# Mispadu: Advertisement for a discounted Unhappy Meal

welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

November 19, 2019


Another in our occasional series demystifying Latin American banking trojans

ESET Research
19 Nov 2019 - 11:30AM

Another in our occasional series demystifying Latin American banking trojans

In this installment of our blog series, we will focus on Mispadu, an ambitious Latin American banking trojan that utilizes McDonald's malvertising and extends its attack surface to web browsers.

We believe this malware family is targeting the general public. Its main goals are monetary and credential theft. In Brazil, we have seen it distributing a malicious Google Chrome extension that attempts to steal credit card data and online banking data, and that compromises the Boleto payment system.

## Characteristics

Mispadu is a malware family, identified during our research of Latin American banking trojans, that targets Brazil and Mexico. It is written in Delphi and attacks its victims using the same method as the families described earlier in this series: by displaying fake pop-up windows and trying to persuade the potential victims to divulge sensitive information.

For its backdoor functionality, Mispadu can take screenshots, simulate mouse and keyboard actions, and capture keystrokes. It can update itself via a Visual Basic Script (VBS) file that it downloads and executes.

As with the other Latin American banking trojans, Mispadu also collects information about its victims, namely:

- OS version
- computer name
- language ID
- whether Diebold Warsaw GAS Tecnologia (an application, popular in Brazil, to protect access to online banking) is installed
- list of installed common Latin American banking applications
- list of installed security products

As in the cases of Amavaldo and Casbaneiro, Mispadu can also be identified by its use of a unique, custom cryptographic algorithm to obfuscate the strings in its code. This is used in all components, as well as to protect its configuration files and C&C communications. Figure 1 illustrates the core code implementing this algorithm, and Figure 2 pseudocode for the algorithm.

```
loc_217A440:
mov     eax, [ebp+encryptedStr]
movzx   eax, word ptr [eax]
sub     eax, 41h ; 'A'
lea     esi, [eax+eax*4]
lea     esi, [esi+esi*4]
mov     eax, [ebp+encryptedStr]
movzx   eax, word ptr [eax+2]
sub     eax, 41h ; 'A'
add     esi, eax
sub     esi, [ebp+seed]
sub     esi, [ebp+key]
test    esi, esi
jz      short loc_217A479
```

*Figure 1. Core of Mispadu's algorithm for data decryption*

```
1  def decrypt_string(data_enc, key):
2  seed = data_enc[0] - 0x41 # 'A'
3  data_dec = str()
4  for i in range(1, len(data_enc), 2):
5  b1 = (data_enc[i] - 0x41) * 25
6  b2 = data_enc[i+1] - 0x41 - seed - key
7  data_dec += chr(b1 + b2)
8  return data_dec
```

*Figure 2. Pseudocode of Mispadu's algorithm for data decryption*

The banking trojan executable comes with four potentially unwanted applications stored in its resource section. These applications are all otherwise legitimate files from Nirsoft, but have been patched to run from the command line with no GUI. They are used by the malware to extract stored credentials from:

- browsers (Google Chrome, Mozilla Firefox, Internet Explorer), and
- email clients (Microsoft Outlook, Mozilla Thunderbird, and Windows Live Mail, among others).

Mispadu also monitors the content of the clipboard and tries to replace potential bitcoin wallets with its own, as Casbaneiro did. However, from examining the attacker's wallet (see Figure 3), it has not been very successful to date.

| **Summary** | |
|---|---|
| Address | 3QWffRcMw6mmwv4dCyYZsXYFq7Le9jpuWc |
| Hash 160 | fa55d2168e3e4e92b71a16f87182622088ae0fb2 |
| **Transactions** | |
| No. Transactions | 3 |
| Total Received | 0.00170508 BTC |
| Final Balance | 0.00032707 BTC |



*Figure 3. Bitcoin wallet used by the Mispadu operator*

## Distribution

Mispadu employs two distribution methods: spam (see Figure 4) and malvertising. While the former method is very common for Latin American banking trojans, the latter is not, so let's look at it more closely. Figure 5 shows how the Mispadu attack unfolds.


*Figure 4. Examples of spam emails distributing Mispadu. The one targeting Brazil (left) claims the recipient has been absent for three package delivery attempts and should follow the URL to get a refund. The one targeting Mexico (right) urges the recipient to download an invoice to avoid account "blockage".*

