

[Products](#)

[All-In-One Protection](#)

ClickFix Deception: A Social Engineering Tactic to Deploy

Malware

[McAfee+ Individual Plans](#)

Complete privacy, identity and device protection for individuals.

mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/

[NEW McAfee+ Family Plans](#)

July 11, 2024

Complete privacy, identity and device protection for up to 6 family members.

[McAfee Labs](#)

Jul 11, 2024

[Antivirus](#)

9 MIN READ

[Scam Protection](#)

[Virtual Private Network \(VPN\)](#)

Authored by [Yashvi Shah](#) and [Vignesh Dhatchanamoorthy](#)

[Mobile Security](#)

[PC Optimizer](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Free Tools & Downloads](#)

[Web Protection](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Password Generator](#)

[Features](#)

[Keep Me Private Online](#)

We have observed malware families such as Lumma Stealer and DarkGate leveraging this technique. Here is the personal data cleanup

[Personal Data Cleanup](#)

[Online Account Cleanup](#)

[VPN \(Virtual Private Network\)](#)

[Social Privacy Manager](#)

[Safeguard My Identity](#)

[Identity Monitoring](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Identity Theft Coverage & Restoration](#)

[Password Manager](#)

[Protect My Devices](#)

[Antivirus](#)

[Scam Protection](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

Figure 1: Prevalence for the last three months

[Our Team](#)

[Social Privacy Manager](#)

[Our Locations](#)

[Why McAfee](#)

Darkgate is a sophisticated malware known for its ability to steal sensitive information, provide remote

access, and establish persistent backdoors in compromised systems. It employs advanced evasion tactics

and can spread within networks, making it a significant cybersecurity threat.

McAfee Labs obtained a phishing email from the spamtrap, having an HTML attachment.

[Support Community](#)

[Password Manager](#)

[Pages](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

Figure 2: Email with Attachment

[VPN \(Virtual Private Network\)](#)

[Our Team](#)

[Social Privacy Manager](#)

[Our Locations](#)

The email masquerades as a Word document, displaying an error prompt to deceive users. This tactic

is used to trick users into taking actions that could lead to the download and execution of malicious

software.

[Support](#)

[Identity Monitoring](#)

[Help](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[FAQs](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 3 Displays extension problem issue

[Why McAfee](#)

[Support](#)

As shown, the sample displays a message stating, “The ‘Word Online’ extension is NOT installed in your

browser. To view the document offline, click the ‘How to fix’ button.”

[Identity Monitoring](#)

[Credit Monitoring](#)

[Security Freeze](#)

Before clicking on this button, let’s examine the underlying code. Upon examining the code, it was

discovered that there were several base64-encoded content blocks present. Of particular significance was

one found within the <Title> tag, which played a crucial role in this scenario.

