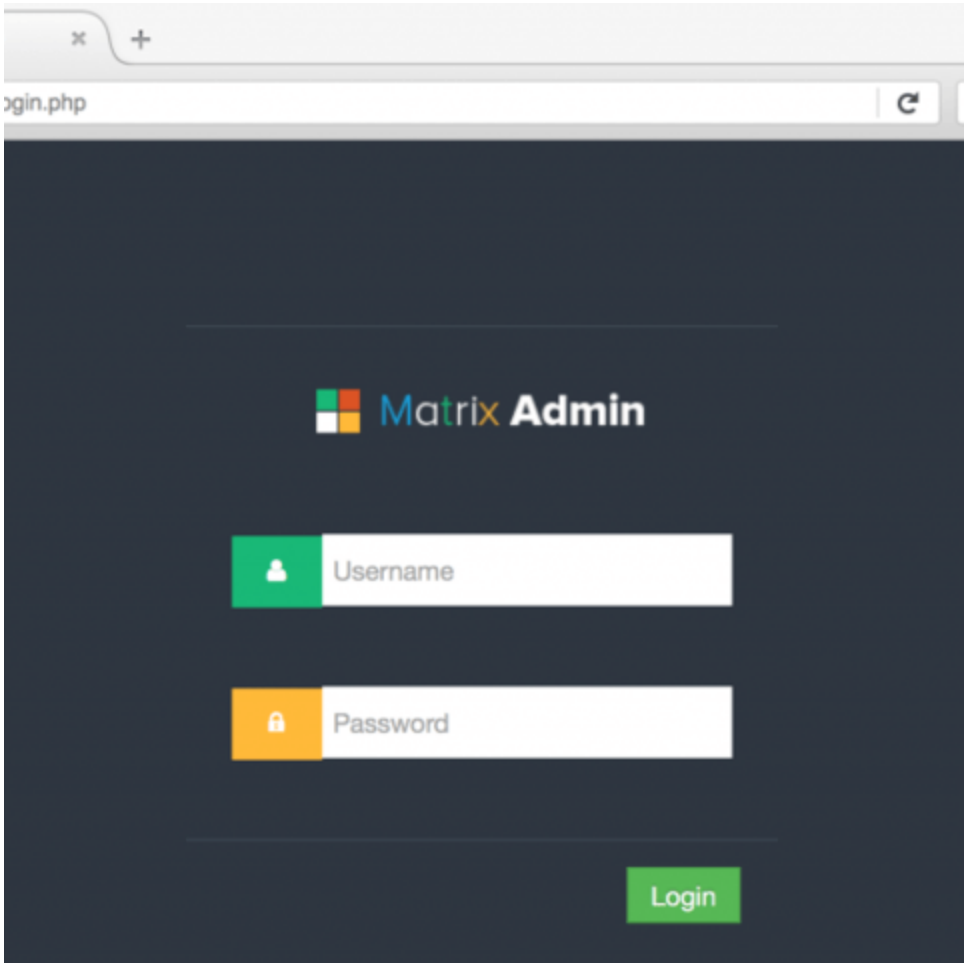
Another Banker Enters the Matrix

arbornetworks.com/blog/asert/another-banker-enters-matrix/



by ASERT Team on June 9th, 2017

This post takes a look at a new banking malware that has, so far, been targeting financial institutions in Latin America—specifically, Mexico and Peru. Initially, we've called it "Matrix Banker" based on its command and control (C2) login panel, but it seems that "Matrix Admin" is a template available for the Bootstrap web framework. Proofpoint calls it "Win32/RediModiUpd" based on a debugging string from an earlier sample.

The malware is under active development, but as with some of the other banking trojans we've analyzed, it's difficult to assess how far and wide this threat will go while it's still so new. Will it become a persistent threat like Panda Banker or have a fate more like Nuclear Bot?

Samples

The sample analyzed for this post is available on VirusTotal. It was compiled on 2017-05-26 and has the following PDB debugging string:

```
C:\Users\W7\Downloads\Project\Bin\Loader.pd
```