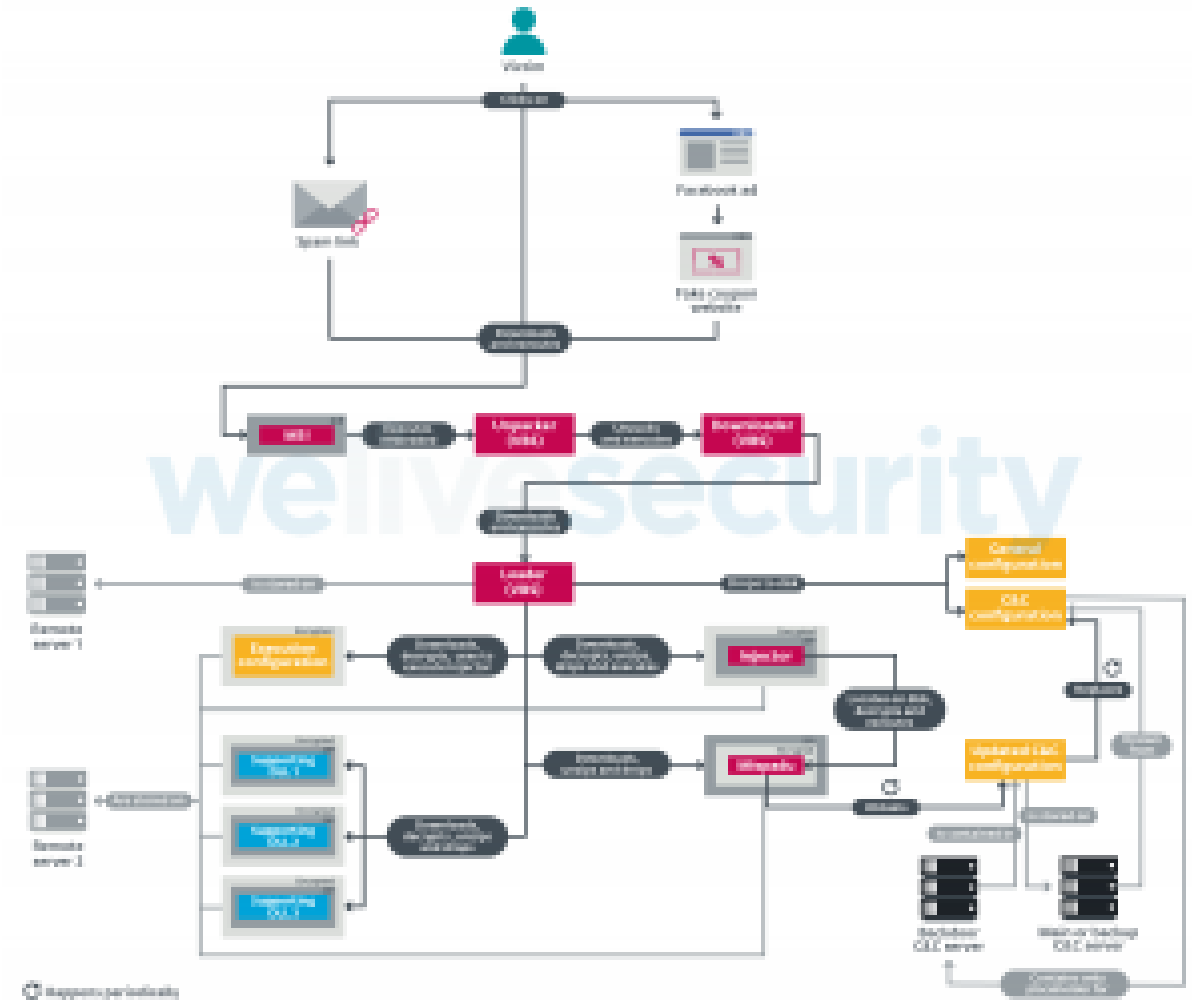

*Figure 5. Mispadu's distribution and execution chain*

The threat actor placed sponsored advertisements (see Figure 6 for a Brazilian example) on Facebook offering fake discount coupons for McDonald's. Clicking the advertisements leads the potential victim to one of the webpages shown in Figure 7. Regardless of a visitor's OS, clicking the button there leads to downloading a ZIP archive containing an MSI installer. Occasionally, this archive also contains legitimate software such as Mozilla Firefox or PuTTY, but they are mere decoys and are not used at all.

Mispadu operators compiled two different versions of the banking trojan based on the country it attacks. Besides that, they decided to use different installers and subsequent stages for each attacked country. However, the logic of both chains is the same and we describe that general form below.

