Behind the CAPTCHA: A Clever Gateway of Malware

mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/

September 20, 2024

McAfee Labs

Sep 20, 2024

8 MIN READ

Authored by Yashvi Shah and Aayush Tyagi

Executive summary

McAfee Labs recently observed an infection chain where fake CAPTCHA pages are being leveraged to distribute malware, specifically Lumma Stealer. We are observing a campaign targeting multiple countries. Below is a map showing the geolocation of devices accessing fake CAPTCHA URLs, highlighting the global distribution of the attack.

Products
All-In-One Protection

NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.

NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.

Other Products & Services

Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Dowloads

Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online

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
Prevent Spam and Phishing
Learn More

Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News

McAfee Newsroom
AI News & Scams
About Us
Our Company

Figure 1: Prevalence on the field

We identified two infection vectors leading users to these fake CAPTCHA pages: one via cracked game download URLs, and the other through phishing emails. GitHub users have been targeted by phishing emails prompting them to address a fictitious “security vulnerability” in a project repository to which they have contributed or subscribed. These emails direct users to visit “github-scanner[.]com” for further information about the alleged security issue.

The CAPTCHA infection chain operates by deceiving users into clicking on buttons like “Verify you are a human” or “I am not a robot.” Once clicked, a malicious script is copied to the user’s clipboard. Users are then misled into pasting the script after pressing the Windows key + R, unknowingly executing the malware. This method of trickery facilitates the infection process, making it easy for attackers to deploy malware.

Figure 2: Infection chain

Attack Vectors and Technical Analysis

As illustrated in the diagram, users are redirected to fake CAPTCHA pages through two main attack vectors:

1. Cracked Gaming Software Download URLs:

Users attempting to download pirated or cracked versions of gaming software are redirected to malicious CAPTCHA pages.

Our Company

Company Overview
Awards & Reviews
Investors
Our Efforts

Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us

Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support

Help

Customer Support
Support Community
FAQs
Contact Us
Activation

Activate Retail Card

Products

All-In-One Protection

NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for Individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services

Antivirus
Scam Protection
Virtual Private Network (VPN)
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

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
Prevent Spam and Phishing
Learn More

Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News

McAfee Newsroom
AI News & Scams
About Us
Our Company

Our Company

Company Overview
Awards & Reviews
Investors
Our Efforts

Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us

Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help

Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products

AI-In-One Protection

NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.

NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.

Other Products & Services

Antivirus
Scam Protection
Virtual Private Network (VPN)
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

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
Prevent Spam and Phishing
Learn More

Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News

McAfee Newsroom
AI News & Scams
About Us
Our Company

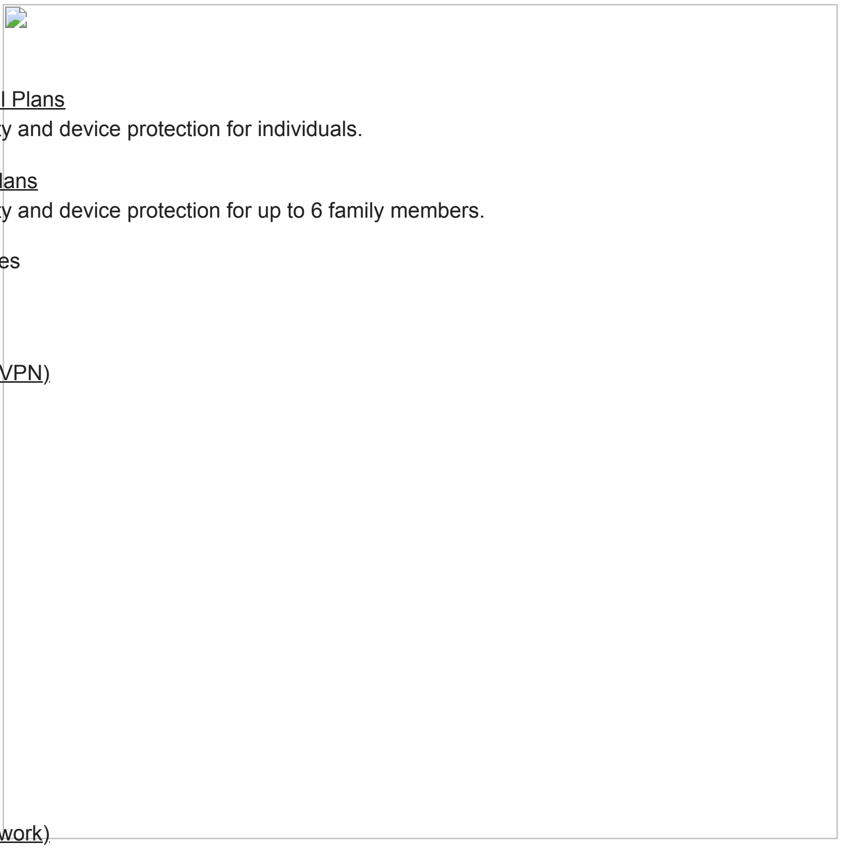

Figure 3: Search to download the cracked version of the game

When users search the Internet for free or cracked versions of popular video games, they may encounter online forums, community posts, or public repositories that redirect them to malicious links.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts

Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us

Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help

Customer Support
Support Community
FAQs
Contact Us
Activation

Activate Retail Card

Products
All-In-One Protection

NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.

NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.