[Password Manager](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

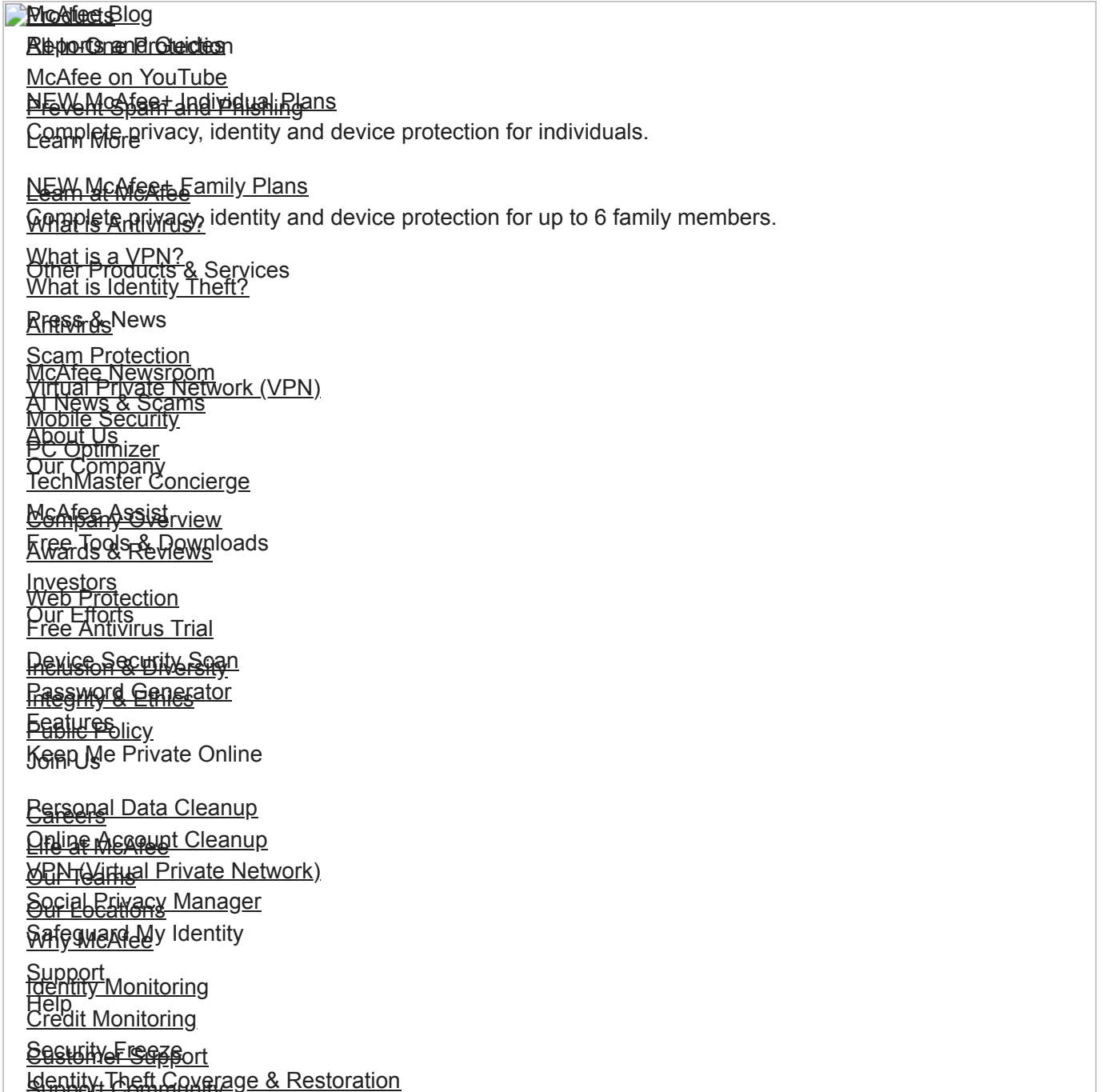


Figure 4-11 HTML Document contains Base64-encoded content in the title tag

Activation
Deactivation

Scam Protection
Activate Retail Card
Web Protection
Protect My Family

Protection Score
Parental Controls
Family Plans
Resources
Stay Updated

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

Figure 5. After decoding the code

[Social Privacy Manager](#)

[Our Locations](#)

[Safeguard My Identity](#)

The `cmd.exe` command demands PowerShell to carry out malicious activities on a system. It starts by

downloading an HTA (HTML Application) file from the URL [https://www.rockcreekdds.com/wp-](https://www.rockcreekdds.com/wp-content/uploads/1/1hta)

[Identity Monitoring](#)
[Credit Monitoring](#)

`content/1/1hta` and saves it locally as `C:\users\public\1x.hta`.

[Security Freeze](#)

The script then executes this HTA file using the `start-process` command, which initiates harmful actions on the system. Additionally, the script includes a command (`Set-Clipboard -Value ''`) to clear the contents of the clipboard. After completing its tasks, the script terminates the PowerShell session with `exit`.

[Identity Theft Coverage & Restoration](#)

[Password Manager](#)

the clipboard. After completing its tasks, the script terminates the PowerShell session with `exit`.

[Protect My Devices](#)

[Contact Us](#)

Upon further inspection of the HTML page, we found a javascript at the end of the code.