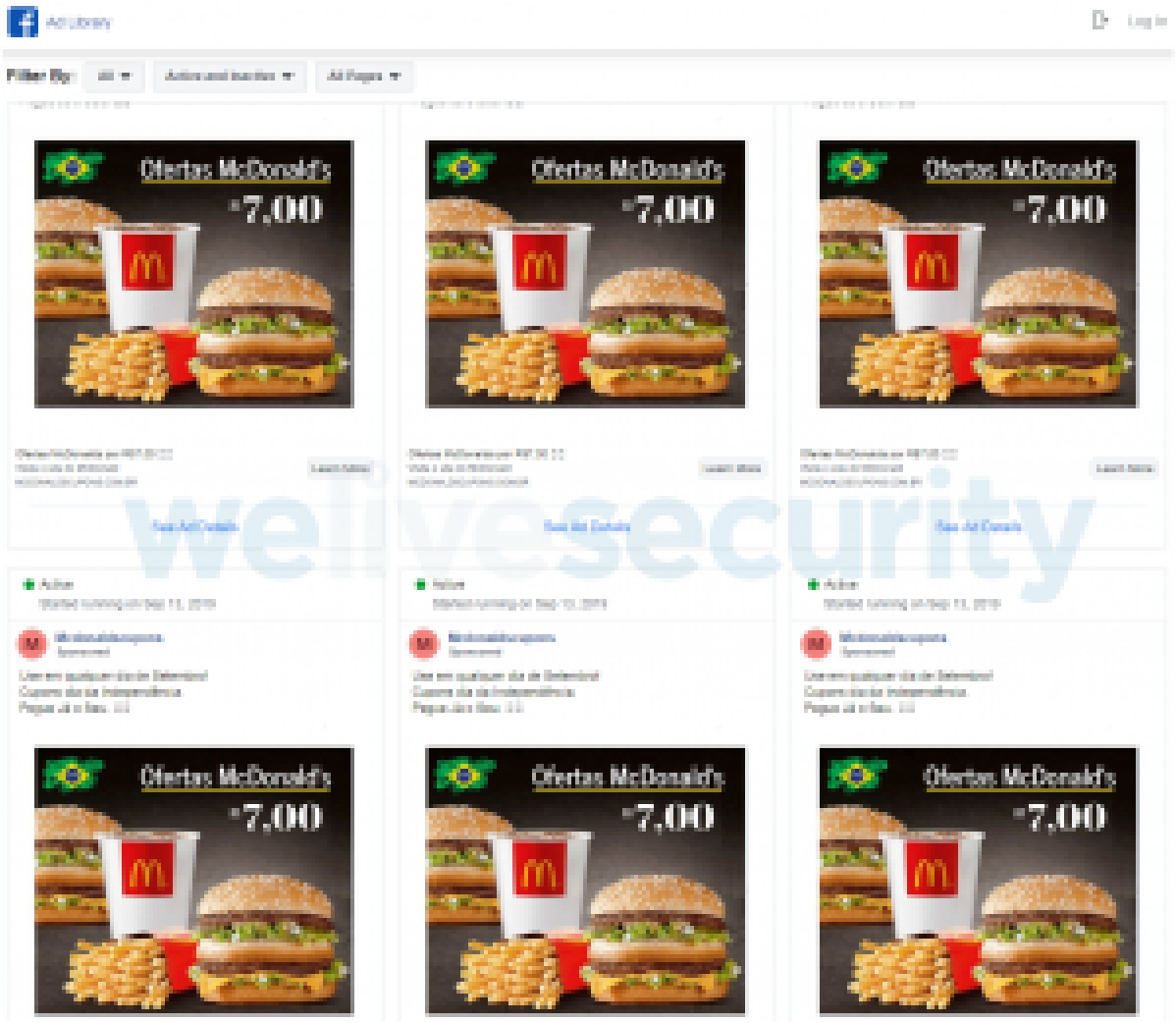


*Figure 6. Facebook ads set up by the Mispadu operators leading to fake McDonald's coupon websites (translation of the ad title: "Use them on any September day! Independence coupons. Get yours now")*

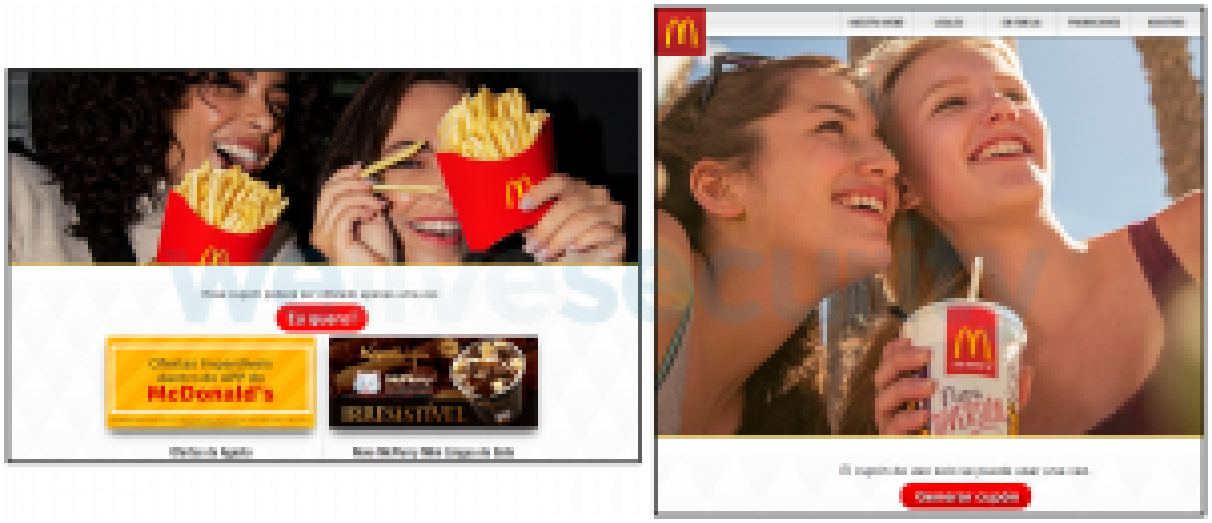


*Figure 7. Malicious webpages offering fake discount coupons for McDonald's Brazil (left) and Mexico (right) (translation of the main text of both: "This coupon can be used only once. I want! / Generate coupon")*

When the potential victim executes the MSI installer, a chain of three subsequent VBS scripts follows. The first script (*unpacker*) decrypts and executes the second script (*downloader*) from its internal data, as seen in Figure 8. The *downloader* script retrieves the third script (*loader*) and executes it (see Figure 9).

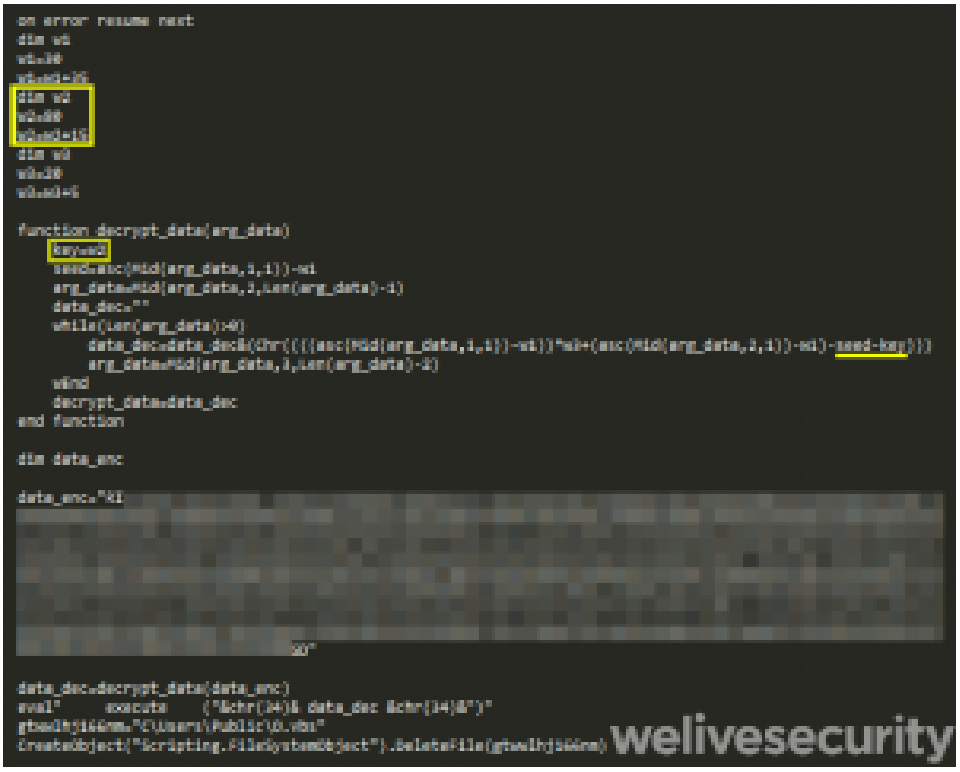


*Figure 8. Mispadu distribution chain unpacker script (stage 1). Notice the key is calculated in variable w2 to the value 95.*


