Vawtrak and UrlZone Banking Trojans Target Japan

proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan

February 5, 2016

Blog
Threat Insight
Vawtrak and UrlZone Banking Trojans Target Japan

February 05, 2016 Proofpoint Staff

Overview

In January and February 2016, Proofpoint researchers observed threat actors spreading banking Trojans in Japan and other countries that had not recently experienced high volumes of this family of malware. These countries certainly have not been targeted previously in the same way as the UK, United States, and others. Instead, it appears that the new campaigns in Japan (and Spain) are continuations of the trend first observed with Shifu in October 2015. The key takeaways are:

- The UrlZone banking Trojan is spreading via email spam and targeting Japanese and Spanish banks
- The Vawtrak Trojan is spreading using Angler Exploit Kit and targeting Japanese banks
- Both Trojans are using the same dynamic injects system that allows them to manipulate a financial institution’s website content (likely sharing resources or renting from the same third party)
- The injects system appears to be written by a Russian author

UrlZone Banking Trojan Campaigns

On January 21st of this year, Proofpoint researchers observed a large spam campaign consisting of tens of thousands of emails targeting Japanese email accounts. Other researchers have also observed an uptick in UrlZone activity in Japan but there are additional details behind this emerging threat that are worth pointing out.

Emails with the subject “copy 3” from multiple Gmail accounts contained a zipped executables and an empty email body. Proofpoint observation of actors such as those spreading Dridex over the past year shows increasing use of very simple lure techniques like this throughout 2015. The simplicity and lack of apparent ruse does not appear to hinder this technique: it is simple to create, requires no imagination on the part of the actor, needs no localization, and may be sufficient to entice the user to click.

Figure 1: Email lure

The attachment utilized in this campaign is Andromeda. Andromeda is multi-purpose bot, but in this case it is primarily used to download UrlZone. However, as is often the case in malware ecosystems, Andromeda was also observed loading a plethora of additional malware.

- *UrlZone*: a man-in-the-browser banking Trojan that has been around for several years
- *Pushdo Downloader*: aside from adding the infected computer to a spam botnet, the loader also downloaded a Neutrino Bot
- *Neutrino Bot*: a multi-purpose bot capable of stealing passwords, DDoS, loading additional payloads, etc. In this instance, it downloaded Pony for additional stealing.
- *Pony*: primarily used for loading additional malware and stealing passwords and Bitcoin wallets. This instance was used for its stealing capabilities.

It is also worth mentioning that Proofpoint observed a related large related Cryptowall campaign on January 27, 2016. The Cryptowall downloaded the same Neutrino Bot that was present in the UrlZone campaign. Also, on December 11, 2015, we observed an email campaign delivering the same Andromeda botnet found in the UrlZone campaign, but in the December campaign, Andromeda only downloaded Pushdo. The observations suggest that these campaigns are likely connected by shared affiliates and/or spamming partners.

Figure 2: UrlZone and related campaigns

The table below shows the banks (and customers) targeted in the UrlZone campaign.

Bank	County	Targeted Domains
Bankiter	Spain	empresas.bankinter.com
Banco Sabadell	Spain	www.bancsabadell.com ww1.sabadellcam.com ww1.sabadellurquijo.com
Banca Multicanal	Spain	www.ruralvia.com
Sumitomo Mitsui Banking Corporation	Japan	directd?.smbc.co.jp
The Musashino Bank	Japan	ib1.musashinobank.co.jp
The Yamagata Bank	Japan	ib1.yamagatabank.co.jp
Juroku Bank	Japan	bk.juroku.co.jp

Chugoku Bank	Japan	direct.chugin.co.jp
Bank of The Ryukyus	Japan	direct.ryugin.co.jp
Hachijuni Bank	Japan	direct1.82bank.co.jp
The Daishi Bank	Japan	ib.daishi-bank.co.jp
Hokkoku Bank	Japan	ib.hokkokubank.co.jp
Shinkin Bank	Japan	www11.ib.shinkin-ib.jp
The Norinchukin Bank	Japan	*direct.jabank.jp
The Tajima Bank	Japan	*parasol.anser.ne.jp
Resona Bank	Japan	*ib.resonabank.co.jp
The Japan Net Bank	Japan	*login.japannetbank.co.jp
Tsukuba Bank	Japan	ib.tsukubabank.co.jp
The Awa Bank	Japan	ib1.awabank.co.jp
MIYAZAKIBANK	Japan	mib.miyagin.co.jp
The Hiroshima Bank	Japan	direct.ib.hirogin.co.jp

Figure 3: Japanese and Spanish banking sites targeted by this instance of UrlZone

Vawtrak Banking Trojan Campaigns

While our colleagues at Sophos and Trend previously wrote about Vawtrak targeting Japan in 2014 and earlier, there are so far no documented campaigns of the updated Vawtrak Trojan targeting Japan in 2015 or 2016. On February 2, 2016, however, we observed Angler EK delivering Vawtrak ID 28 to Japanese users.