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

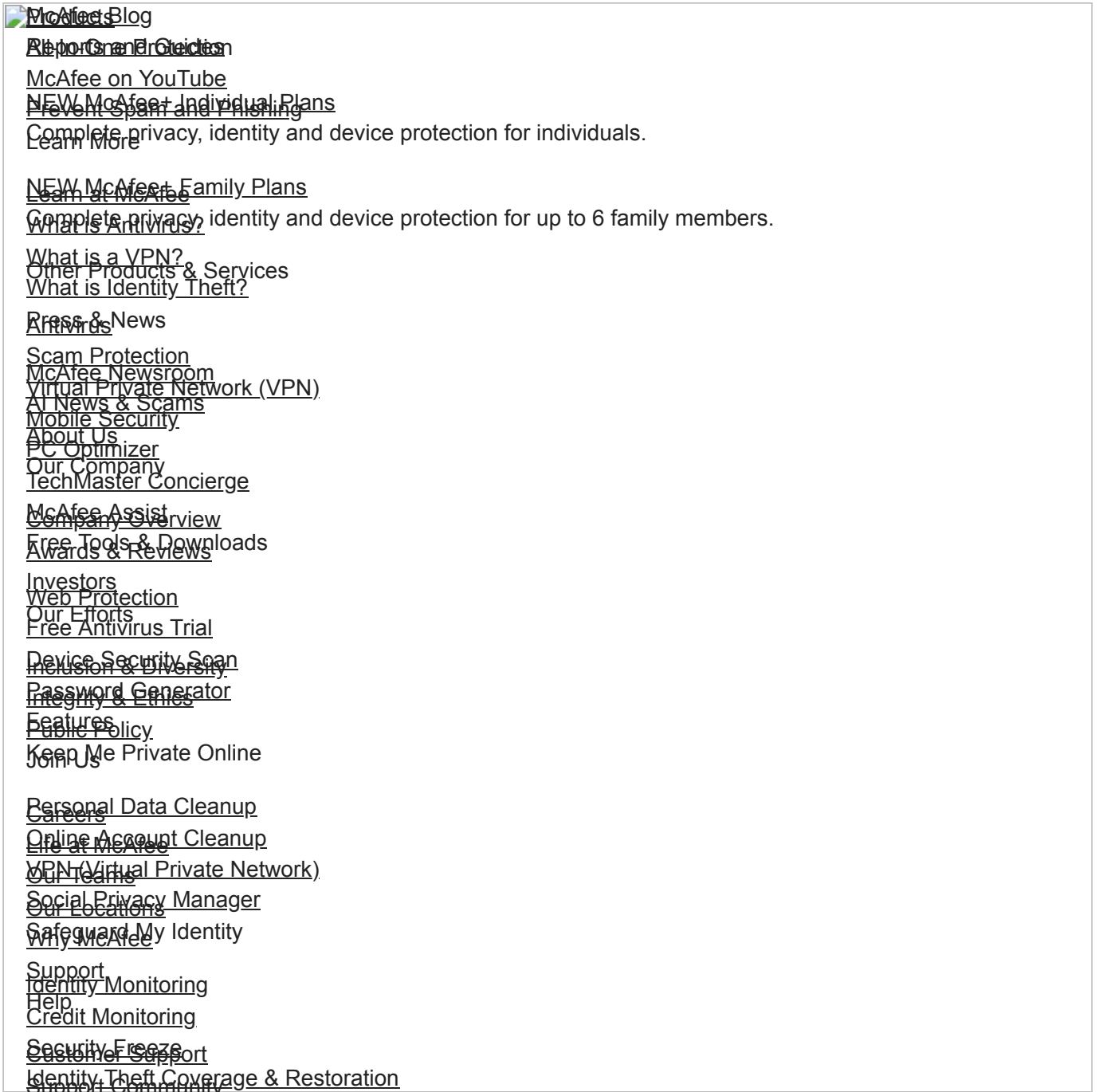


Figure 6-14: McAfee function snippet

Activation
This JavaScript snippet decodes and displays a payload, manages modal interactions for user feedback, and provides functionality for copying content to the clipboard upon user action.

Web Protection
In a nutshell, clicking on the “How to fix” button triggers the execution of JavaScript code that copies the PowerShell script directly onto the clipboard. This script, as previously discussed, includes commands to download and execute an HTA file from a remote server.

Parental Controls
Let's delve into it practically:

Resources
Stay Updated

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 7-5 Clipboard contains malicious command

[Why McAfee Identity](#)

[Support](#)

[Identity Monitoring](#)

[Credit Monitoring](#)

[Customer Support](#)

[Downloaded Script](#)

[Support Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[FAQs](#)

[Protect My Devices](#)

Once the User does this, the HTA file gets downloaded.