*Figure 9. Mispadu distribution chain downloader script (stage 2). Notice the hardcoded key is the same as in the previous stage.*

The *loader* script is more complicated than the first two stages. It is locale-specific; it checks the language identifier of the potential victim machine to verify it really comes from the country targeted by the current campaign (Brazil or Mexico, respectively). It can detect some virtual environments as well; if a virtual environment is detected or the desired locale is not found, the *loader* quits.

Otherwise, the *loader* script continues by setting up configuration files (described in detail later) and downloading (i) a Mispadu banking trojan, (ii) an injector (DLL) used to execute it and (iii) legitimate support DLLs. Each file is downloaded in a separate ZIP archive as illustrated in Figure 5. We provide pseudocode for the decryption algorithm in Figure 10.

```
1  def decrypt_payload(data_enc):
2  key = data_enc[0]
3  data_dec = str()
4  for i in range(1, len(data_enc)):
5  data_dec += chr(data_enc[i] - ((key + i - 1) % 10))
6  return data_dec
```

*Figure 10. Pseudocode of Mispadu's payload decryption algorithm*

Mispadu's download servers check the validity of requests they receive. Sending an invalid request results in an obscene image response we cannot reproduce here.

Finally, the *loader* script sets up persistence by creating a link in the startup folder and executing the injector. This is done via rundll32.exe by calling an exported function of the injector DLL whose name comes from one of the previously set up configuration files. The injector locates the encrypted banking trojan, then decrypts and executes it.

We found an open directory on one of the servers Mispadu uses, and files connected to a very similar campaign were stored there. Those files can be used to set up a webpage imitating AreaVIP (a tabloid website in Brazil) and to force a fake Adobe Flash Player update on its potential victims. We have not observed that campaign in the wild and believe it may be a setup for the future.

Since the Mispadu campaign targeting Brazil used the Tiny.CC URL shortener, we were able to gather statistics. As seen in Figure 11, this campaign produced almost 100,000 clicks, exclusively from Brazil. The clicks originating from Android are most likely the result of the fact that the advertisement is shown on Facebook regardless of the user's device. You can also see that the campaign is recurring – one phase ended in the second half of September 2019 and emerged again at the beginning of October 2019.

