Panda Banker Zeros in on Japanese Targets

arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/

by ASERT Team on March 27th, 2018

Key Findings

- A threat actor using the well-known banking malware Panda Banker (a.k.a Zeus Panda, PandaBot) has started targeting financial institutions in Japan.
- Based on our data and analysis this is the first time that we have seen Panda Banker injects targeting Japanese organizations.
- It is likely a new campaign or actor started using Panda Banker since in addition to the previously unseen Japanese targeting, Arbor has not seen any indicator of compromise (IOC) overlaps with previous Panda Banker campaigns.
- The sample used in this campaign was the first sample we observed in the wild to use the newest version of Panda Banker, version 2.6.6.

Overview

Panda Banker is based on the Zeus malware family. One of its main functions is stealing user credentials, account numbers, and ultimately money from financial institutions. It does this by using a technique known as "man in the browser" along with "webinjects" that specify what websites to target and how. This banking malware was first seen in the wild in the beginning of 2016 (version 2.1.x) and has had consistent, incremental development since then. While some details have changed, our "Who Let the Pandas Out? Zeus, Zeus, Zeus, Zeus" blog post is still

a good introduction to the technical details of the malware. Panda Banker is sold as a kit on underground forums so there are multiple users of the malware. Cybercrime threat actors tend to focus their campaigns on particular countries—usually dependent on their ability to convert stolen credentials and account details from those locations into real money. Over the years we've seen Panda Banker campaigns focus on financial institutions in: Italy, Canada, Australia, Germany, United States, United Kingdom, and now Japan.

Campaign Analysis

A new version of Panda Banker, version 2.6.6, was observed being distributed in the wild on March 26th:

SHA256: 8db8f6266f6ad9546b2b5386a835baa0cbf5ea5f699f2eb6285ddf401b76ccb7

Compilation date: 2018-03-26 09:54:57 While we didn't see any significant changes to the malware itself (possibly just a "bug fix" release), the campaign using this sample stood out for two reasons:

1. No IOC overlap with any previous Panda Banker campaigns that we've seen.
2. Webinjects targeting Japan, a country we haven't seen targeted by Panda Banker before.