Other Products & Services

Antivirus
Scam Protection
Virtual Private Network (VPN)
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

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
Prevent Spam and Phishing
Learn More

Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News

McAfee Newsroom
AI News & Scams
About Us
Our Company

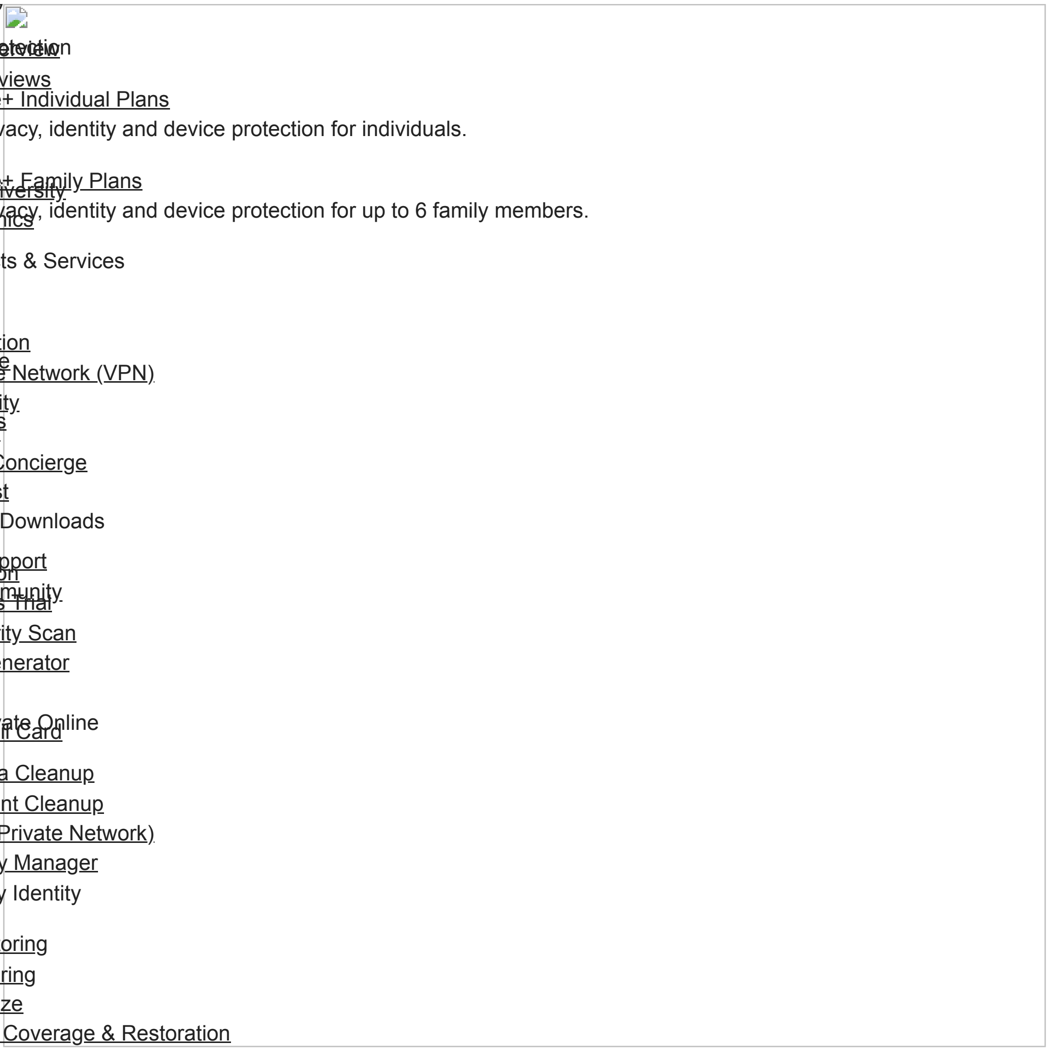

Figure 4: Runkit directing the user to download the game

In this instance, a public Runkit notebook hosts the malicious link (highlighted in blue). When the user accesses the URL (highlighted in red), they are redirected to fake CAPTCHA websites.

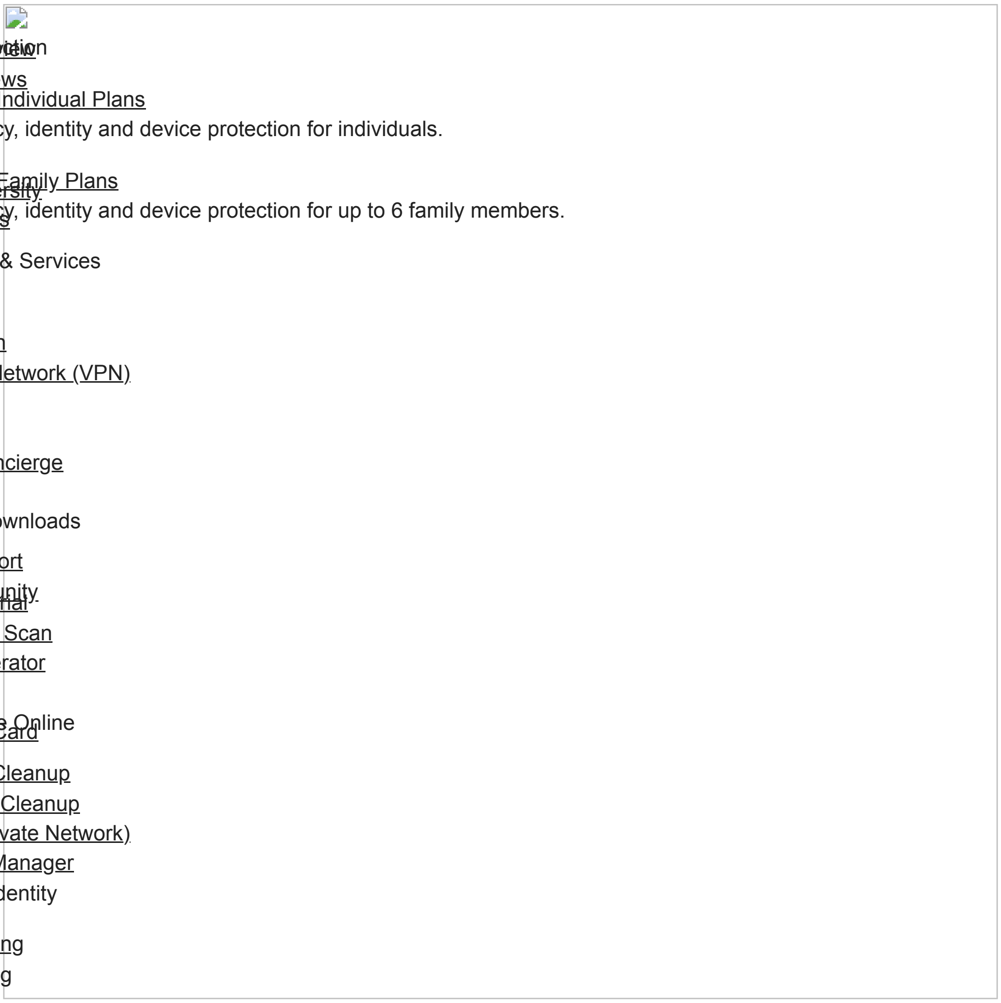

Figure 5: Redirection happening while accessing the link

On this page, after the user clicks the “I’m not a robot” button, a malicious PowerShell script is copied to their clipboard, and they are prompted to execute it.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