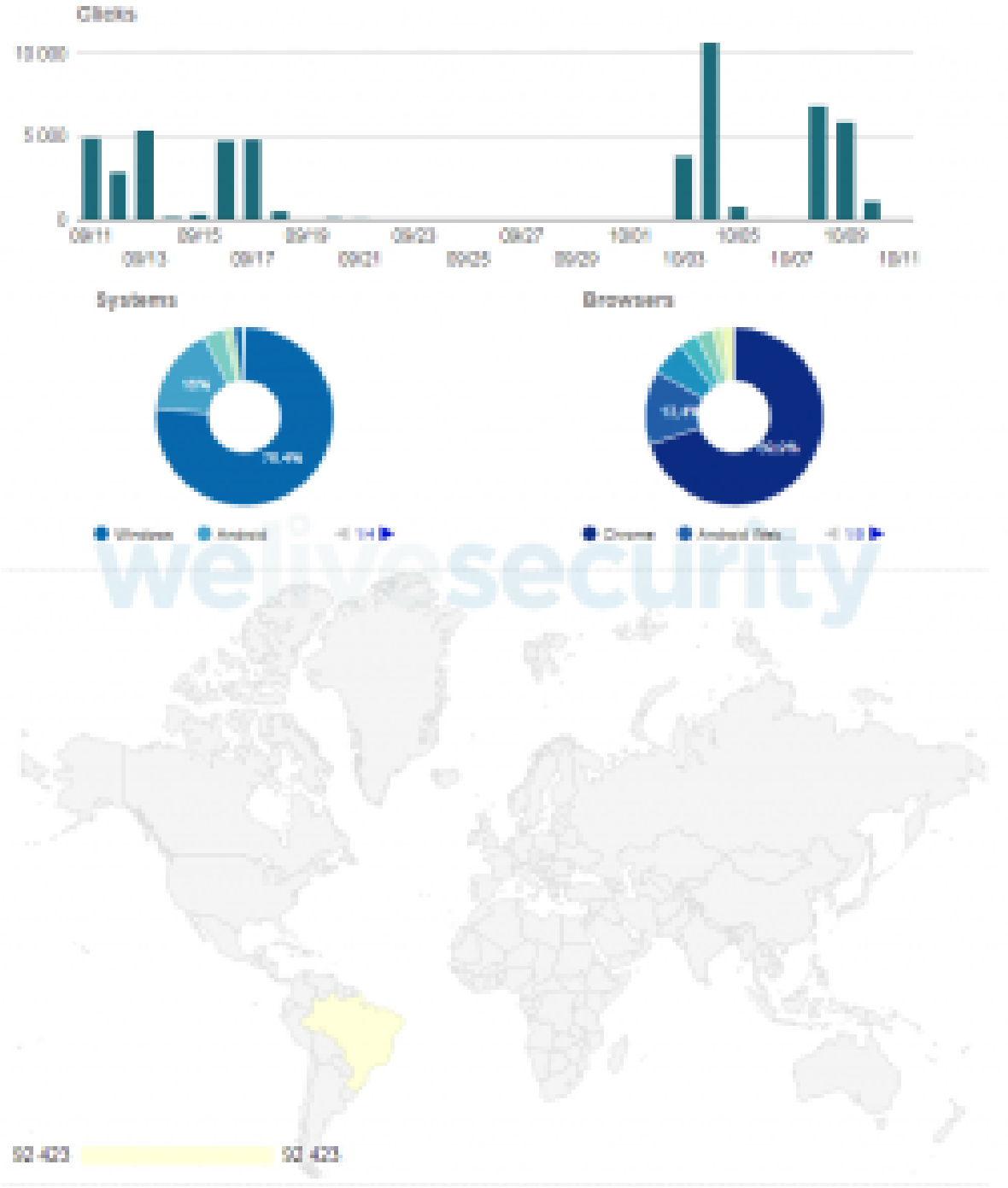


*Figure 11. Brazilian Mispadu campaign statistics*

## Sharing an email attachment

Both spam emails and the fake McDonald's website are interesting in one more aspect: from where the fake coupon is downloaded. Mispadu's operators abused the Russian Yandex.Mail platform to store their payload (see Figure 12). The most probable scenario is that the operators created an account on Yandex.Mail, sent an email with the malicious coupon as an attachment to themselves and then pointed the potential victim to a direct link to this attachment.


*Figure 12. The URL from which the archive containing the malicious Mispadu MSI installer is downloaded*

## Configuration

The use of configuration files is quite uncommon among Latin American banking trojans; yet, overall, Mispadu utilizes three different ones and it cannot function without them. All of the configuration files are either contained in, or obtained by, the *loader* script described earlier.

Mispadu's execution configuration is stored solely in memory with data downloaded from one of its download servers (Remote server 1 in Figure 5). It contains three crucial pieces of information:

- a string necessary to create the URL to download the injector
- the name of the folder where the malware will be installed
- the name of the injector's exported function to be called in order for it to execute the banking trojan

General configuration data are dropped to C:\Users\Public\%COMPUTERNAME%[1], being named as the second letter in the victim's computer name (so for a computer named "JOHN-PC", the file would be named "O"). It is created from data contained in the *loader* script and in the execution configuration file and contains the version information, cryptographic key and file system paths.

C&C configuration data are stored to a file in the same location as the previous one under the same filename with "_" appended ("O_", to continue the previous example). It consists of:

- #ip# (a placeholder for an IP address the banking trojan uses to receive backdoor commands)
- #wp[1-3]# (placeholders for 3 ports associated with #ip#)
- two lists of 31 domains each (main list and backup list)

Mispadu chooses its main and backup C&C domains from these lists based on the current day of the month. It then tries to obtain an updated version of the C&C configuration file from that domain every few hours and replaces the dropped one with it. We believe the main idea behind this approach is to fill in the placeholders in order to activate the backdoor functionality.

## Protect your Chrome

It's a good idea, just don't do it with the malicious Google Chrome browser extension we have observed being distributed together with the Mispadu banking trojan in Brazil (see Figure 13). The extension (see Figure 14 is named "Securty [*sic*] System 1.0" and claims to help you "Protege seu Chrome" (translation: "Protect your Chrome"). It consists of three malicious JavaScript files that we describe below.

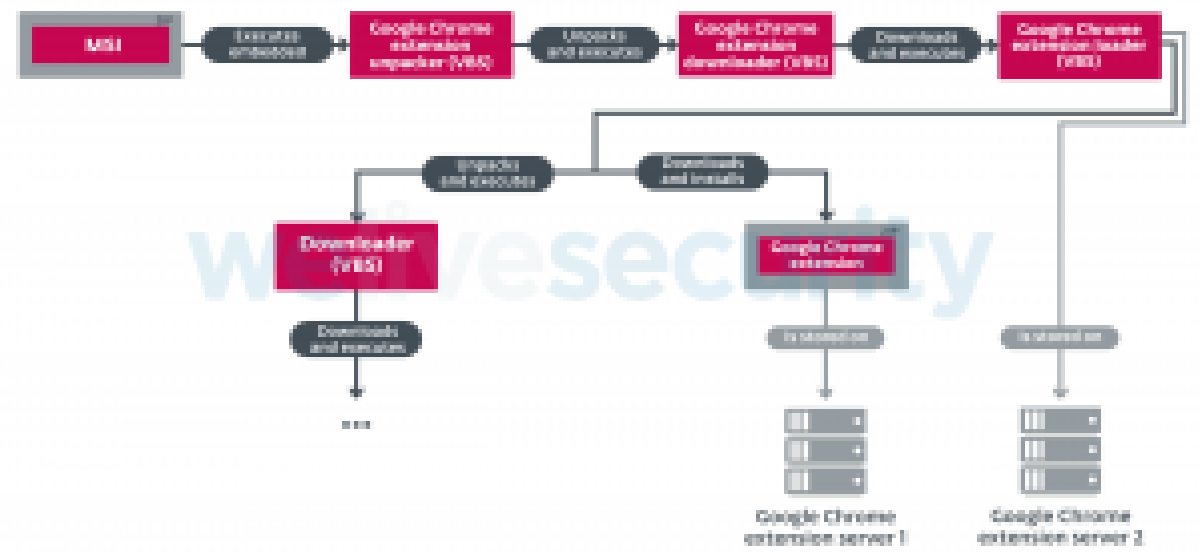

*Figure 13. Part of Mispadu's distribution chain that changes when the malicious Google Chrome extension is distributed as well. The rest of the distribution chain remains the same.*

