Mispadu Banking Trojan Resurfaces

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces

Additional insights and analysis by Don Ladores and Raphael Centeno

Recent spam campaigns leading to URSA/Mispadu banking trojan (detected by Trend Micro as TrojanSpy.Win32.MISPADU.THIADBO) have been uncovered, as reported by malware analyst Pedro Tavares in a Twitter post and by Seguranca Informatica in a blog post. Mispadu malware steals credentials from users' systems.

This attack targets systems with Spanish and Portuguese as system languages. It is also likely that they have targets similar to previous Mispadu attacks where users from Mexico, Spain, Portugal, and other nearby regions were targeted. This behavior is in line with past Mispadu schemes, such as the one where spam emails for fake discount coupons were used as bait.

Analysis of the campaigns

For this particular case, Mispadu's entry vector is spam, similar to past campaigns involving the malware. By sending messages that refer to overdue invoices, attackers create a seemingly urgent situation that then persuades receivers to download a .zip file from malicious URLs.

This zip file contains an MSI (Microsoft Installer file) that has a VBScript. This is followed by three layers of obfuscation that, when deobfuscated, reveal the final VBScript file that executes an AutoIT Loader/Injector.

The final VBScript also retrieves data on the operating system version. If the script detects a virtual environment such as the following, the script terminates its execution:

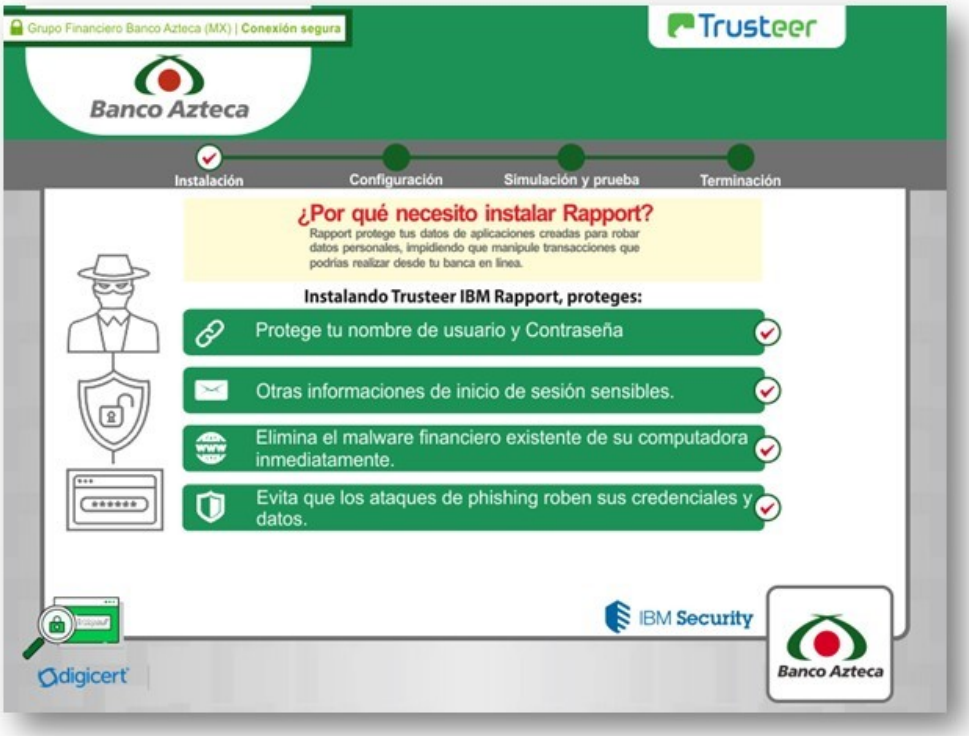
- Hyper-V
- VirtualBox
- VMWare

It also inspects whether the system is using any of the following languages:

Language	Language Code
Spanish – Spain (Traditional)	1034
Portuguese – Brazil	1046
Spanish – Mexico	2058
Portuguese – Portugal	2070
Spanish	58378, 3082

As aforementioned, the attackers are targeting users whose machines are set to use these identified languages. If the system is using a different language ID from those listed, the attack process stops. It also terminates the attack if the computer name is equal to "JOHN-PC."