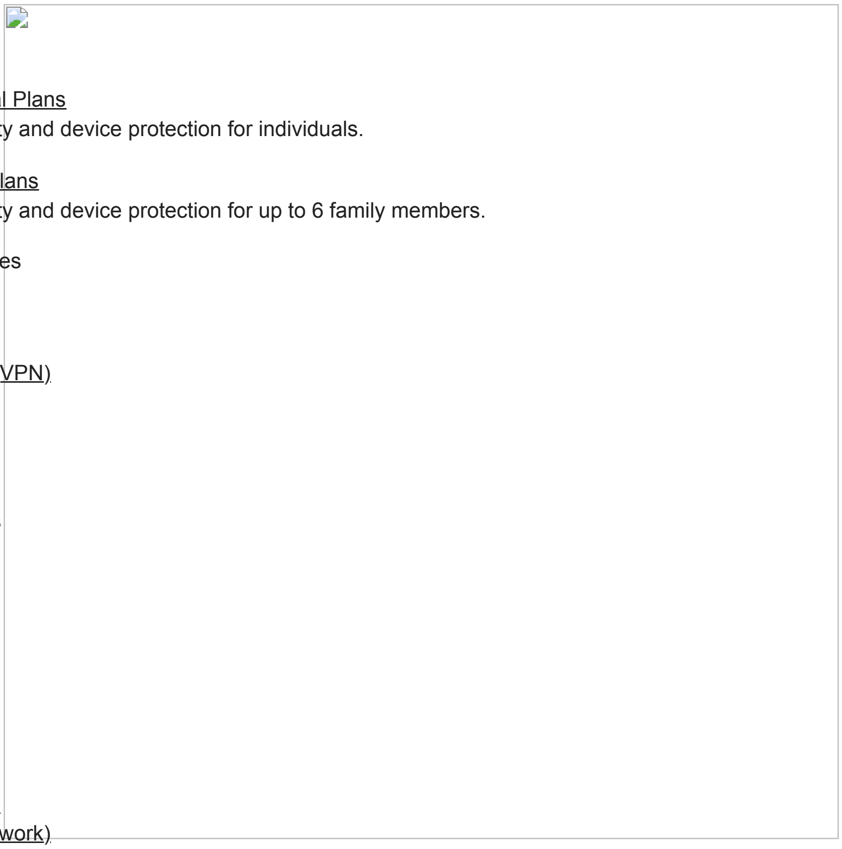

Figure 6: Backend script on the click button

The website includes JavaScript functionality that copies the script to the clipboard.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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

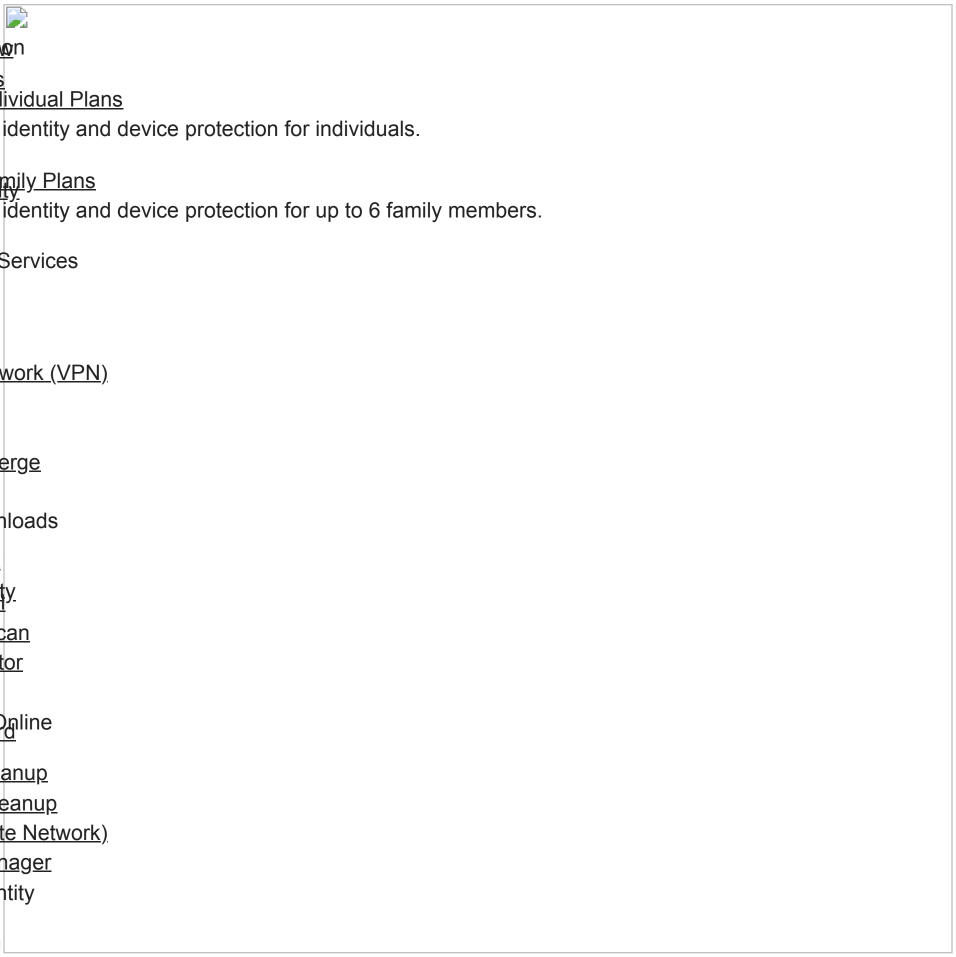

Figure 7: Decoded script

The script is Base64-encoded (highlighted in blue), to reduce the readability to the user. Upon decoding it (highlighted in red), mshta was found to be leveraged. The file hosted at https://verif.dlvideosfre[.]click/2ndhsoru contains a Windows binary, having scripts appended as the overlay. Without the overlay appended, the file is a clean Windows binary.