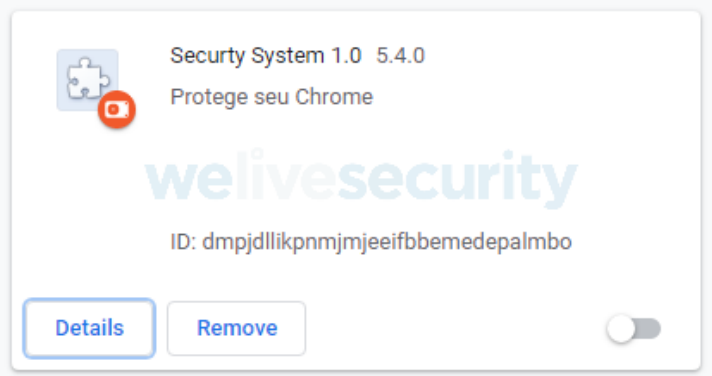


*Figure 14. The malicious Google Chrome extension installed by Mispadu*

## Component 1: Manipulating windows

This simple component has only a single functionality: it creates a new Google Chrome window and closes all others. This component was not present in all samples we analyzed and we believe it is still in the testing phase.

## Component 2: Stealing credit card data

The second component contains a hardcoded list of websites. In pages served from these sites, it looks for any input field containing "text", "email", "tel", "number", "password" or "radio". If "CVV", "CÓD SEG" or their variants are found anywhere on the website, the content of those input fields is sent to the attacker when the victim submits the information. This clearly reveals the intention of this part of the extension – theft of credit card data.

## Component 3: Stealing banking and Boleto data

The third component is the most advanced one. First, using a DGS-like algorithm, it generates two strings based on current day of month and month number. Those strings are then used to form a GitHub URL in the form of https://raw.githubusercontent.com/%FIRST_STRING%/w/master/%SECOND_STRING%, where %FIRST_STRING% is a GitHub username. Data downloaded from the generated URL are decrypted into a different URL we will call *payload URL*.

This component also contains a hardcoded list of targeted websites, as the previous one did. If the victim visits one of these websites, a malicious JavaScript file specific to that website is obtained from the *payload URL* and dynamically loaded via JavaScript's eval function.

Besides that, this component also attempts to compromise the use of Boleto, a popular payment system common in Brazil. The system has been an attractive target for attackers for a long time (you can read more in this paper from 2014). To pay using this system, you have to print a ticket (boleto). That contains mainly an ID number specific to the bank account that should receive the payment, and a barcode (see Figure 15). Payment is then done by either scanning the barcode or typing the ID number manually.

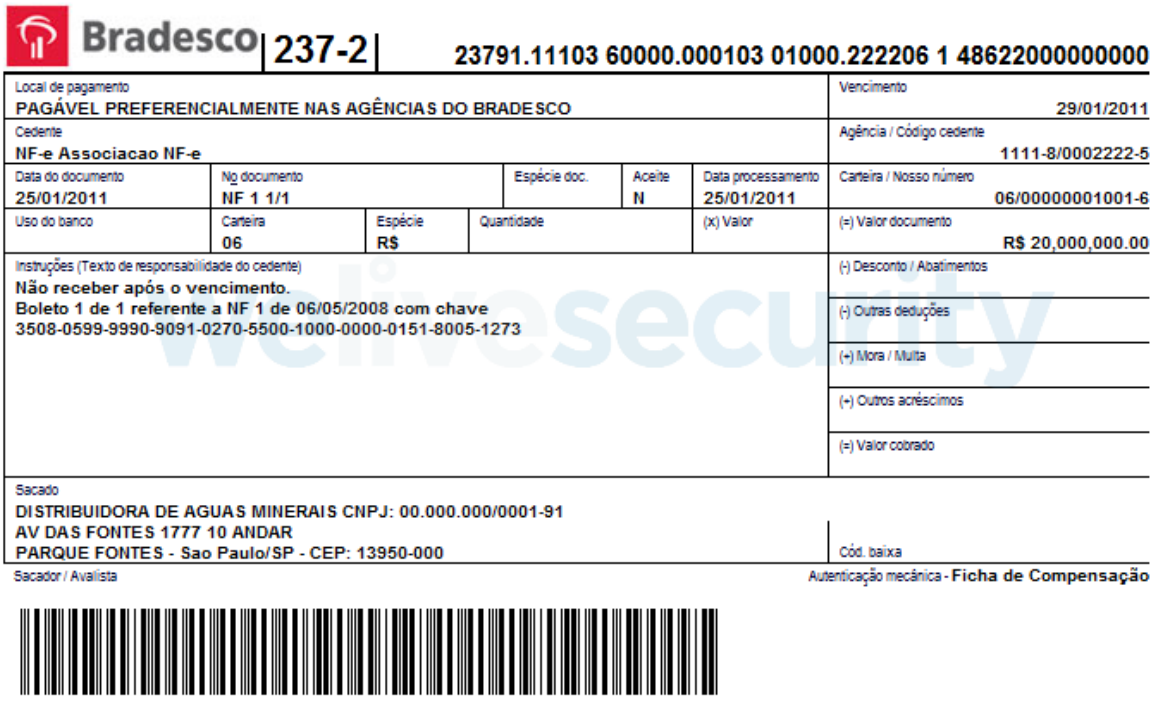


*Figure 15. An example of a boleto (source: Wikipedia)*

Using a regular expression, the malware component tries to find the ID number and replace it with the attacker's (obtained dynamically). Additionally, it abuses a legitimate website to generate the payment barcode using the attacker's account number and replaces the legitimate one with that. The part of the code responsible for compromising Boleto is shown in Figure 16.

