view Word/PDF.
- **Email Attachment Error**: HTML file disguised as a .docx/.pdf launches the trick.
- **Video Call Error**: Fake Zoom/Google Meet errors suggesting hardware issues.
- **Fake CAPTCHA**: Users are tricked into running code to "prove they're human."

RECOMMENDATIONS:

To mitigate the risks posed by ClickFix-based attacks, organizations should take a **layered approach** to cybersecurity that combines technical controls with user awareness and education:

Technical Controls

1. **Restrict Access to PowerShell:**
   - Use AppLocker or Windows Defender Application Control (WDAC) to restrict execution of PowerShell scripts for non-admin users.
   - Implement constrained language mode for PowerShell where applicable.
2. **Disable/Restrict Win + R Execution:**
   - Group Policy or third-party endpoint protection tools can block or monitor the use of Win + R.
3. **Email and Web Gateway Protection:**
   - Deploy email filters that block or quarantine suspicious HTML attachments and links.
   - Enable web content filtering to block access to known malicious or suspicious domains.
4. **Endpoint Detection & Response (EDR):**
   - Monitor systems for abnormal command-line behavior such as sudden PowerShell execution initiated by user interface interaction.

User Awareness and Policy

5. **Security Awareness Training:**
    - Regularly train employees to recognize social engineering tactics, especially those involving prompts to manually run scripts or commands.
6. **Incident Reporting Culture:**
    - Encourage staff to report suspicious messages or unusual website behavior promptly.
    - Implement a streamlined reporting mechanism for quick IT/security team response.
7. **Security Policies:**
    - Include guidelines in acceptable use policies that prohibit manual execution of unsolicited scripts or commands.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.kaspersky.com/blog/what-is-clickfix/53348