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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

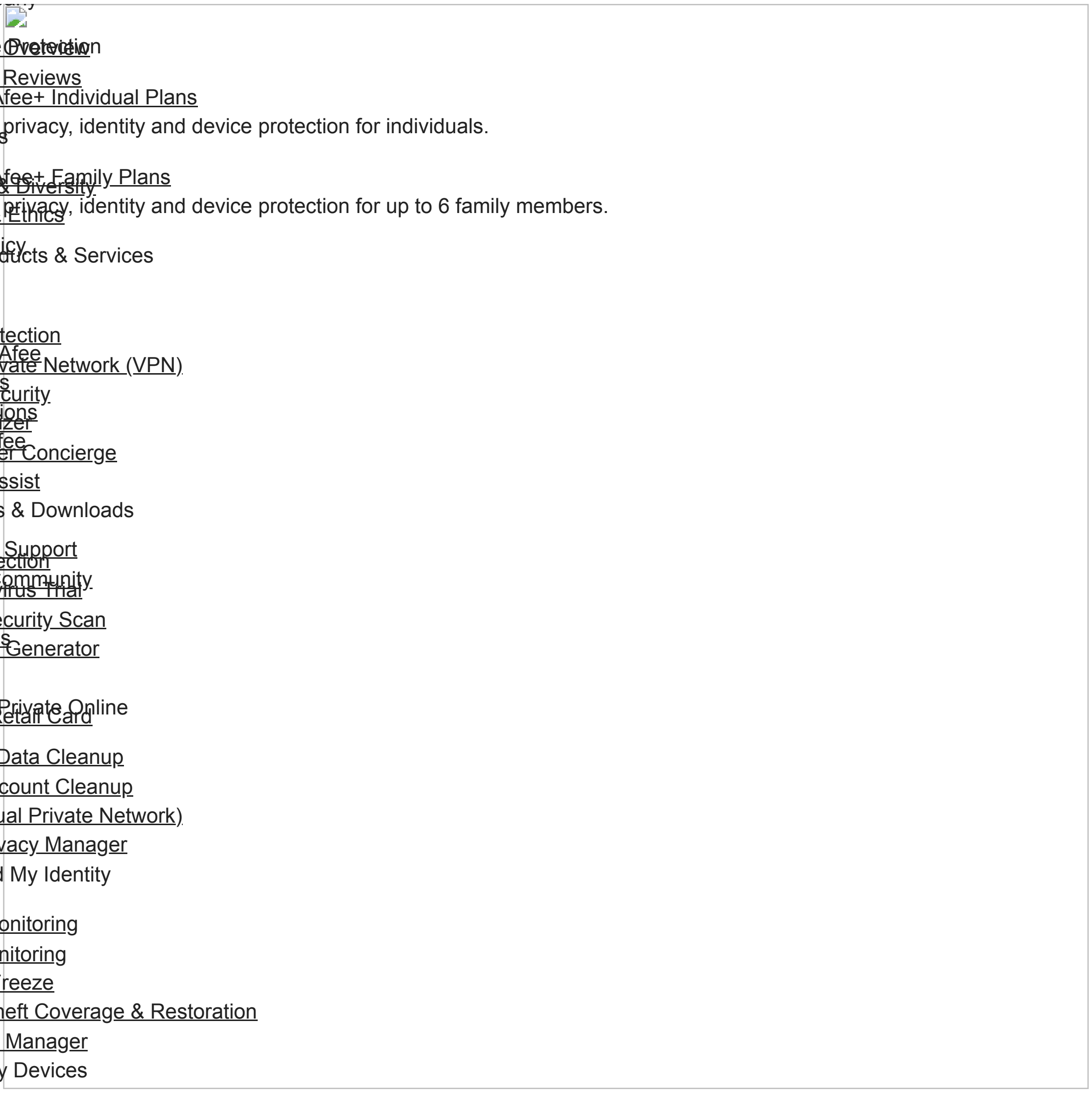

Figure 8: Windows binary with appended script

The mshta utility searches for the <script> tag within a file and executes the script embedded in it, completely ignoring the binary portion of the file. This allows attackers to embed malicious scripts alongside non-executable content, making it easier for the malware to go undetected while still being executed through mshta.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Figure 9: Obfuscated script appended in the downloaded file

Upon analysis, the script was found to be an encrypted JavaScript file, utilizing two layers of encryption. This multi-level encryption obscures the script's true functionality, making detection and analysis more challenging for security tools. Further analysis revealed that the decrypted JavaScript was designed to download Lumma Stealer using AES-encrypted PowerShell command and drop it in the Temp folder. This technique helps the malware avoid detection by placing the payload in a commonly used, less scrutinized directory, facilitating the next stage of the infection.