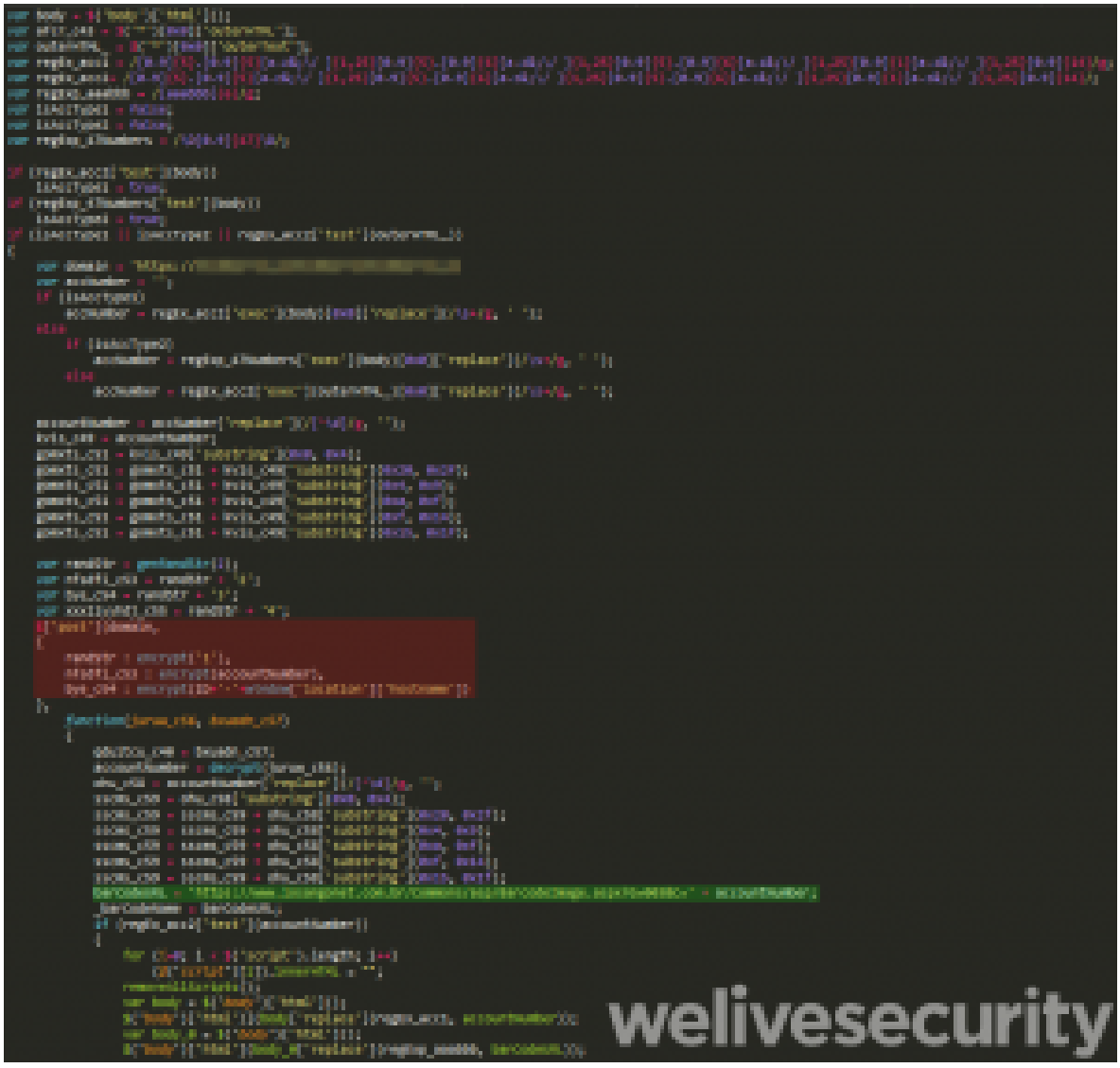

*Figure 16. Mispadu's Google Chrome extension that compromises Boleto. Code obtaining the attacker's account number is marked in red, malicious barcode generation in green.*

## Differences between campaigns

Besides the already mentioned differences and the obvious fact that each variant of the Mispadu banking trojan targets a different set of banks dependent on country of residence, the Brazilian campaign differs from the Mexican one in several other minor aspects.

It seems to randomize the file system paths and filenames where configuration files are stored and the banking trojan is installed for each victim. Additionally, the *loader* script contains a part that is not used at the time of writing but that is ready to abuse Windows mshta.exe to execute the actual banking trojan instead of rundll.exe.

## Conclusion

In this blog post, we have talked about Mispadu, another Latin American banking trojan family isolated during our research. We have shown its main characteristics including reasons why we consider it a Latin American banking trojan – it is written in Delphi, targets Brazil and Mexico, uses pop-up windows and contains backdoor functionality.

We have described its most recent distribution chain and focused on some interesting aspects like Yandex.Mail being abused to store the malicious payloads and the usage of malicious Facebook ads. We have analyzed the configuration files used by Mispadu as well.

Finally, we have talked about a malicious Google Chrome extension that we have seen Mispadu distributing in Brazil. This extension's goal is to steal credit card information, sensitive banking information and attempt to steal money from its victims by compromising the Boleto payment system in Brazil.

