

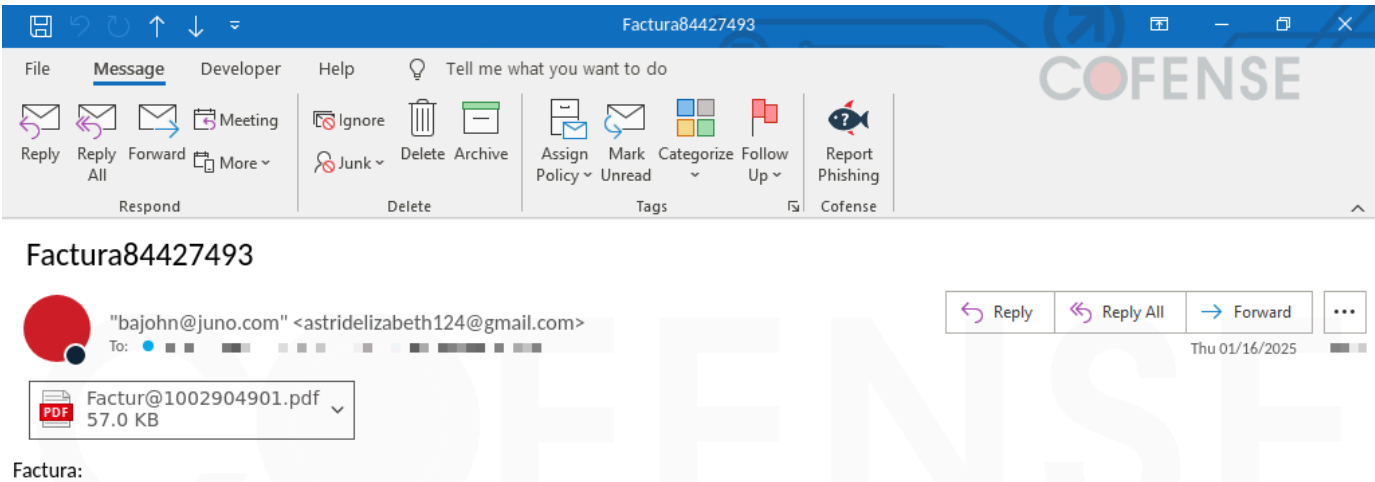
Mispadu Phishing Malware Baseline: Delivery Chains, Capabilities, and Common Campaigns

 cofense.com/blog/mispadu-phishing-malware-baseline

By: Max Gannon, Intelligence Team

Mispadu is a long-standing Banking Trojan that has only continued to grow in popularity since its first observation in 2019. Although originally appearing in small numbers, at the time of this analysis Mispadu is the top Latin American Banking Trojan that Cofense sees.

Current campaigns are seen on a weekly basis, with initial phishing emails bypassing multiple Secure Email Gateways (SEGs) to reach the inboxes of employees across the world. The most popular targeted countries continue to be Latin American, specifically Mexico and Brazil, however some instances of recipients in Europe have also been seen. The most common delivery method continues to be attached PDFs that lead to a chain of scripts before Mispadu is run using legitimate files.



Tactic: PDF Attachment | Threat: Mispadu | SEG: Abnormal Security; Microsoft ATP; Proofpoint; Cisco Ironport

Figure 1: SEG bypass email delivering Mispadu via a chain beginning with an attached PDF.

Key Points

- Mispadu is a Latin American targeted Banking Trojan that focuses primarily on Spanish-speaking Latin American countries like Mexico, Argentina, and Brazil.
- Mispadu has self-propagation capabilities via Outlook contacts, which allows compromised hosts to spread further Mispadu campaign emails without the threat actor specifically targeting further recipients.
- Unlike many other Latin American Banking Trojans, Mispadu targets a large number of online banks, but injects relatively little content into their websites.
- While phishing campaigns delivering Mispadu originally spoofed brands like BBVA Bancomer, Comision Federal de Electricidad, and MEO, most campaigns in the last year did not have well-developed brand spoofing.

History

Mispadu was first written about in depth by [ESET](#) in 2019. At the time, it was a relatively simplistic malware that was primarily delivered via malicious advertisements, notably those for McDonald's coupons. It used external utilities for information theft, easily decoded scripts, and poorly developed pop-up windows.

Mispadu remained relatively small-scale when Cofense saw it again in 2020 through 2023 before taking off in mid 2024. High volumes of well-developed campaigns kicked off in June of 2024, and the volumes have continued to grow ever since.

Current versions feature extensive anti-analysis techniques, obfuscated scripts, geofenced payload downloads, password-protected attachments, dynamically generated payloads, and the use of legitimate files to disguise activities.

Notable Uses by APT Groups

Mispadu does not appear to be a stand-alone malware family utilized by multiple threat actors or APT groups, but is instead a software designed and used by a single APT group. This group is tracked by multiple monikers, but the 3 most often used are:

- TA 2725
- This group has been involved with other Latin American banking trojans such as Grandoreiro but was specifically linked to Mispadu by the [New Jersey Cybersecurity & Communications Integration Cell](#).
- Malteiro

- [SCILabs](#) began tracking the threat actors behind Mispadu/URSA in 2021 using this moniker and notes its continued development and improvements upon past Tactics, Techniques, and Procedures (TTPs).
- Manipulated Caiman
- [Perception Point's](#) IR team tracks the threat actors behind Mispadu with this moniker based on a May 2023 campaign analysis. They note that the APT group has likely accumulated over \$55 million over the course of their usage of Mispadu.

Capabilities

The original version of Mispadu had basic Trojan functionalities, including the ability to take screenshots, send keyboard and mouse input, log keystrokes, and download and run additional malware. It included several additional binaries that enabled it to perform basic credential theft and steal stored credentials from browsers, email clients, and FTP clients. It was able to tamper with clipboard contents, which were used to replace Bitcoin wallet addresses. Additionally, it was capable of injecting basic content into web browsers in order to solicit additional information from victims.

