Mphasis
The Next Applied

Sophisticated Phishing Scheme

Date: 08th April 2024 | Severity: High

Summary

A new phishing campaign targeting Latin American Windows users has emerged, utilizing email attachments and fake invoices to distribute malicious payloads. The campaign employs tactics such as using temporary domains and country-specific redirections to evade detection.

Trustwave SpiderLabs researchers noted similarities with past malware campaigns, such as Horabot, targeting Spanish-speaking users. Concurrently, Malwarebytes uncovered a malvertising scheme distributing a remote access trojan via fake NordVPN ads on Microsoft Bing.

Trustwave said the campaign exhibits similarities with that of Horabot malware campaigns that have targeted Spanish-speaking users in Latin America in the past.

Additionally, SonicWall found instances of fake Java installers and Golang malware installing cryptocurrency miners and establishing HTTPS communications with command-and-control servers.

Attack Vectors

- The attack vector primarily involves a phishing email containing a ZIP file attachment, which, when extracted, reveals an HTML file posing as an invoice.
- This HTML file directs users to a malicious link. The attackers employ evasion techniques such as using temporary domains and country-specific redirects.
- Malvertising campaigns are used to distribute malware via fake ads on popular search engines. These ads lead users to download malicious payloads disguised as legitimate software.
- Attackers exploit vulnerabilities in software installers to deploy cryptocurrency miners and establish communication with command-and-control servers.

Phobos Ransomware distribution several ways to end up on your machine:

- The phishing email contained a ZIP file attachment that when extracted reveals an HTML file that leads to a malicious file download posing as an invoice.
- The email message, the company said, originates from an email address format that uses the domain “temporary.link” and has Roundcube Webmail listed as the User-Agent string.

- The HTML file points containing a link “facturasmex.cloud” that displays an error message saying, “this account has been suspended,” but when visited from an IP address geolocated to Mexico, loads a CAPTCHA verification page that uses Cloudflare Turnstile.
- It redirects to another domain from where a malicious RAR file is downloaded. The RAR archive comes with a PowerShell script that gathers system metadata as well as checks for the presence of antivirus software in the compromised machine.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 8f4cf379ee2bef6b60fec792d36895dce3929bf26d0533fbb1fdb41988df7301
IP	• 5.75.147[.]135 • 5.75.149[.]1 • 88.218.170[.]169 • 88.218.170[.]169 • 162.55.188[.]246 • 167.235.134[.]14
Domains	• temporary.link • facturasmex.cloud • tributaria[.]website • facturacionmarzo[.]cloud • m9b4s2[.]site • wiqp[.]xyz • ckws[.]info • amarte[.]store
URLs	• hxxps://facturasmex.cloud • hxxps://facturas.co.in/index.php?va • hxxp://ad2.gotdns.ch/22/22 • hxxp://86.38.217.167/ps/index.php • hxxps://www[.]dropbox[.]com/scl/fi/k6hxua7lwt1qcgmqou6q3/m[.]zip?rlkey=7wu6x4pfvbt64atx11uqpk34l&dl=1 • https://daily-mashriq.org/goyxdrkhjilchyigflztv • http://ip-api.com/json/

Recommendation

- User Education
- Email Filtering
- Endpoint Protection
- Patch Management
- Multi-factor Authentication (MFA)
- Incident Response Plan
- Continuous Monitoring
- Vendor Risk Management
- Regular Security Audits.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/cybercriminals-targeting-latin-america.html
- https://github.com/Cisco-Talos/IOCs/blob/main/2023/05/new-horabot-targets-americas.txt