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

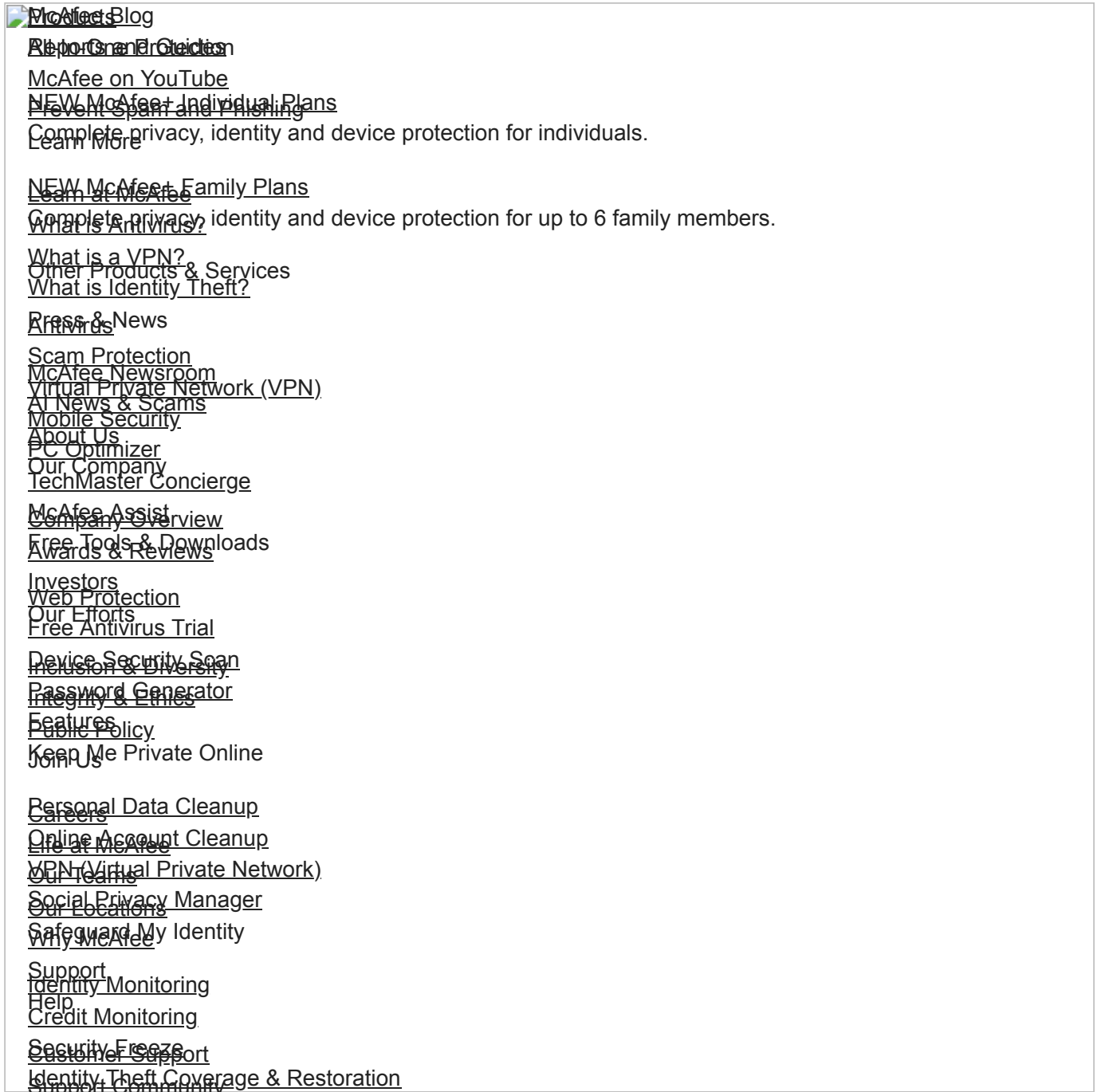


Figure 8-11 McAfee Devices

The above file attempts to connect to the marked domain and execute a PowerShell file from this malicious software. The above is the malicious script that is stored remotely and executed.

[Scan Protection](#)
[Web Protection](#)
[Protect My Family](#)

[Protection Score](#)
[Parental Controls](#)
[Family Plans](#)
[Resources](#)
[Stay Updated](#)