The final VBScript also loads the AutoIT file, which loads into the memory the final payload: a Delphi file containing the trojan code and processes. The Delphi binary executes a browser banking overlay that steals the victim's data and uses the name and logo of legitimate banks.



Figures 1-2. Fake banking overlays using logos of legitimate banks

The binary also has two legitimate tools, NirSoft's WebBrowserPassView and Mail PassView, which can collect user's data.

Delving deeper into related attacks, we analyzed indicators of compromise (IOCs) shared in a Twitter post by CronUp Red Team and Threat Intelligence Leader Germán Fernández. The tweet shared information such as open-dir logs supposedly used by the malware. Using this information, we were able to analyze related malicious files and dig up some possible exfiltration sites (URLs) from the samples we analyzed. This list is featured in the IOC portion. Behavior-wise, the results of the analysis echo Tavares' findings.

Banking on protection against spam

As institutions directly handling finances, banks are attractive targets for cybercriminals who are after monetary gain. Trojans are one of the tools threat actors use to steal from users of banking systems, and spam is one of the ways that they are propagated.

To avoid compromise brought about by malicious emails, the following steps are recommended:

- Never open links or download attachments from emails from untrusted sources.
- Check if the sender's email address is spoofed.
- Inspect the email for grammatical errors or misspelled words, which are common in spam emails.
- Contact the companies that supposedly sent the emails to verify that the messages came from them.

Here are some recommended security solutions for protecting yourself from spam:

- Trend Micro™ Email Security – protects systems against spam, phishing, Business Email Compromise (BEC), and other email threats.
- Trend Micro™ Deep Discovery™ Email Inspector – has an optimal gateway module that filters inbound messages based on senders, spam and phishing filters, and content.

Indicators of Compromise

URLs

- hxxp://01fckgwxqweod01.ddns.net
- hxxp://01odinxqwefck01.ddns.net
- hxxp://02fckgwxqweod02.ddnsking.com
- hxxp://02odinxqwefck02.ddnsking.com
- hxxp://03fckgwxqweod03.3utilities.com
- hxxp://03odinxqwefck03.3utilities.com
- hxxp://04fckgwxqweod04.bounceme.net
- hxxp://04odinxqwefck04.bounceme.net
- hxxp://05fckgwxqweod05.freedynamicdns.net
- hxxp://05odinxqwefck05.freedynamicdns.net
- hxxp://06fckgwxqweod06.freedynamicdns.org
- hxxp://06odinxqwefck06.freedynamicdns.org
- hxxp://07fckgwxqweod07.gotdns.ch
- hxxp://07odinxqwefck07.gotdns.ch
- hxxp://08fckgwxqweod08.hopto.org
- hxxp://08odinxqwefck08.hopto.org
- hxxp://09fckgwxqweod09.myddns.me
- hxxp://09odinxqwefck09.myddns.me
- hxxp://10fckgwxqweod10.myftp.biz
- hxxp://10odinxqwefck10.myftp.biz
- hxxp://11fckgwxqweod11.myftp.org
- hxxp://11odinxqwefck11.myftp.org
- hxxp://12fckgwxqweod12.ddns.net
- hxxp://12odinxqwefck12.ddns.net
- hxxp://13fckgwxqweod13.ddnsking.com
- hxxp://13odinxqwefck13.ddnsking.com
- hxxp://14fckgwxqweod14.3utilities.com