Recent versions of Mispadu continue to use Nirsoft's Web Browser Password Viewer and Email Password Recovery applications, as well as relying on some legitimate executables and DLL files. The threat actors have added the ability to self-propagate on infected hosts via email and expanded the target online banking websites to include banks outside of Latin America as well as cryptocurrency-based exchanges.

Additionally, QR code-based content appears to have been added based on commands such as "QR Novo". Additional IP address geolocation checking tools have also been added to ensure that the victim is in one of the targeted locations. This is done by a combination of IP address-based geolocation utility websites and device language/region fingerprinting from the infected computer.

In The Wild

Although this campaign originally was distributed via advertisements, recently, threat actors have settled into one primary method of delivery with a single variant. As of 2025, all Mispadu campaigns observed by Cofense were initiated by an HTA (HTML Application) file.

The only variation is that sometimes the URL delivering the HTA files is embedded in an attached, password-protected PDF rather than embedded in the email itself. In all recent campaigns, Mispadu makes use of an AutoIT loader and various legitimate files to run the malicious content. Each step of the delivery chain from the attached PDF to AutoIT script is dynamically generated. This means that every hash except for the AutoIT compiler is unique to each install, further frustrating EDR.

Delivery Mechanisms

In 2025, Mispadu has always been delivered by a dynamically generated HTA file, which downloads a dynamically generated JavaScript, which finally downloads a dynamically generated VBS file. The only alternative to this chain is that sometimes the URL to download the HTA file is embedded in an attached PDF rather than the email.

From 2019 through March 2025, the first delivery mechanism in the chain to deliver Mispadu has been either a PDF 64% of the time or an HTA file 26% of the time. In all cases where a PDF was first, an HTA file followed it. Only 2% of the time was Mispadu delivered by an executable, and 9% of the time by an HTML file. Across the measured time, there were 9 different ways that Mispadu was delivered:

Table 1: Infection chains of Mispadu.

Chain	Percent Share of Campaigns
DelphiLoader, Mispadu	2%
HTA, JSDropper, VBS, Mispadu	22%
HTA, Mispadu	4%
HTML, HTA, JSDropper, VBS, Mispadu	4%
HTML, Mispadu	4%
Mispadu	2%
PDF, HTA, JSDropper, VBS, Mispadu	43%
PDF, HTA, Mispadu	18%

A particular note to observe is the fact that the chains are dominated by HTA and PDF, and the HTA to JavaScript File to VBS to Mispadu chain appears the majority (69%) of the time.

Language

Emails delivering Mispadu have been seen targeting a large number of countries from Latin America to Spain, Italy, and Portugal. However, the language most commonly seen on these emails is overwhelmingly Spanish, with approximately 81% of campaigns delivering Mispadu being in Spanish and approximately 18% being in Portuguese. The majority of the Spanish-language emails target customers in Mexico, but have also been seen targeting Colombia and Argentina.

Behavior

Mispadu is currently delivered as a compiled AutoIT script and an associated encrypted file that is run using the legitimate AutoIT interpreter. The same Auto IT interpreter binary (md5: *0adb9b817f1df7807576c2d7068dd931*) has been used in almost every campaign going back to June of 2024 at the time of this report. However, because this is technically a legitimate file and sees use in environments with AutoIT scripts, simply blocking this file is not feasible for most organizations. Once the compiled AutoIT script is run, the malicious code and legitimate Nirsoft binaries are injected into the legitimate process `attrib.exe`. Then, additional legitimate DLLs are downloaded and dropped to the same directory, and the configuration sections are decoded. For much of 2024 and early 2025, Mispadu made use of clearly separated configuration sections denoted by the string `"l4riss4"`. Before being filled with data, the sections looked like the following:

```
l4riss4*#ip*##wp1*##wp2*##wp3*#udx1397*mtxgay*
```

```
@#ip2*##wp20*##ip3*##wp30*##bk2*##bk3*
```

After being filled out with data, those same sections appeared as the following:

```
l4riss4*140[.]82[.]18[.]85*9711***udx1397*mtxgay*
```

```
*@140[.]82[.]18[.]85*9722*140[.]82[.]18[.]85*9733*,4,5,13,43,44,58,,*,*
```

Over time, these configuration sections have become less common, and the threat actors behind Mispadu have taken steps to further obfuscate their stored C2s and directives. Although the string `"l4riss4"` remains in memory in current versions of Mispadu, the large sections with 60+ dynamic DNS domain name C2s in plain text, which used to be visible in older versions of Mispadu have now largely disappeared.

When Mispadu has been in place on an infected computer for long enough and the computer meets some basic criteria such as language and location, Mispadu will begin self-propagating by emailing templates it has received from its C2. The templates are complete with links to download new versions of the files that deliver the malware. An HTML rendering of one of the templates used is shown below in Figure 2.

Descarga Factura

COFENSE

Estimado/a Cliente,[-LN-]
Hoy [-data-]

Tenemos el placer de informarte que tu factura ya está disponible en formato PDF y XML. Por favor, utiliza el botón de abajo para descargarla de forma segura.

Tienes hasta **[-data2-]**, para el reconocimiento de cargo que se te gener..., **(GFAC-[-randomstring-])** por la cantidad de **\$[-valor-]** Pesos.

Agradecemos tu confianza y preferencia. Quedamos a tu disposici...n para cualquier consulta.

[Descargar Factura](#)

Data del archivo: **[-data-]**
Factura: **FAC-[-randomnumber-]**

Figure 2: Rendered HTML template email used by Mispadu to self-propagate.