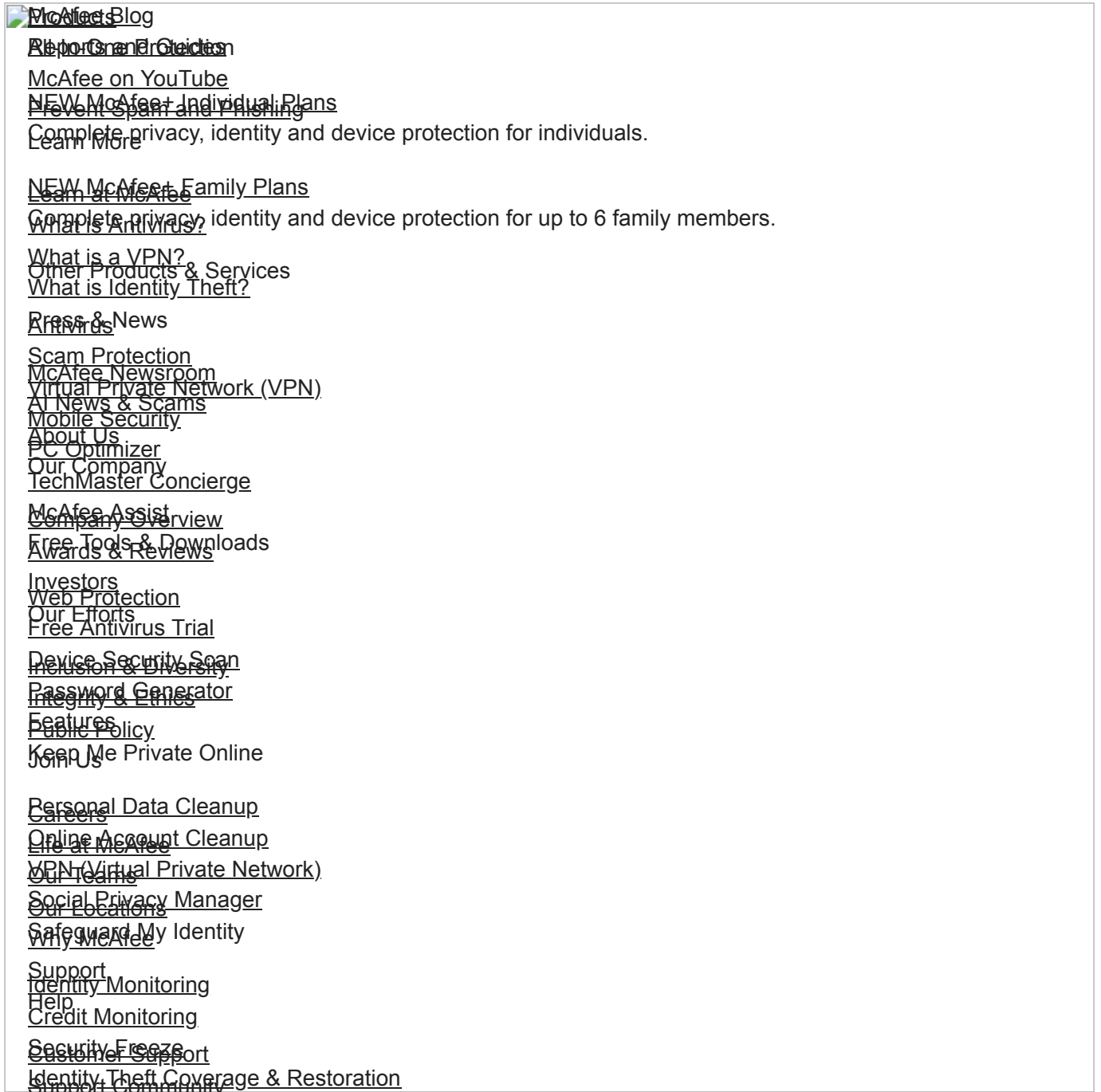


Figure 2: PowerShell code snippet

As this PowerShell script is executed implicitly without any user interaction, a folder is created in the C drive, a batch file, an executable and script are dropped and executed automatically.

[Web Protection](#)
[Protect My Family](#)

[Protection Score](#)
[Parental Controls](#)
[Family Plans](#)
[Resources](#)
[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 10. Downloaded zip contains AutoIT script

[Why McAfee](#)

[Support this](#)

Following this, Dark Gate begins its malicious activity and starts communicating with its command and

control server.

[Identity Monitoring](#)

[Help \(G2\) server](#)

[Credit Monitoring](#)

[Security Freeze](#)

A similar ClickFix social engineering technique was found to be dropping Lumma Stealer.

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[Protect My Devices](#)

Lumma Stealer Ingesting via “ClickFix”

[Contact Us](#)

After this, Dark Gate discovered a website displaying an error message indicating that the browser is encountering issues displaying the webpage. The site provides steps to fix the problem, which are designed to deceive users into executing malicious actions.

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 11. Showing error on accessing the webpage

[Why McAfee](#)

[Support](#)

It over the target user to perform the following steps:

[Identity Monitoring](#)

[Help](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Identity Theft Coverage & Restoration](#)

[Open Windows PowerShell \(Admin\).](#)

[Password Manager](#)

[Protect My Devices](#)

[Wait for the update to complete.](#)

[Activation](#)

[Antivirus](#)

Let's analyze the code that gets copied when clicking the "Copy Fix" button.