- hxxp://14odinxqwefck14.3utilities.com
- hxxp://15fckgwxqweod15.bounceme.net
- hxxp://15odinxqwefck15.bounceme.net
- hxxp://16fckgwxqweod16.freedynamicdns.net
- hxxp://16odinxqwefck16.freedynamicdns.net
- hxxp://17fckgwxqweod17.freedynamicdns.org
- hxxp://17odinxqwefck17.freedynamicdns.org
- hxxp://18fckgwxqweod18.gotdns.ch
- hxxp://18odinxqwefck18.gotdns.ch
- hxxp://19fckgwxqweod19.hopto.org
- hxxp://19odinxqwefck19.hopto.org
- hxxp://20fckgwxqweod20.myddns.me
- hxxp://20odinxqwefck20.myddns.me
- hxxp://21fckgwxqweod21.myftp.biz
- hxxp://21odinxqwefck21.myftp.biz
- hxxp://22fckgwxqweod22.myftp.org
- hxxp://22odinxqwefck22.myftp.org
- hxxp://23fckgwxqweod23.ddns.net
- hxxp://23odinxqwefck23.ddns.net
- hxxp://24fckgwxqweod24.ddnsking.com
- hxxp://24odinxqwefck24.ddnsking.com
- hxxp://25fckgwxqweod25.3utilities.com
- hxxp://25odinxqwefck25.3utilities.com
- hxxp://26fckgwxqweod26.bounceme.net
- hxxp://26odinxqwefck26.bounceme.net
- hxxp://27fckgwxqweod27.freedynamicdns.net
- hxxp://27odinxqwefck27.freedynamicdns.net
- hxxp://28fckgwxqweod28.freedynamicdns.org
- hxxp://28odinxqwefck28.freedynamicdns.org
- hxxp://29fckgwxqweod29.gotdns.ch
- hxxp://29odinxqwefck29.gotdns.ch
- hxxp://30fckgwxqweod30.hopto.org
- hxxp://30odinxqwefck30.hopto.org
- hxxp://31fckgwxqweod31.myddns.me
- hxxp://31odinxqwefck31.myddns.me
- hxxp://87.98.137.173/
- hxxp://87.98.137.173/gt21.php
- hxxp://87.98.137.173/k1oa
- hxxp://87.98.137.173/m/k1

SHA-256	Trend Micro Pattern Detection
048afd4276b67b78fdb03714c3bcc766f83407ea4012aa6eae9de5c7cb2d87b8	Trojan.Win32.MISPADOENC.THIADBO
073f9d7bbdca94b3e6f5e572522e8ed17629abf6ef27f0e6a65895a107b52881	Trojan.VBS.MISPADU.THIAHBO
0d57869a4d6509a13ff48af46492f1a8bb2ee33f5c01897e6ccdc4dd29b1cc85	Trojan.AutoIt.MISPADO.THIADBO
1590e809dbad3c77d555e1354125537e80294d0847e7867cc8a9b5893eb2269f	Trojan.VBS.MISPADU.THIADBO
23892054f9494f0ee6f4aa8749ab3ee6ac13741a0455e189596edfcdf96416b3	Trojan.VBS.MISPADU.THIAHBO
2f21d474ca430cab72f924117ace06d8c5b42377a993fe8f6fd4c52733e04575	Trojan.VBS.MISPADU.THIAHBO
400b411a9bffd687c5e74f51d43b7dc92cdb8d5ca9f674456b75a5d37587d342	HKTL_MAILPASSVIEW
58fae847c81a61fe43b12885b9886303e58ad4f96d53393a146999ad4d700c4f	Trojan.VBS.MISPADU.THIADBO

5b91c8acffe1980653718a493e24bde7211ee825ea2947df54c03e9733d61a70	Trojan.VBS.MISPADU.THIAHBO
779e52e5dd7f28a6d51a333f651da4e50ff0aabdd99a4f341159ba76363b4c10	Trojan.VBS.MISPADU.THIADBO
93488eab403fafb3d8e10d38c80f0af745e3fa4cf26228acff24d35a149f6269	Trojan.VBS.MISPADU.THIAHBO
c96b32d44a44cd6f1496f88bc22739b9dd885b56af05ae925fbb57706ad48420	TrojanSpy.Win32.MISPADU.THIADBO
d1fb8a5061fc40291cc02cec0f1c2d13168b17d22ffcabea62816e14ed58e925	Trojan.Win32.MISPADO.THENC
de7168cd978a33926ea7ffad027cc151aa1ea2d2f2581da3ce4fe22bad25c904	Trojan.Win32.MISPADU.THIADBO
f999357a17e672e87fbed66d14ba2bebd6fb04e058a1aae0f0fdc49a797f58fe	HackTool.Win32.NirsoftPT.SM
fb91bdd5ee38a3e163231fa78fd85e2da890e4e116ac530f2b4879e0e50a76a5	HackTool.Win32.NirsoftPT.SM
fe8c60df1fbc9c983ae135829980874e6d793631684d40f93d2321b6d687cff6	Trojan.VBS.MISPADU.THIAHBO

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats