NCA-05.030425 – National CERT Advisory: Fake CAPTCHA-Based Phishing Campaign Delivering Lumma Stealer Malware

Introduction

A large-scale phishing campaign has been identified, exploiting fake CAPTCHA images in PDF files to distribute the Lumma Stealer malware. This campaign has already compromised thousands of users across various sectors, including technology, financial services, and manufacturing, with a focus on North America, Asia, and Southern Europe.

Threat actors are using search engine manipulation to lure victims into downloading malicious PDFs that redirect them to fraudulent sites. These sites either steal financial information or infect systems with malware using PowerShell-based techniques. This advisory provides detailed insights into the attack methodology, indicators of compromise (IOCs), and recommended security measures.

Campaign Details

Attack Mechanism

1. **Malicious PDFs with Fake CAPTCHAs:** Attackers distribute PDF files containing deceptive CAPTCHA images.
2. **Redirection to Malicious Websites:** Clicking the CAPTCHA leads users to phishing sites that either steal sensitive financial data or deploy malware.
3. **PowerShell and MSHTA Exploits:** The malware is executed via a hidden PowerShell script triggered through an MSHTA command, enabling silent installation of Lumma Stealer.
4. **SEO Poisoning:** Malicious PDFs are hosted on platforms like PDFCOFFEE, PDF4PRO, and Internet Archive, appearing in legitimate search engine results.

Lumma Stealer Capabilities

Lumma Stealer is a Malware-as-a-Service (MaaS) tool capable of:

- Stealing login credentials, browser cookies, and cryptocurrency wallet data.
- Using GhostSocks, a proxy malware, to exploit victims' internet connections.
- Selling stolen credentials on underground hacking forums like Leaky[.]pro.

Indicators of Compromise (IOCs)

Malicious Domains

- hxxps://pdf-freefiles[.]com
- hxxps://webflow-docs[.]info

- hxxps://secure-pdfread[.]site
- hxxps://docsviewing[.]net

SHA256 Hashes of Malicious Files

- 8a5f1c9b2e4a64e192c09c04f1b10c71615c62b3aa0a34c4c051e3b8d5314b4d
- d4623a7f7c9b8c42a6735c6f812e9d06ab6c614f3325a17db7bc2b5e2f9a90c7

Recommendations and Action Items

1. Prevention Measures

a. **User Education:** Train employees on identifying phishing tactics, including fake CAPTCHAs and malicious PDFs.

b. **Endpoint Protection:** Deploy advanced endpoint detection and response (EDR) solutions to block PowerShell abuse.

c. **SEO Monitoring:** Organizations should track and report fraudulent domains impersonating legitimate services.

d. **Restrict PowerShell and MSHTA Execution:** Implement Group Policy restrictions to prevent unauthorized execution of scripts.

2. Detection Measures

a. **PowerShell Logging:** Enable detailed logging to monitor for unauthorized PowerShell execution.

b. **Threat Intelligence Feeds:** Subscribe to security feeds to detect new malicious URLs and file hashes.

PKCERT

c. **Use Sigma Rules:** Implement the following Sigma detection rules for monitoring PowerShell download and execution:

```
title: PowerShell MSHTA Execution
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    - Image|endswith: '\mshta.exe'
    - CommandLine|contains: 'http'
condition: selection
level: high
```

3. Incident Response and Mitigation

a. **Block Malicious Domains:** Add identified domains to DNS and web filters to prevent access.

b. **Deploy Behavioral Analysis Tools:** Monitor network traffic for anomalies linked to Lumma Stealer.

c. **Backup and Disaster Recovery:** Regularly back up critical data and validate recovery procedures.

4. Best Practices

a. **Patch Management:** Ensure all systems are updated to mitigate vulnerabilities exploited by PowerShell and MSHTA.

b. **Restrict Admin Privileges:** Limit administrative access to essential personnel to prevent privilege escalation.

c. **Multi-Factor Authentication (MFA):** Enforce MFA to mitigate credential theft risks.

d. **Application Whitelisting:** Allow only trusted applications and scripts to run on enterprise systems.

Conclusion

This advisory underscores the evolving nature of phishing campaigns using fake CAPTCHAs to distribute malware. Given the increasing sophistication of such attacks, National CERT strongly urges organizations to enhance their cybersecurity defenses through proactive monitoring, endpoint protection, and user awareness training.

PKCERT

Organizations should implement the recommended security measures to mitigate the risk posed by this growing threat.