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

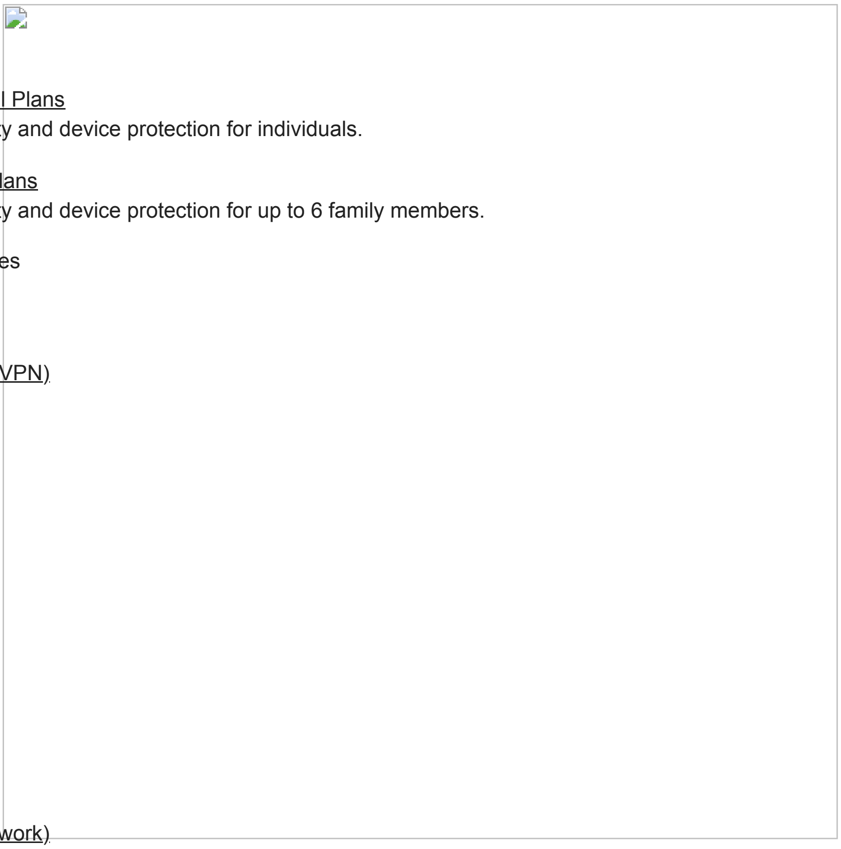

Figure 10: Process tree

2. Phishing Emails impersonating the GitHub team

In the second vector, users receive phishing emails, often targeting GitHub contributors, urging them to address a fake “security vulnerability.” These emails contain links leading to the same fake CAPTCHA pages.

Our Company

Company Overview

Awards & Reviews

Investors

Our Efforts

Inclusion & Diversity

Integrity & Ethics

Public Policy

Join Us

Careers

Life at McAfee

Our Teams

Our Locations

Why McAfee

Support

Help

Customer Support

Support Community

FAQs

Contact Us

Activation

Activate Retail Card

Products

All-In-One Protection

NEW McAfee+ Individual Plans

Complete privacy, identity and device protection for individuals.

NEW McAfee+ Family Plans

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

Other Products & Services

Antivirus

Scam Protection

Virtual Private Network (VPN)

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

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

Prevent Spam and Phishing

Learn More

Learn at McAfee

What is Antivirus?

What is a VPN?

What is Identity Theft?

Press & News

McAfee Newsroom

AI News & Scams

About Us

Our Company

Figure 11: Phishing email impersonating GitHub

Once the user clicks on the link, they're redirected to the fake captcha pages.

Figure 12: Fake CAPTCHA page

These pages use the same technique: the malicious script is copied to the clipboard when the user clicks the button, and they are then prompted to execute it.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

