Mispadu Trojan Targets Europe, Thousands of Credentials Compromised

Date: 4th April 2024 | Severity: High

Summary

The Mispadu Trojan is a notorious banking trojan that has been active for several years, primarily targeting users in Latin America, particularly Brazil and Mexico. However, if it's now targeting Europe and has compromised thousands of credentials, it represents a significant expansion of its operations.

Mispadu, also called URSA, came to light in 2019, when it was observed carrying out credential theft activities aimed at financial institutions in Brazil and Mexico by displaying fake pop-up windows. The Delphi-based malware is also capable of taking screenshots and capturing keystrokes.

The campaign has resulted in thousands of stolen credentials, with records dating back to April 2023. The threat actor leverages these credentials to orchestrate malicious phishing emails, posing a significant threat to recipients.

Attack Vectors

Mispadu typically spreads through malicious email attachments, phishing websites, or other social engineering techniques. Once installed on a victim's computer, it can steal sensitive information such as login credentials, banking details, and personal information. The bypass is simple and relies on a parameter that references a network share, rather than a URL. The crafted .URL file contains a link to a threat actor's network share with a malicious binary.

Mispadu, once launched, reveals its true colors by selectively targeting victims based on their geographic location (America or Western Europe) and system configurations, and then proceeds to establish contact with a command-and-control (C2) server for follow-on data exfiltration. Mispadu uses techniques such as keylogging, screen scraping, browser credential theft, phishing injection, and Bitcoin address hijacking.

Mispadu Trojan distribution several ways to end up on your machine:

- phishing emails with attachments
- PDF's
- Attachments in Invoice themed mails
- Zip Files
- Fake pop-ups
- Shortened URL
- Google Chrome extension

Indicator of Compromise

File Hash:

- A4EDA0DD2C33A644FEEF170F5C24CF7595C19017
- A9BADCBF3BD5C22EEB6FAF7DB8FC0A24CF18D121
- CFE21DBFB97C2E93F099D351DE54099A3FC0C98B
- 63DCBE2DB9CC14564EB84D5E953F2F9F5C54ACD9
- 8B950BF660AA7B5FB619E1F6E665D348BF56C86A
- F6021380AD6E26038B5629189A7ADA5E0022C313
- 76F70276EB95FFEC876010211B7198BCBC460646
- E903B37B1E42D0B8BF0514CB13A46233
- E5967A8274D40E0573C28B664670857E
- a96125294afa1c3f92ab7be615dc1cbe

IP address:

- 104.238.182.44
- 104.238.182.44
- 140.82.47.181
- 140.82.47.181
- 3.19.223.147
- 51.75.95.179

URLs:

- https[:]//www.zairtaz[.]com/wpcontent/plugins/license/inc/hydra/do/it.php?f=9&w=Windows%2010
- http[:]//luzca[.]com/img/do/it.php?f=2&w=Windows%207
- http[:]//luzca[.]com/img/do/it.php?f=2&w=Windows%207
- http[:]//blog.traveldealsbd.com/images/arrow/do/it.php?b1=1&v1=1033&v2=1033&v3=Windows%207&v4=User&v5=X64
- http[:]//tripsapata.com/assets/images/swan/do/it.php
- https[:]//bola.com.au/images/hh/cfdi/do/it.php?f=2&w=Windows%2010
- https[:]//splendidgifts.com.my/hiway/ap2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=User&v6=X64

Recommendation

Do not trust intrusive ads, especially if they are displayed on dubious web pages.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Software should not be downloaded through third party downloaders, unofficial websites, Peer-to-Peer networks such as torrent clients, eMule, or other such tools/sources.

Protect systems from malware attacks by regularly scanning them with a reputable anti-spyware or antivirus suite and ensure that it is up to date.

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/mispadu-trojan-targets-europe-thousands.html

https://www.metabaseq.com/mispadu-banking-trojan/

https://www.pcrisk.com/removal-guides/16423-mispadu-trojan.

Copyright © Mphasis Corporation. All rights reserved.