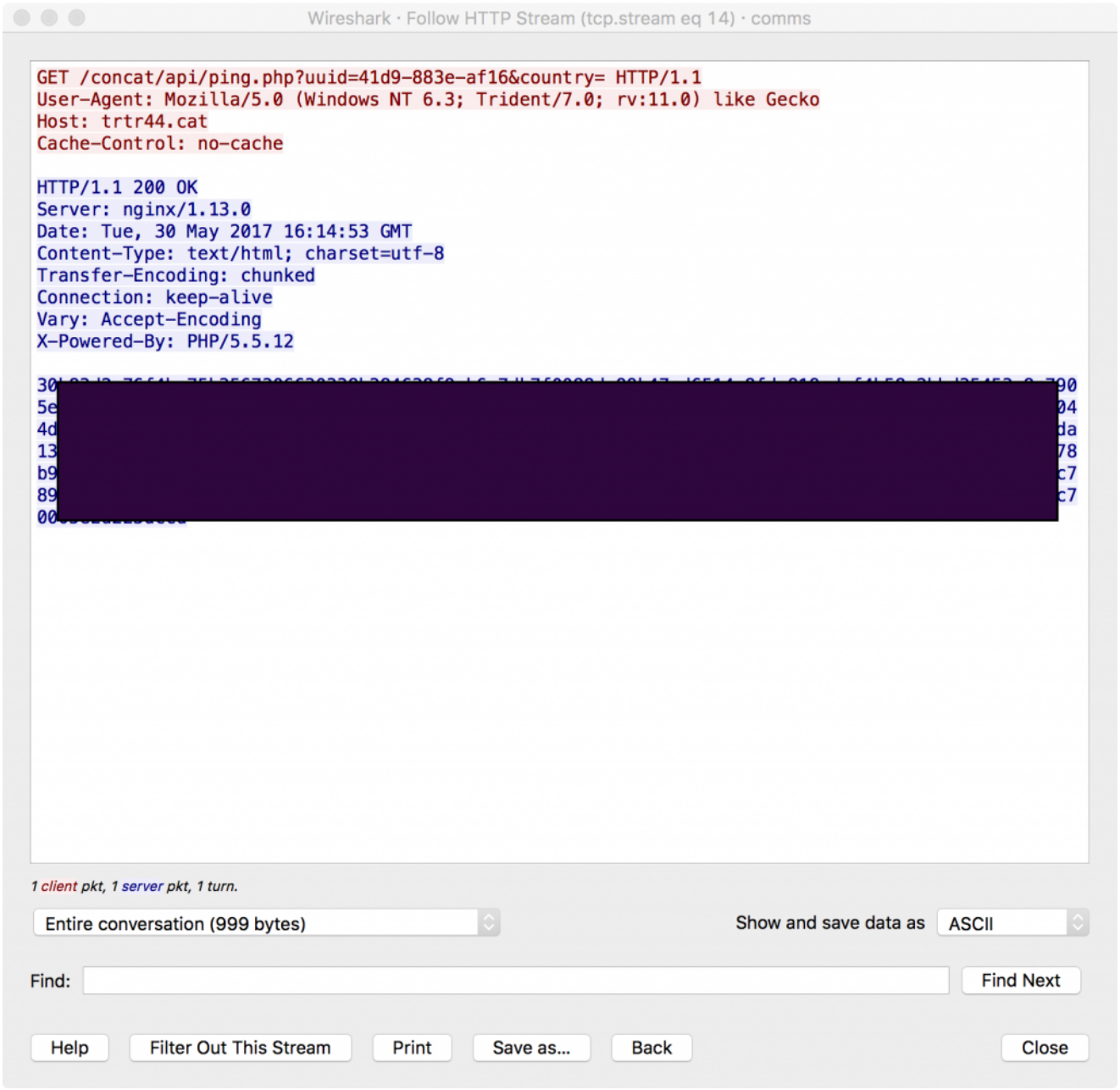
The Matrix Loaded

As suggested by the PDB string, the sample starts off as a loader. It performs the following tasks:

- Creates a “LoaderMutex” mutex
- Sets up Registry Run persistence using “GITSecureService” as the value name.
- Extracts a 32-bit and 64-bit DLL named “main_32.dll / main_64.dll” from a resource named “BINARY”.
- Using the “ReflectiveLoader” technique and code, injects the appropriate DLL into chrome.exe, firefox.exe, iexplore.exe, or microsoftedgecp.exe.

Main DLLOnce the main DLL is injected in a browser, it starts by hooking the appropriate browser functions (e.g. PR_Read and PR_Write for Firefox) to setup a “man-in-the-browser” (MitB).

It then phones home to its C2 server to get the webinject config. The request looks like this:



The URI path and file are hardcoded, but we've seen other paths in other samples. "uuid" is randomly generated and "country" is currently left blank—though there is placeholder code for it.

Responses from the C2 are hex encoded and encrypted using the Salsa20 crypto algorithm. This is the first malware family that we've seen that uses this algorithm. The following Python snippet decrypts the response:

```
import sys# https://pypi.python.org/pypi/salsa20/0.3.0
import salsa20

fp = open(sys.argv[1], "rb")
data = fp.read()
fp.close()

iv = "K\x84\x8eH\xf1]E\xa5"
key =
"\xa1\x9cA\x89\xb4\x9d\x15ae\xf1a\x8bLQj\x16\xf1l\x18\x1d\x81\xb8\x18\x18\xe1\x81e\x1c


data_nohex = data.replace("\n", "").decode("hex")
plain = salsa20.Salsa20_xor(data_nohex, iv, key)
print plain
```

So far the key and initialization vector (IV) have been the same for all the samples we've analyzed. An example webinject config looks like this:

```
rule2:targeturl=*[redacted]*&br&&br&<meta http-equiv="refr
esh" content="0; url=https://[redacted].llinea.com/[redacted]" />&
br&<script>&br&top.location.href="https://[redacted].llinea.com/[redacted]
[redacted]";&br&</script>
```

While functional, the webinject format looks to be under construction. Earlier samples use a different, simpler format and there is plenty of work to do to catch up with the industry standard Zeus webinjects. Rules are "\n" separated and there are two types: "rule1" and "rule2". So far we've only seen "rule2"s. The targeted financial institution is specified in "targeturl". The rest of the pieces, which are "&br&" delimited, are eventually concatenated together and injected into the page if the browser visits a targeted URL.

In this example the code that is injected is a HTML and JavaScript redirect that automatically redirects the browser to a phishing page hosted on "llinea[.]com" that looks exactly like the targeted financial institution. Hoping the victim doesn't notice the redirect, the threat actor will harvest the victim's banking credentials.

Campaign

Per VirusTotal, the analyzed sample was first seen in the wild on 2017-05-29 and being distributed by the following sites:

- hxxp://neext[.]com[.]mx/Loader.exe
- hxxp://notaria94[.]com[.]mx/real.exe

Furthermore we can link the second drop site to an instance of Beta Bot (available on VirusTotal) and see it dropping Matrix Banker. The two malwares also share a common C2 server, trtr44[.]cat.

Conclusion

This post has been a quick analysis of a new banking malware currently targeting countries in Latin America. It is too soon to assess how active and widespread this new family will become, but it is actively being developed and targeting financial institutions in the wild.

Posted In

- Analysis
- Botnets
- Encryption
- Interesting Research
- Malware
- Reverse Engineering
- threat analysis

Subscribe

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