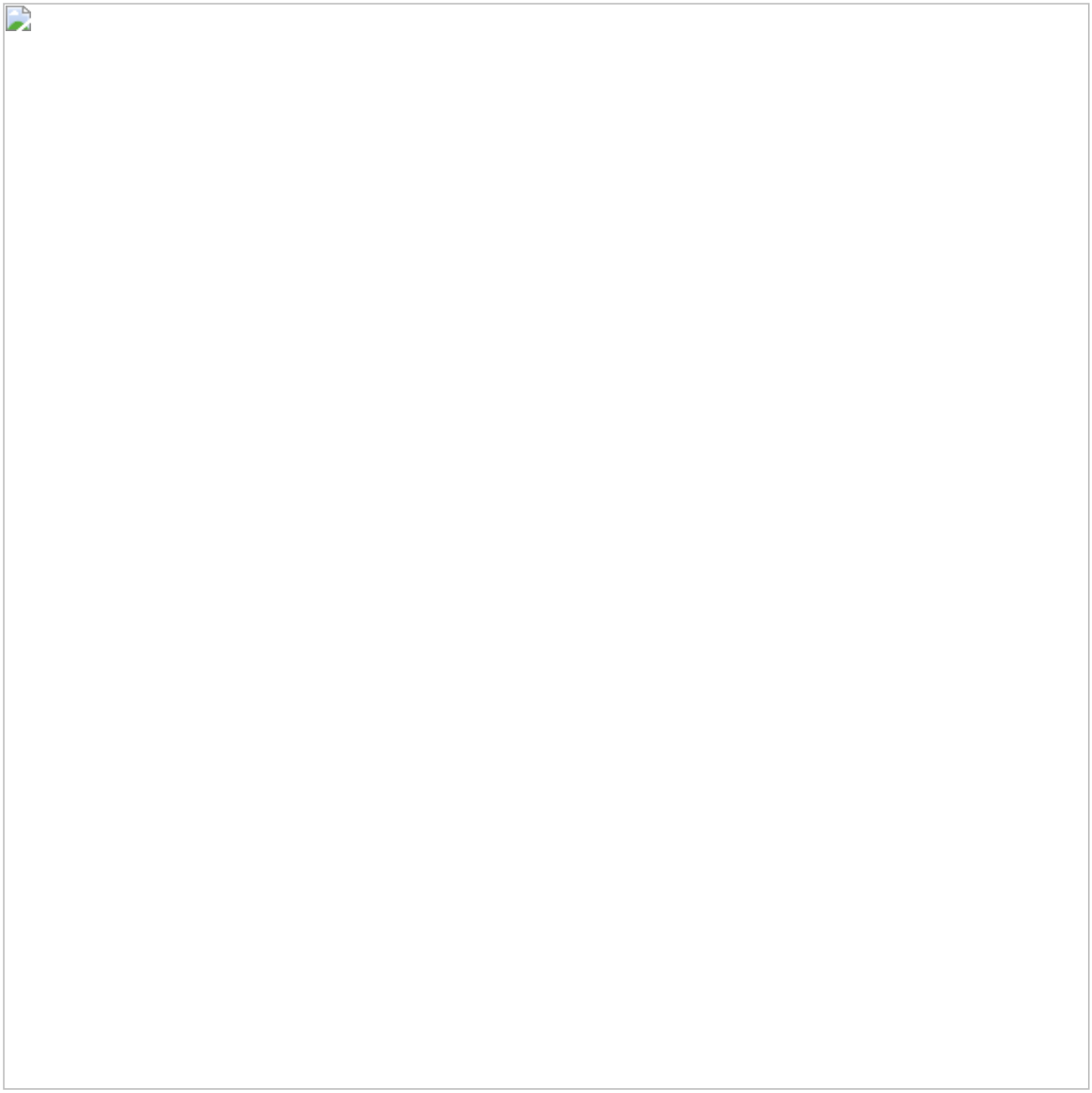
Command & Control (C2) The C2 servers configured for this sample are listed below:

- https://hillaryzell[.]xyz/1wekenauhivwauvaxquor.dat
- https://buscamapa1[.]top/2yrfuupcovylaawubitvy.dat
- https://buscamapa2[.]top/3toaxkatoindyepidikuv.dat
- https://buscamapa3[.]top/4heequktuepahvoyfofit.dat
- https://buscamapa4[.]top/5ufyfegtuobekpykobeul.dat
- https://buscamapa5[.]top/6lubanuoxapywinlaokow.dat

At the time of research, only hillaryzell[.]xyz was operational and it was registered to a "Petrov Vadim" using an email address of "yalapinziw@mail.ru". *Campaign Name* The threat actor named this campaign "ank". *Webinjects* At the time of research, the C2 server returned 27 webinjects that can be broken down into the following categories:

- 17 Japanese banking web sites mostly focusing on credit cards
- 1 US based web email site
- 1 US based video search engine
- 4 US based search engines
- 1 US based online shopping site
- 2 US based social media sites
- 1 US based adult content hub

An example, redacted webinject for this campaign looks like the following: [caption id="attachment_9530" align="aligncenter" width="700"]



Example webinject targeting Japan.[/caption] The webinjects in this campaign make use of a "grabber" / automated transfer system (ATS) system known as "Full Info Grabber" to capture credentials and account information. As can be seen in figures above, the threat actor is using a path of "jpccgrab" possibly meaning "Japanese credit card grabber". Given the targeting, this name makes some sense. *Distribution (update March 28, 2018)* Security researcher kafeine has released more details on how this threat is being distributed in the wild: a malicious advertisement (malvertising) is redirecting victims to a RIG exploit kit which is distributing the Panda Banker malware.

Conclusion

Japan is no stranger to banking malware. Based on recent reports, the country has been plagued by attacks using the Ursnif and Urlzone banking malware. This post was our first analysis of the first Panda Banker campaign that we've seen to target financial institutions in Japan.

Posted In

- Analysis
- Botnets
- Indicators of Compromise
- Interesting Research
- Malware
- threat analysis

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.