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 17: Base64-encoded content

[Why McAfee Identity](#)

[Support](#)

As we can see, the code includes base64-encoded content. Decoding this content, we get the following

Identity Monitoring

Help

scored Credit Monitoring

[Security Freeze](#)

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[FAQs](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

Figure 13 After decoding the Base64 content

[Why McAfee](#)

[Support](#)

[Identity Monitoring](#)

This PowerShell script flushes the DNS cache and then decodes a base64-encoded command to fetch and

[Help](#)

execute a script from a remote URL [https://weoleycastleletaxis.co.uk/chao/baby/cow\[.\].html](https://weoleycastleletaxis.co.uk/chao/baby/cow[.].html), masquerading

[Credit Monitoring](#)

the request with a specific User-Agent header. The fetched script is then executed, and the screen is

[Customer Support](#)

cleared to hide the actions. Subsequently, it decodes another base64 string to execute a command that

[Coverage & Restoration](#)

sets the clipboard content to a space character. The script is likely designed for malicious purposes, such

[Support Community](#)

[Password Manager](#)

[Easy](#)

[as downloading and executing remote code covertly while attempting to hide its activity from the user.](#)

[Contact Us](#)

[Activation](#)

Upon activation, the following process tree flashes:

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

[Figure It Out Process Tree](#)

[Why McAfee](#)

[Support](#)

As we know, it is downloading the malware from the given URL, a new folder is created in a Temp folder and help is downloaded:

[Identity Monitoring](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[FAQs](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Team](#)

[Social Privacy Manager](#)

[Our Locations](#)

[Figure 15 Network activity](#)

[Why McAfee](#)

The software is unzipped and dropped in the same folder:

[Support](#)

[Identity Monitoring](#)

[Help](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Password Manager](#)

[FAQs](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[Protect My Family](#)

[McAfee Blog](#)

[Reports and Guides](#)

[McAfee on YouTube](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[NEW McAfee Family Plans](#)

[Learn at McAfee](#)

Complete privacy, identity and device protection for up to 6 family members.

[What is Antivirus?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

[Press & News](#)

[Announcements](#)

[Scam Protection](#)

[McAfee Newsroom](#)

[Virtual Private Network \(VPN\)](#)

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[PC Optimizer](#)

[Our Company](#)

[TechMaster Concierge](#)

[McAfee Assist](#)

[Company Overview](#)

[Free Tools & Downloads](#)

[Awards & Reviews](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Free Antivirus Trial](#)

[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Teams](#)

[Social Privacy Manager](#)

[Our Locations](#)

[Figure 16: Dropped files](#)

[Why McAfee Identity](#)

[Support](#)

The malware starts communicating with its C2 server as soon as it gets dropped in the targeted system.

[Identity Monitoring](#)

[Help](#)

[Credit Monitoring](#)

Conclusion

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

In conclusion, the Clickfix social engineering technique showcases a highly effective and technical method for malware deployment. By embedding base64-encoded scripts within seemingly legitimate error prompts, attackers deceive users into performing a series of actions that result in the execution of malicious

[Protect My Devices](#)

commands. These commands typically download and execute payloads, such as HTA files, from remote servers, subsequently deploying malware like DarkGate and Lumma Stealer.

[Activate Retail Card](#)

[Web Protection](#)

Once the malware is active on the system, it begins its malicious activities, including stealing users' personal data and sending it to its command and control (C2) server. The script execution often includes steps to evade detection and maintain persistence, such as clearing clipboard contents and running processes in minimized windows. By disguising error messages and providing seemingly helpful

[Protection Score](#)

instructions, attackers manipulate users into unknowingly executing harmful scripts that download and run various kinds of malware.

[Family Plans](#)

[Resources](#)

[Stay Updated](#)

Mitigations:

[Reports and Guides](#)
At McAfee Labs, we are committed to helping organizations protect themselves against sophisticated cyber threats. McAfee has pioneered the [Dark Web](#) engineering technique. Here are our recommended mitigations and controls to protect privacy, identity and device protection for individuals.
[Learn More](#)

