مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Lumma Stealer Malware Exploits Fake CAPTCHA Pages

Tracking #:432316431

Date:25-10-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed threat actors exploits fake CAPTCHA pages to deliver Lumma Stealer Malware.

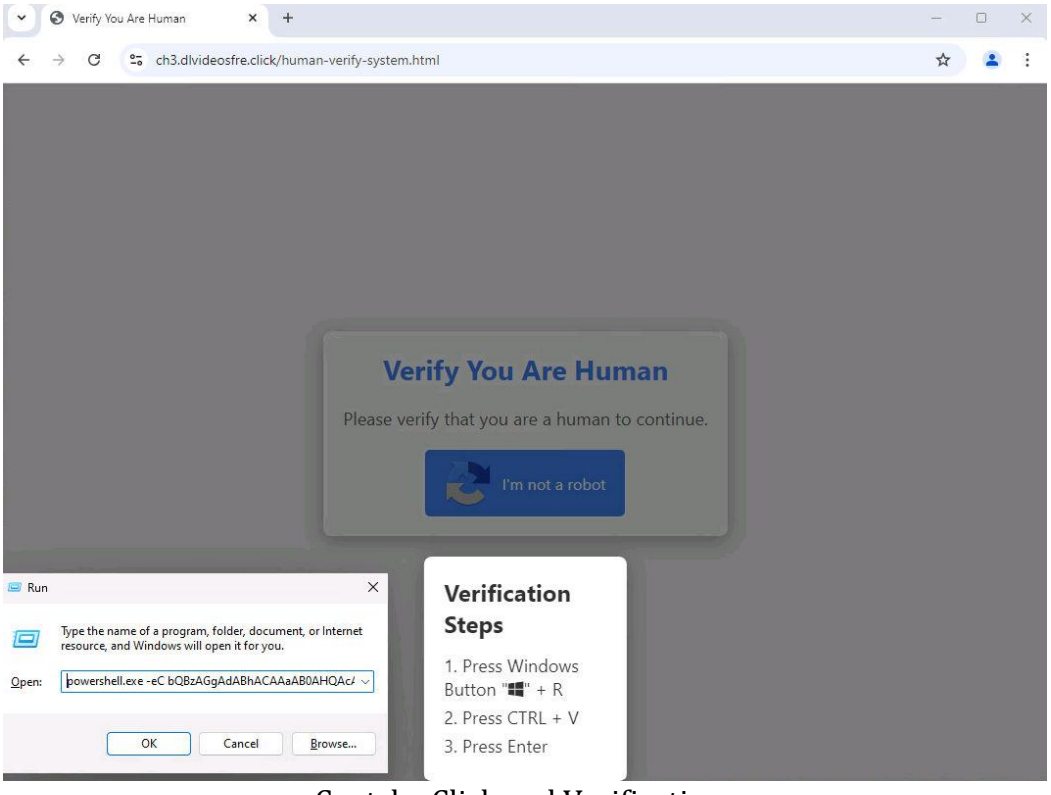
TECHNICAL DETAILS:

Lumma Stealer is an advanced information-stealing malware distributed through a sophisticated Malware-as-a-Service (MaaS) model. It targets sensitive data such as passwords, browser information, and cryptocurrency wallet details. The malware has evolved its tactics, moving from traditional phishing methods to using fake CAPTCHA verification pages. These pages exploit legitimate software to deliver Lumma Stealer, making it a persistent threat. Recent campaigns have shown the use of multi-stage fileless techniques and deceptive delivery methods, highlighting the need for heightened vigilance and robust cybersecurity measures.

Details:

Attack Vector and Execution Chain

- Phishing Campaigns: Threat actors create phishing sites hosted on platforms like Amazon S3 and CDNs. These sites mimic legitimate verification pages, including fake Google CAPTCHA forms
- Fake CAPTCHA Verification: Users are tricked into executing a PowerShell command by completing fake CAPTCHA steps, which downloads an initial malware stager onto their machine
- Multi-Stage Fileless Techniques: The attack chain involves multiple stages, including the use of mshta.exe to execute obfuscated JavaScript, which further downloads encrypted payloads



Captcha Click and Verification

Payload Delivery and Execution

- Obfuscation and Encryption: The malware uses Base64-encoded scripts and AES-encrypted payloads to evade detection6.
- Process Hollowing: Lumma Stealer employs process hollowing techniques, injecting its payload into legitimate processes like BitLockerToGo.exe.
- Data Exfiltration: After infection, Lumma Stealer searches for sensitive files related to cryptocurrency and passwords, exfiltrating data via command-and-control servers using ".shop" domains

Indicators of Compromise (IoC)

- Use of Cloudflare CDN for payload delivery.
- Connection attempts to ".shop" domain C2 servers.
- Presence of specific file names like seed.txt, pass.txt, *.kbdx on infected systems.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

1. User Education and Awareness
    - Educate users about the risks of phishing attacks and the specific dangers of fake CAPTCHA pages.
    - Encourage skepticism towards unusual requests to run commands via the "Run" dialog or paste unknown commands.
2. Technical Measures
    - Deploy advanced 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 systems and software to mitigate vulnerabilities.
3. Incident Response and Threat Hunting
    - Incorporate threat detection queries into security playbooks to identify signs of Lumma Stealer infections.
4. Network Security Enhancements
    - Implement Content Delivery Network (CDN) filtering to block malicious sites.
    - Ensure robust firewall configurations to prevent unauthorized access and data exfiltration.

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://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha#iocs