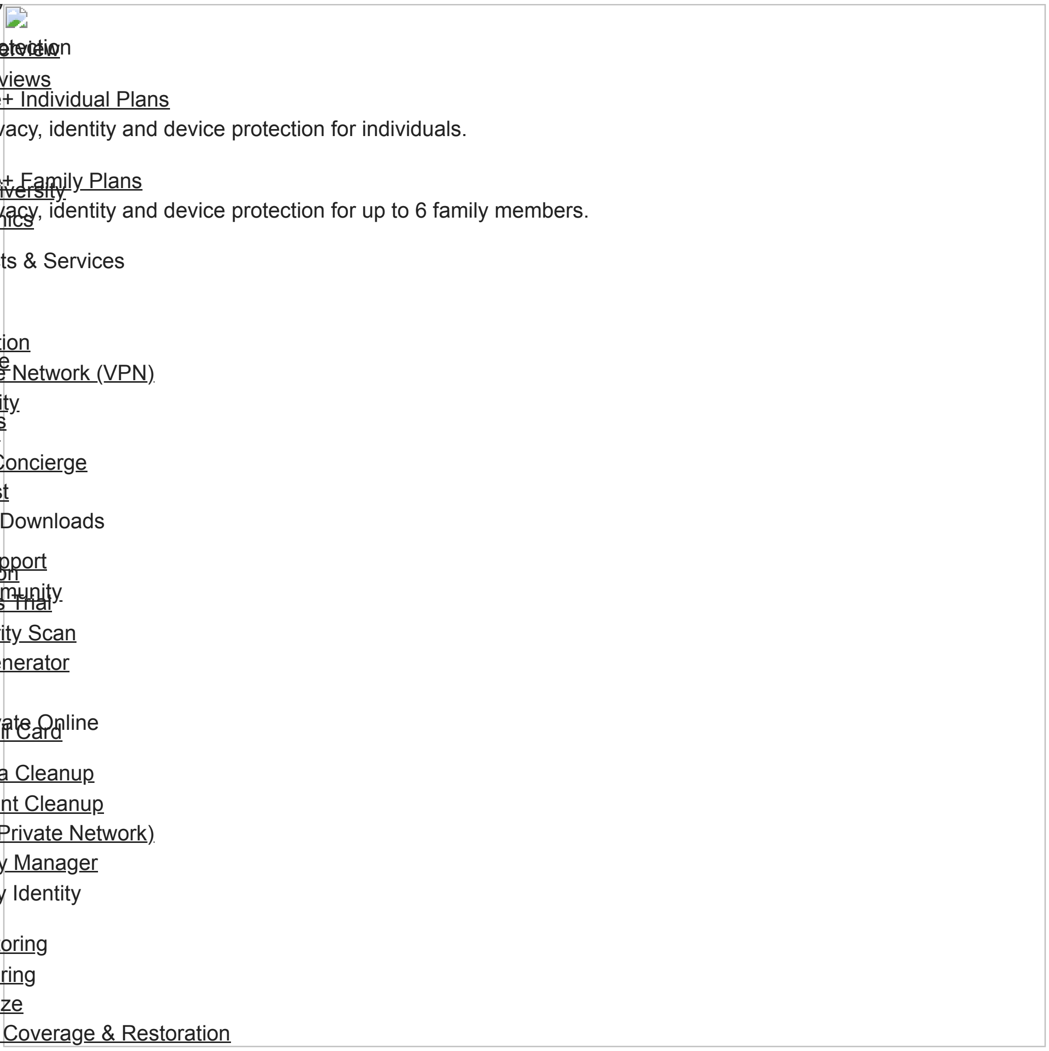

Figure 13: Script copied onto clipboard

This script retrieves and executes the contents of a text file hosted on an online server.

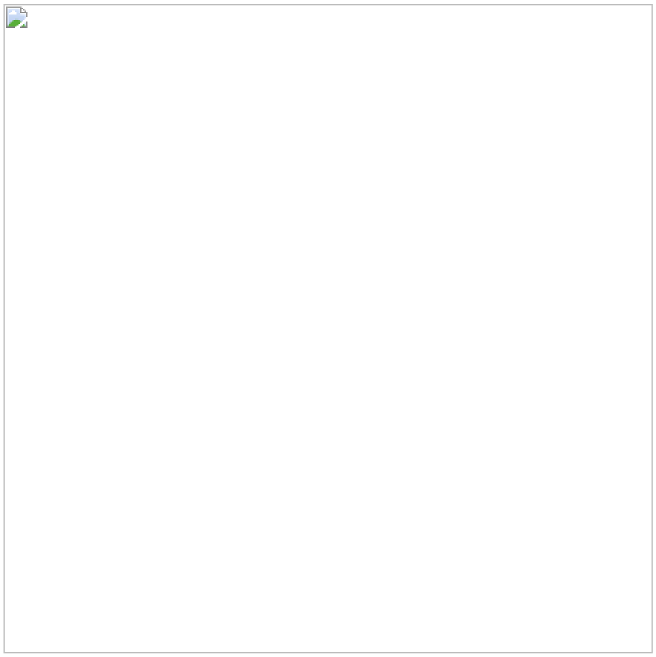

Figure 14: Invoking the remote script

The content of the text file contains PowerShell commands that download an executable file or a zip file. These files are saved into the temp folder and then executed. The downloaded files, in these cases, are Lumma Stealer samples.

Detection and Mitigation Strategies

McAfee blocks this infection chain at multiple stages.

1. URL blocking of the fake CAPTCHA pages.

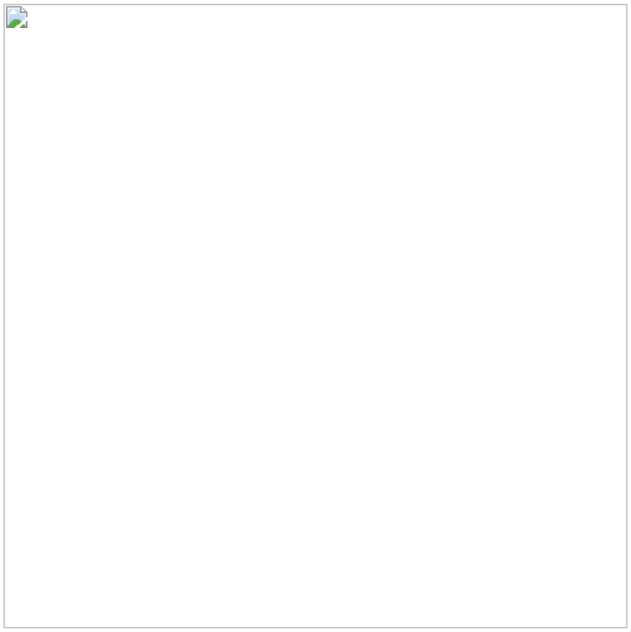

Figure 15: McAfee blocking URLs

2. Heuristic blocking of malicious use of mshta.

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
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
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