- [NEW McAfee Family Plans](#) sessions to educate users about social engineering tactics and phishing
- [Complete privacy, identity and device protection for up to 6 family members.](#)
- [2. Install and maintain updated antivirus and anti-malware software on all endpoints.](#)
- [3. Use a VPN & Services](#) email filtering to block phishing emails and malicious attachments.
- [4. Use web filtering solutions to prevent access to known malicious websites.](#)
- [5. Deploy firewalls and intrusion detection/prevention systems \(IDS/IPS\) to monitor and block malicious](#)
- [6. Implement network segmentation to limit the spread of malware within the organization.](#)
- [7. Enforce the principle of least privilege \(PoLP\) to minimize user access to only necessary resources.](#)
- [8. Implement security policies to monitor and restrict clipboard usage, especially in sensitive](#)
- [9. Implement multi-factor authentication \(MFA\) for accessing sensitive systems and data.](#)
- [10. Ensure all operating systems, software, and applications are kept up to date with the latest security](#)
- [11. Regularly monitor and analyze system and network logs for signs of compromise.](#)
- [12. Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.](#)
- [13. Regularly backup important data and store backups securely to ensure data recovery in case of a](#)
- [14. Regularly update software attack or data breach.](#)

Indicators of Compromise (IoCs)

Personal Data Cleanup	
Online Account Cleanup	
VPN (Virtual Private Network)	
Secure Privacy Manager	
Safeguard My Identity	
Email	c5545d28faee14ed94d650bda28124743e2d7dacdefc8bf4ec5fc76f61756df3
Identity Monitoring	0db16db812cb9a43d5946911501ee8c0f1e3249fb6a5e45ae11cef0dddbbe4889
Credit Monitoring	
Security Freeze	204217d48f2565990dfdf2269c26113bd14c204484d8f466fb873312da80cf
Identity Theft Coverage & Restoration	
Password Manager	648589aa3e15ce61c6a3be4fc98429581be738792ed17a713b4980c9a4a2
Protect My Devices	8c382d51459b91b7f74b23fbad7dd2e8c818961561603c8f6614edc9bb1637d1
Anti-ransomware	7d8a4aa184eb350f4be8706afb0d7527fca40c4667ab0491217b9e1e9d0f9c81
Scam Protection	
Lumina Stealer	
Protect My Family	turninehd[.]com
Protection Score	7594ba29d456e140a171cba12d8d9a2db8405755b81da063a425b1a8b50d073
Parental Controls	
Family Plans	6608aeae3695b739311a47c63358d0f9dbe5710bd0073042629f8d9c1df905a8
Resources	e60d911f2ef120ed782449f1136c23ddf0c1c81f7479c5ce31ed6dcea6f6adf9
Stay Updated	



McAfee Blog

Introducing McAfee:

[Reports and Guides](#)

Identify theft, protection and privacy for your digital life

[McAfee on protection](#)

[NEW McAfee Individual Plans](#)

[Prevent Spam and Phishing](#)

McAfee Labs Threat Research Team

[Learn More](#)

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity

[NEW McAfee Family Plans](#)

through McAfee See our blog posts below for more information.

[Learn at McAfee](#)

[What's Airing?](#)

[What is a VPN?](#)

[Other Products & Services](#)

[What is Identity Theft?](#)

More from McAfee Labs

[Press & News](#)

[Announcements](#)

[The Scam Botest Back: Exploiting the CrowdStrike Outage](#)

[McAfee Newsroom](#)

[Autonomous Private Network \(VPN\)](#)

Author: Lakshya Mathur, Vallabh Chole & Abhishek Karnik Recently we witnessed one of the most

[AI News & Scams](#)

[Mobile Security](#)

[About Us](#)

[Jul 26, 2024 | 6 MIN READ](#)

[Our Company](#)

[TechMaster Concierge](#)

[Olympics Has Fallen – A Misinformation Campaign Featuring a Voice Cloned Elon Musk](#)

[Company Overview](#)

[Autonomous Private Network \(VPN\) and Abhishek Karnik As the world gears up for the 2024 Paris Olympics,...](#)

[Awards & Reviews](#)

[Jul 26, 2024 | 6 MIN READ](#)

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Quarterly Analyst Trial the Counter-Intuitive GenAI Key.](#)

[Device Security Scan](#)

It's been a while since OpenAI launched ChatGPT, driving increased mainstream awareness of

[Password Generator](#)

[Integrity & Ethics](#)

[Jul 26, 2024 | 3 MIN READ](#)

[Features](#)

[Keep Me Private Online](#)

[Join Us](#)

[Fake Bahrain Government Android App Steals Personal Data Used for Financial Fraud](#)

[Personal Data Cleanup](#)

[Autonomous Private Network \(VPN\) Many government agencies provide their services online for the convenience of](#)

[Online Account Cleanup](#)

[Autonomous Private Network \(VPN\)](#)

[Autonomous Private Network \(VPN\)](#)