Figure 4: Angler EK delivering Vawtrak payload with Japanese targeting

The table below shows the banks specifically targeted by Vawtrak in the recent campaign:

Bank	County	Targeted Domains
Sumitomo Mitsui Banking Corporation	Japan	directd?.smbc.co.jp
The Musashino Bank	Japan	ib1.musashinobank.co.jp
The Yamagata Bank	Japan	ib1.yamagatabank.co.jp
Juroku Bank	Japan	bk.juroku.co.jp
Chugoku Bank	Japan	direct.chugin.co.jp
Bank of The Ryukyus	Japan	direct.ryugin.co.jp
The Daishi Bank	Japan	ib.daishi-bank.co.jp
Hokkoku Bank	Japan	ib.hokkokubank.co.jp
Hachijuni Bank	Japan	direct1.82bank.co.jp
Tsukuba Bank	Japan	ib.tsukubabank.co.jp
The Awa Bank	Japan	ib1.awabank.co.jp
MIYAZAKIBANK	Japan	ib.miyagin.co.jp
The Hiroshima Bank	Japan	direct.ib.hirogin.co.jp
Shinkin Bank	Japan	www11.ib.shinkin-ib.jp
The Norinchukin Bank	Japan	direct.jabank.jp
Resona Bank	Japan	ib.resonabank.co.jp
The Japan Net Bank	Japan	login.japannetbank.co.jp
The Tajima Bank	Japan	parasol.anser.ne.jp

SBI Sumishin Net Bank	Japan	netbk.co.jp

Figure 5: Japanese banking sites targeted by Vawtrak ID 28

Dynamic Injects Shared by Vawtrak and UrlZone

After extracting the injects code from both Trojans we observed that there is an overlap in the targeted banks. Both banking Trojans are using the same dynamic injects system that allows them to manipulate a financial institution’s website content. This means that the two banking Trojans use the same JavaScript code for stealing login credentials, PINs, one-time-passwords, etc. This could also mean that the responsible actors are sharing resources or renting from the same third party. Additionally, the injects JavaScript code appears to be written by a Russian developer, as observed by code comments such as “Startuem nash interval na proverku statusa”, which translates to “Begin our interval for checking the status”.

Figure 6: Screenshot of part of the inject code

Conclusion

As others have noted, the emergence of banking Trojans in Japan and Spain presents some particular challenges. While organizations in other countries like the UK and the United States have been targets for massive Dridex, Dyre, Vawtrak (and other banking Trojans) campaigns and businesses there have implemented a number of protections, countries with less experience combatting these threats may find themselves vulnerable to considerable losses. Unfortunately, as threat actors saturate targets in many geographies, it's only a matter of time until new geographies begin experiencing the same sorts of volumes and persistence that characterize recent campaigns with Dridex and other malware.

Appendix A : IOCs from campaigns containing UrlZone

Value	Type
1a86cf4fb4dcb0e4e3aad41bc039d8302e0fd6f9fabe203efc77e3aec35e2f66	Andromeda hash
606708C9479E1DF26545D469D3D54A0E268F01AD8AA061F6504968C3B1594A0C	UrlZone hash
757F2C62637765CBC8C7B9F5F63ED4AB00F34485F516A66B2A81B4EDFB731920	Pushdo hash
CE08A35831F6F5777DB6E8FEA9BAC40808917FEC019338BA00285082737611FB	Neutrino Bot hash

E90050D963D376C1F75416EBF9BC6FFA2299046F8ADD1DDE6D67752443587411	Pony hash
1d6d7ea0eeec99da1add9e83f672533eeee900dc817018ee6edbf635bb08cf0a	UrlZone hash
f3b9815ea4a6c603eafadb26efebec21565deec315ee007d59e92f0f656a90bb	UrlZone hash
15896a44319d18f8486561b078146c30a0ce1cd7e6038f6d614324a39dfc6c28	UrlZone hash
[hxxp://huremoke[.]net/get.php]	Andromeda C2
[hxxp://votehad[.]su/paris.php]	Andromeda C2
[hxxp://shardsound[.]net/images.php]	Andromeda C2
[hxxp://kernsmee[.]ru/news.php]	Andromeda C2
[hxxp://masabodhi[.]com/andoluse.php]	Andromeda C2
[hxxps://hwnbv5woeedjffn[.]com]	UrlZone C2
[hxxp://5.45.179[.]179/ajax.php]	Neutrino Bot C2
[hxxp://5.45.179[.]179/p/ajax.php]	Pony C2
[hxxp://www.fondazionelanza[.]it/eng/v3.exe]	Andromeda downloading UrlZone
[hxxp://www.fondazionelanza[.]it/eng/akeyb.exe]	Andromeda downloading Pushdo loader

[hxxp://www.tajjquartet[.]com/ff/serif/payload.exe]	Pushdo loader downloading Neutrino Bot
[hxxp://www.tajjquartet[.]com/ff/serif/ponik.exe]	Neutrino Bot downloading Pony
[hxxps://ifree-online[.]com]	UrlZone Injects C2

Appendix B: IOCs from campaigns containing Vawtrak

Value	Type
9f1de72234dcf77ddf25b69df98058a7f9e633f803ddc2720209bb315ef3a04c	Vawtrak hash
[hxxp://begiekee[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://searalihid[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://zofienie[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://deehiesei[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://keanees[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://peazor[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://xeaberal[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://dietoog[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://mafoovoo[.]com/rss/feed/stream]	Vawtrak C2
[hxxp://geeseazei[.]net/rss/feed/stream]	Vawtrak C2
91.242.163[.]74:8080	Vawtrak C2

[hxxp://5.187.2[.]19/module/272a5ad4a1b97a2ac874d6d3e5fff01d]	Vawtrak downloading module
[hxxp://5.187.2[.]19/module/2f6421d9a99d75c5d153edda3f1fe5e3]	Vawtrak downloading module
[hxxp://5.187.2[.]19/module/9079dae8e107342d8f3747fa74ab8a57]	Vawtrak downloading module
[hxxp://5.187.2[.]19/module/7afb9776a27d97b2f43f8de256448072]	Vawtrak downloading module
[hxxp://5.187.2[.]19/upd/28]	Vawtrak downloading update

Subscribe to the Proofpoint Blog