*For any inquiries, contact us at threatintel@eset.com. Indicators of Compromise can also be found in our GitHub repository.*

## Indicators of Compromise (IoCs)

### Hashes

#### Brazilian campaign

| SHA-1 | Description | ESET detection name |
|---|---|---|
| A4EDA0DD2C33A644FEEF170F5C24CF7595C19017 | MSI installer | VBS/TrojanDownloader.Agent.RVY |
| A9BADCBF3BD5C22EEB6FAF7DB8FC0A24CF18D121 | Mispadu injector | Win32/Injector.EHXF |
| 337892E76F3B2DF0CA851CCF4479E56EAF2DB8FD | Mispadu banking trojan (PE compilation timestamp 8 Sep, 2019) | Win32/Spy.Mispadu.C |
| A8CD12CC0BBD06F14AA136EA5A9A2E299E450B18 | Mispadu banking trojan (PE compilation timestamp 2 Oct, 2019) | Win32/Spy.Mispadu.C |

#### Mexican campaign

| SHA-1 | Description | ESET detection name |
|---|---|---|
| CFE21DBFB97C2E93F099D351DE54099A3FC0C98B | MSI installer | VBS/TrojanDownloader.Agent.RVY |
| 251AC7386D1B376FB1CB0E02BDFC45472387C7BC | Mispadu injector | Win32/Injector.EHXF |
| A4FC4162162A02CE6FEADFE07B22465686A0EC39 | Mispadu banking trojan (PE compilation timestamp 10 Sep, 2019) | Win32/Spy.Mispadu.J |

| SHA-1 | Description | ESET detection name |
|---|---|---|
| 710A20230B9774B3D725539385D714B2F80A5599 | Mispadu banking trojan (PE compilation timestamp 11 Sep, 2019) | Win32/Spy.Mispadu.J |

**Google Chrome extension**

| SHA-1 | Description | ESET detection name |
|---|---|---|
| 3486F6F21034A33C5425A398839DE80AC88FECA8 | Component 1 (manipulating windows) | JS/Spy.Banker.DQ |
| 1D19191FB2E9DED396B6352CBF5A6746193D05E8 | Component 2 (credit cards) | JS/Spy.Banker.DQ |
| 22E6EBDFAB7C2B07FF8748AFE264737C8260E81E | Component 3 (banking and Boleto data) | JS/Spy.Banker.DQ |

**Potentially unwanted applications for credential theft**

| SHA-1 | Description | ESET detection name |
|---|---|---|
| 63DCBE2DB9CC14564EB84D5E953F2F9F5C54ACD9 | Email client credential stealer | Win32/PSWTool.MailPassView.E |
| 8B950BF660AA7B5FB619E1F6E665D348BF56C86A | Google Chrome credential stealer | Win32/PSWTool.ChromePass.A |
| F6021380AD6E26038B5629189A7ADA5E0022C313 | Mozilla Firefox credential stealer | Win32/PSWTool.PassFox.F |
| 76F70276EB95FFEC876010211B7198BCBC460646 | Internet Explorer credential stealer | Win32/PSWTool.IEPassView.NAH |

## Filenames

- C:\Users\Public\%COMPUTERNAME%[1]
- C:\Users\Public\%COMPUTERNAME%[1]_
- C:\Users\Public\{winx86,libeay32,ssleay32}.dll (legitimate DLLs downloaded by the *loader* script; partial indicator)

## Servers used

- http://18.219.25[.]133/br/mp1a{1,sq,sl,ss}.aj5

- http://3.19.223[.]147/br/mp1a{1,sq,sl,ss}.aj5
- http://51.75.95[.]179/la8a{1,sq,sl,ss}.ay2

### Discount coupon URLs

- Brazil
  - http://promoscupom[.]cf/
  - http://mcdonalds.promoscupom[.]cf/index3.html
- Mexico
  http://mcdonalds.promoscupom[.]cf/index2.html

### Bitcoin wallet

3QWffRcMw6mmwv4dCyYZsXYFq7Le9jpuWc

## MITRE ATT&CK techniques

| Tactic | ID | Name | Description |
|---|---|---|---|
| Initial Access | T1192 | Spearphishing Link | In Mispadu spam campaigns, the victim is led to the payload by a malicious link. |
| Execution | T1085 | Rundll32 | Mispadu banking trojan is executed by an injector that is run via rundll32.exe. |
| Persistence | T1176 | Browser Extensions | Mispadu variant targeting Brazil utilizes a Google Chrome browser extension. |
| T1060 | Registry Run Keys / Startup Folder | Mispadu ensures persistence by creating a link in the startup folder. | |
| Defense Evasion | T1140 | Deobfuscate/Decode Files or Information | Mispadu uses encoded configuration files. |
| T1036 | Masquerading | Mispadu masquerades as a discount coupon. | |
| T1064 | Scripting | Mispadu utilizes VBS exclusively in its distribution chains. | |
| Credential Access | T1056 | Input Capture | Mispadu may execute a keylogger. Its Google Chrome extension tries to steal various sensitive information via input capturing. |
| T1081 | Credentials in Files | Mispadu uses other tools to extract credentials for email clients and web browsers from files. | |
| T1214 | Credentials in Registry | Mispadu uses other tools to extract credentials for email clients and web browsers from the Windows Registry. | |

| Tactic | ID | Name | Description |
|---|---|---|---|
| Discovery | T1083 | File and Directory Discovery | Mispadu searches for various filesystem paths in order to determine what applications are installed on the victim's machine. |
| T1057 | Process Discovery | Mispadu searches for various process names in order to determine what applications are running on the victim's machine. | |
| T1063 | Security Software Discovery | Mispadu scans the system for installed security software. | |
| T1082 | System Information Discovery | Mispadu extracts the version of the operating system, computer name and language ID. | |
| Collection | T1115 | Clipboard Data | Mispadu captures and replaces bitcoin wallets in the clipboard. |
| T1113 | Screen Capture | Mispadu contains a command to take screenshots. | |
| Command and Control | T1024 | Custom Cryptographic Protocol | Mispadu uses a custom cryptographic protocol to protect its data. |
| Exfiltration | T1041 | Exfiltration Over Command and Control Channel | Mispadu sends the data it collects to its C&C server. |

19 Nov 2019 - 11:30AM



## Newsletter

## Discussion