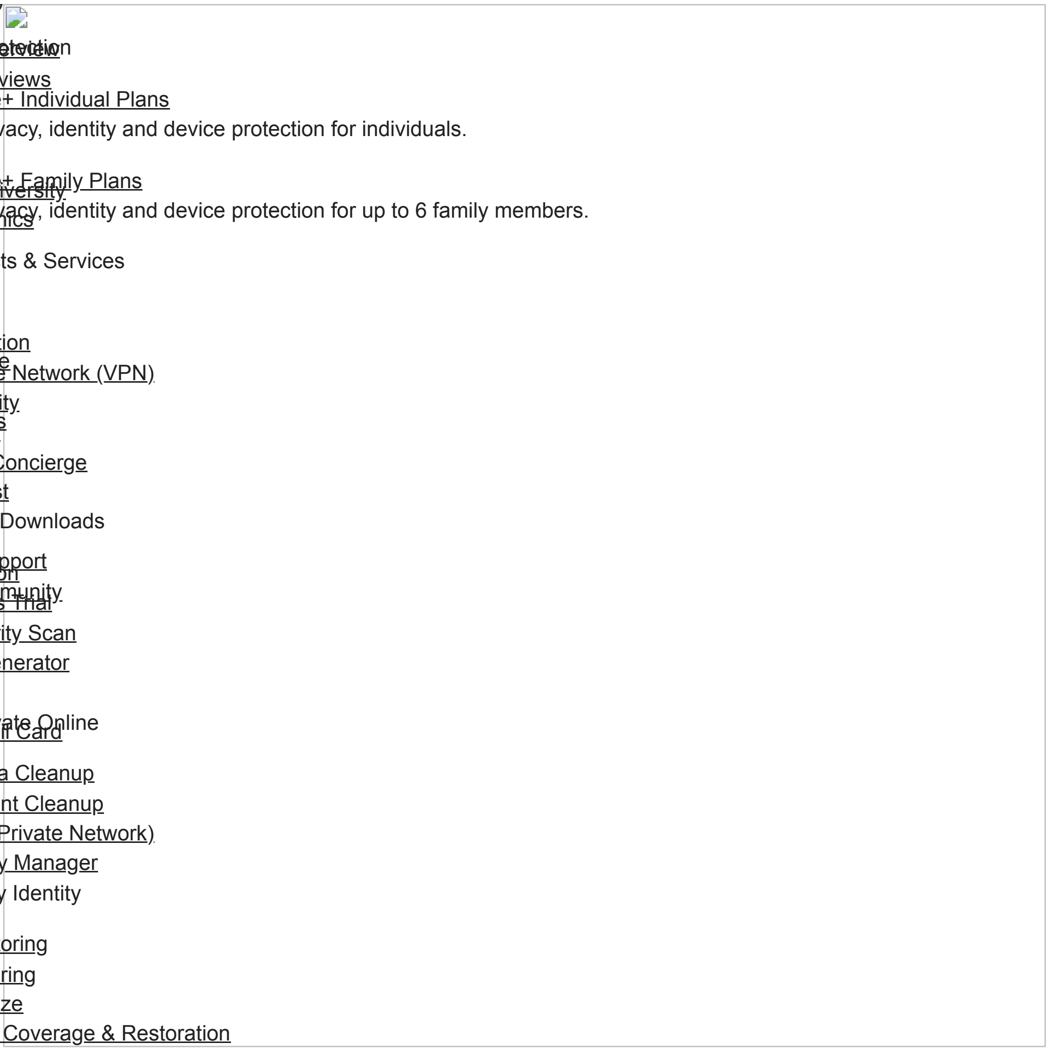

Figure 16: McAfee blocking the malicious behavior

Conclusion and Recommendations

In conclusion, the ClickFix infection chain demonstrates how cybercriminals exploit common user behaviors—such as downloading cracked software and responding to phishing emails—to distribute malware like Lumma Stealer. By leveraging fake CAPTCHA pages, attackers deceive users into executing malicious scripts that bypass detection, ultimately leading to malware installation.

The infection chain operates through two main vectors: cracked gaming software download URLs and phishing emails impersonating GitHub. In both cases, users are redirected to malicious CAPTCHA pages where scripts are executed to download and install malware. The use of multi-layered encryption further complicates detection and analysis, making these attacks more sophisticated and harder to prevent.

At McAfee Labs, we are committed to helping organizations protect themselves against sophisticated cyber threats, such as the Clickfix social engineering technique. Here are our recommended mitigations and remediations:

1. Conduct regular training sessions to educate users about social engineering tactics and phishing schemes.
2. Install and maintain updated antivirus and anti-malware software on all endpoints.
3. Implement robust email filtering to block phishing emails and malicious attachments.
4. Use network segmentation to limit the spread of malware within the organization.
5. Ensure all operating systems, software, and applications are kept up to date with the latest security patches.
6. Avoid downloading cracked software or visiting suspicious websites.
7. Verify URLs in emails, especially from unknown or unexpected sources.
8. Restrict clipboard-based scripts and disable automatic script execution.
9. Keep antivirus solutions updated and actively scan.
10. Educate users to avoid suspicious CAPTCHA prompts on untrusted sites.
11. Regularly patch browsers, operating systems, and applications.
12. Monitor the Temp folder for unusual or suspicious files.

Indicators of Compromise (IoCs)

File Type	SHA256/URLs
	Fake Captcha Websites
URL	Goseverydayre[.]click/
URL	Newvideozones[.]click/veri[.]html
URL	Clickthistogo[.]com/go/67fe87ca-a2d4-48ae-9352-c5453156df67?var_3=F60A0050-6F56-11EF-AA98-FFC33B7D3D59
URL	Downloadstep[.]com/go/08a742f2-0a36-4a00-a979-885700e3028c
URL	Betterdirectit[.]com/
URL	Betterdirectit[.]com/go/67fe87ca-a2d4-48ae-9352-c5453156df67
URL	heroic-genie-2b372e[.]netlify[.]app/please-verify-z[.]html
URL	Downloadstep[.]com/go/79553157-f8b8-440b-ae81-0d81d8fa17c4
URL	Downloadsbeta[.]com/go/08a742f2-0a36-4a00-a979-885700e3028c
URL	Streamingsplays[.]com/go/6754805d-41c5-46b7-929f-6655b02fce2c
URL	Streamingsplays[.]com/go/b11f973d-01d4-4a5b-8af3-139daaa5443f
URL	Streamingszone[.]com/go/b3ddd860-89c0-448c-937d-acf02f7a766f?c=AOsl62afSQUAEX4CAEJPFwASAAAAAABQ
URL	Streamingsplays[.]com/go/1c406539-b787-4493-a61b-f4ea31ffbd56
URL	github-scanner[.]shop/
URL	github-scanner[.]com/
URL	botcheck.b-cdn[.]net/captcha-verify-v7.html

Redirecting Websites

URL	Rungamepc[.]ru/?load=Black-Myth-Wukong-crack
URL	game02-com[.]ru/?load=Cities-Skylines-2-Crack-Setup
URL	Rungamepc[.]ru/?load=Dragons-Dogma-2-Crack
URL	Rungamepc[.]ru/?load=Dying-Light-2-Crack
URL	Rungamepc[.]ru/?load=Monster-Hunter-Rise-Crack

Websites Containing Malicious URLs

URL	Runkit[.]com/wukong/black-myth-wukong-crack-pc
URL	Runkit[.]com/skylinespc/cities-skylines-ii-crack-pc-full-setup
URL	Runkit[.]com/masterposte/dying-light-2-crack-on-pc-denuvo-fix
URL	Runkit[.]com/dz4583276/monster-hunter-rise-crack-codex-pc/1.0.0/clone
URL	Groups[.]google[.]com/g/hogwarts-legacy-crack-empress
URL	By[.]tribuna[.]com/extreme/blogs/3143511-black-myth-wukong-full-unlock/