[Social Privacy Manager](#)

[Our Locations](#)

[How Scammers Hijack Your Instagram](#)

[Why McAfee Identity](#)

[Autonomous Private Network \(VPN\) Author: Vignesh Dhatchanamoorthy, Rachana S Instagram, with its vast user base and dynamic](#)

[Identity Monitoring](#)

[Credit Monitoring](#)

[May 14, 2024 | 6 MIN READ](#)

[Security Freeze](#)

[Customer Support](#)

[From Spill to AsyncRAT & Restoration in Non-PE Cyber Threats](#)

[Support Community](#)

[Autonomous Private Network \(VPN\) Author: Vignesh Dhatchanamoorthy, Rachana S AsyncRAT, also known as "Asynchronous Remote Access](#)

[Protect My Devices](#)

[Trojan presents a...](#)

[Activation](#)

[Antivirus](#)

[The Scam Botest Back: Exploiting Autohotkey & Attempt to Evade Smartscreen](#)

[Web Protection](#)

[Autonomous Private Network \(VPN\) Author: Vignesh Dhatchanamoorthy, Rachana S McAfee Labs has recently uncovered a](#)

[Protect My Family](#)

[Apr 29, 2024 | 13 MIN READ](#)

[Protection Score](#)

[Parental Controls](#)

[Redline Stealer: A Novel Approach](#)

[Family Plans](#)

[Autonomous Private Network \(VPN\) Author: Mohansundaram M and Neil Tyagi A new packed variant of the Redline Stealer trojan was...](#)

[Resources](#)

[Apr 17, 2024 | 10 MIN READ](#)

[Stay Updated](#)

[Distribution Campaign Evolution of Pikabot Malware](#)

[Pikabot One-Click](#)

Author: [Anandhika](#) and [Preksha](#) Introduction PikaBot is a malicious backdoor that has been active since early on YouTube

[NEW McAfee Individual Plans](#)

App: [Prevent Spam and Phishing](#)

Complete privacy, identity and device protection for individuals.

[Learn More](#)

[Android Phishing Scam Using Malware-as-a-Service on the Rise in India](#)

[NEW McAfee Family Plans](#)

Author: [Zepeng Chen](#) and [Wenfeng Yu](#) McAfee Mobile Research Team has observed an active scam malware... Complete privacy, identity and device protection for up to 6 family members.

[What is a VPN?](#)

Mac: [McAfee VPN](#) READ

[Other Products & Services](#)

[What is Identity Theft?](#)

[Rising Deceptive PDF: The Gateway to Malicious Payloads](#)

[McAfee News](#)

Author: [Pranav Yashvi Shah](#) and [Preksha Saxena](#) McAfee Labs has recently observed a significant surge in the virtual Private Network (VPN)

[AI News & Scams](#)

Mac: [Mobile Security](#) MIN READ

[About Us](#)

[PC Optimizer](#)

[Guardian Unpacked: Decrypting the Threat of Malicious SVG Files](#)

[TechMaster Concierge](#)

Author: [Vignesh Dhatchanamoorthy](#) In the ever-evolving landscape of cybersecurity threats, staying ahead of malicious actors requires...

[McAfee Tools & Downloads](#)

Feb 28, 2024 | 5 MIN READ

[Investors](#)

[Web Protection](#)

[Our Efforts](#)

[Backdoor Virus Trial](#)



[Device Security Scan](#)

[Inclusion & Diversity](#)

[Password Generator](#)

[Integrity & Ethics](#)

[Features](#)

[Public Policy](#)

[Keep Me Private Online](#)

[Join Us](#)

[Personal Data Cleanup](#)

[Careers](#)

[Online Account Cleanup](#)

[Life at McAfee](#)

[VPN \(Virtual Private Network\)](#)

[Our Team](#)

[Social Privacy Manager](#)

[Our Locations](#)

[Safeguard My Identity](#)

[Why McAfee](#)

[Support](#)

[Identity Monitoring](#)

[Help](#)

[Credit Monitoring](#)

[Security Freeze](#)

[Customer Support](#)

[Identity Theft Coverage & Restoration](#)

[Support Community](#)

[Pages](#)

[Password Manager](#)

[Protect My Devices](#)

[Contact Us](#)

[Activation](#)

[Antivirus](#)

[Scam Protection](#)

[Activate Retail Card](#)

[Web Protection](#)

[Protect My Family](#)

[Protection Score](#)

[Parental Controls](#)

[Family Plans](#)

[Resources](#)

[Stay Updated](#)