Malware Samples

PS	b6a016ef240d94f86e20339c0093a8fa377767094276730acd96d878e0e1d624
PS	cc29f33c1450e19b9632ec768ad4c8c6adbf35adaa3e1de5e19b2213d5cc9a54
ZIP	632816db4e3642c8f0950250180dfffe3d37dca7219492f9557faf0ed78ced7c
ZIP	19d04a09e2b691f4fb3c2111d308dcfa2651328dfddef701d86c726dce4a334a
EXE	d737637ae5f121d11a6f3295bf0d51b06218812b5ec04fe9ea484921e905a207

Our Company
Products
All-In-One Protection
Company Overview
Awards & Reviews
NEW McAfee+ Individual Plans
Investors
Complete privacy, identity and device protection for individuals.
Our Efforts
NEW McAfee+ Family Plans
Inclusion & Diversity
Complete privacy, identity and device protection for up to 6 family members.
Integrity & Ethics
Public Policy
Other Products & Services
Join Us
Antivirus
Careers
Scam Protection
Life at McAfee
Virtual Private Network (VPN)
Our Teams
Mobile Security
Our Locations
PC Optimizer
Why McAfee
TechMaster Concierge
Support
McAfee Assist
Help
Free Tools & Downloads
Customer Support
Web Protection
Support Community
Free Antivirus Trial
FAQs
Device Security Scan
Contact Us
Password Generator
Activation
Features
Keep Me Private Online
Activate Retail Card
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
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company

EXE	bbf7154f14d736f0c8491fb9fb44d2f179cdb02d34ab54c04466fa0702ea7d55
HTA	fa58022d69ca123cbc1bef13467d6853b2d55b12563afdbb81fc64b0d8a1d511

Introducing McAfee+

Keep your data private, avoid scams, and protect yourself with AI-powered technology.

McAfee Labs Threat Research Team

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs

Cracked Software or Cyber Trap? The Rising Danger of AsyncRAT Malware

Authored by Neil Tyagi In cybersecurity, threats constantly evolve, and new ways to exploit unsuspecting users are...

Sep 18, 2024 | 14 MIN READ

New Android SpyAgent Campaign Steals Crypto Credentials via Image Recognition

Authored by SangRyol Ryu Recently, McAfee's Mobile Research Team uncovered a new type of mobile malware that...

Sep 05, 2024 | 10 MIN READ

The Scam Strikes Back: Exploiting the CrowdStrike Outage

Authored by Lakshya Mathur, Vallabh Chole & Abhishek Karnik Recently we witnessed one of the most significant...

Jul 30, 2024 | 5 MIN READ

Olympics Has Fallen – A Misinformation Campaign Featuring a Voice Cloned Elon Musk

Authored by Lakshya Mathur and Abhishek Karnik As the world gears up for the 2024 Paris Olympics,...

Jul 26, 2024 | 6 MIN READ

ClickFix Deception: A Social Engineering Tactic to Deploy Malware

Authored by Yashvi Shah and Vignesh Dhatchanamoorthy McAfee Labs has discovered a highly unusual method of malware...

Jul 11, 2024 | 9 MIN READ

Quality Over Quantity: the Counter-Intuitive GenAI Key

It's been almost two years since OpenAI launched ChatGPT, driving increased mainstream awareness of and access to...

Jun 28, 2024 | 3 MIN READ

Fake Bahrain Government Android App Steals Personal Data Used for Financial Fraud

Authored by Dexter Shin Many government agencies provide their services online for the convenience of their citizens....

May 31, 2024 | 7 MIN READ

How Scammers Hijack Your Instagram

Authored by Vignesh Dhatchanamoorthy, Rachana S Instagram, with its vast user base and dynamic platform, has become...

May 14, 2024 | 6 MIN READ

From Spam to AsyncRAT: Tracking the Surge in Non-PE Cyber Threats

Authored by Yashvi Shah and Preksha Saxena AsyncRAT, also known as "Asynchronous Remote Access Trojan," represents a...

May 08, 2024 | 10 MIN READ

The Darkgate Menace: Leveraging Autohotkey & Attempt to Evade Smartscreen

Authored by Yashvi Shah, Lakshya Mathur and Preksha Saxena McAfee Labs has recently uncovered a novel infection...

Apr 25, 2024 | 13 MIN READ

Redline Stealer: A Novel Approach

Authored by Mohansundaram M and Neil Tyagi A new packed variant of the Redline Stealer trojan was...

Apr 17, 2024 | 10 MIN READ

Distinctive Campaign Evolution of Pikabot Malware

Authored by Anuradha and Preksha Introduction PikaBot is a malicious backdoor that has been active since early...

Apr 02, 2024 | 10 MIN READ

Back to top

Back to top

Our Company

Products

All-in-One Protection

Company Overview

Awards & Reviews

NEW McAfee+ Individual Plans

Investors

Complete privacy, identity and device protection for individuals.

Our Efforts

NEW McAfee+ Family Plans

Inclusion & Diversity

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

Integrity & Ethics

Public Policy

Other Products & Services

Join Us

Antivirus

Careers

Scam Protection

Life at McAfee

Virtual Private Network (VPN)

Our Teams

Mobile Security

Our Locations

PC Optimizer

Why McAfee

TechMaster Concierge

Support

McAfee Assist

Help

Free Tools & Downloads

Customer Support

Web Protection

Support Community

Free Antivirus Trial

FAQs

Device Security Scan

Contact Us

Password Generator

Activation

Features

Keep My Privacy Online

Activate Retail Card

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

Prevent Spam and Phishing

Learn More

Learn at McAfee

What is Antivirus?

What is a VPN?

What is Identity Theft?

Press & News

McAfee Newsroom

AI News & Scams

About Us

Our Company