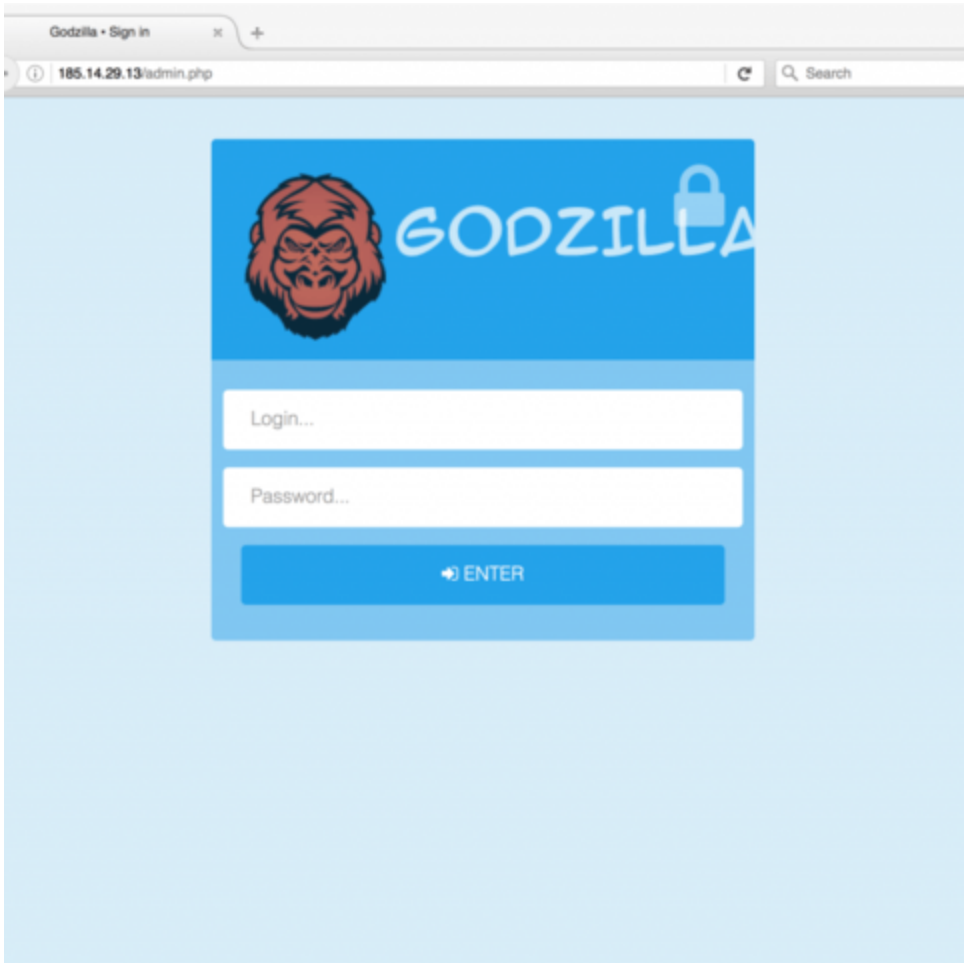
TrickBot Banker Insights

arbornetworks.com/blog/asert/trickbot-banker-insights/



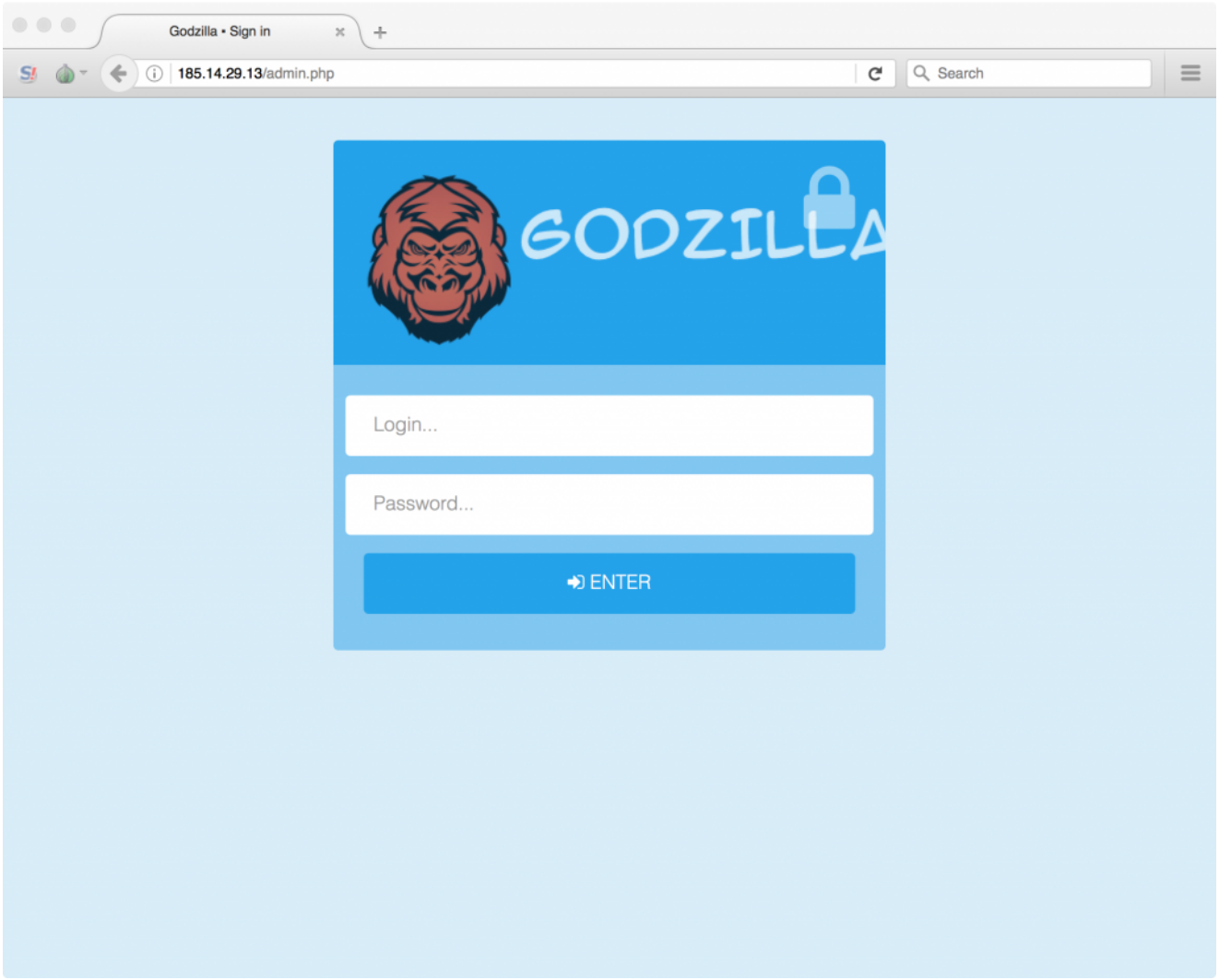
by ASERT Team on October 25th, 2016

A new banking trojan, TrickBot, has seemingly risen from the ashes left behind by the November 2015 takedown of Dyreza/Dyre infrastructure and the arrests of threat actors identified by Russian authorities. Dyreza was used to target customers of over 1000 U.S. and U.K. banks and other companies during the peak of operations. Researchers at Threat Geek and MalwareBytes have already extensively covered general TrickBot functionality.

During ASERT's research, we uncovered a few new peculiarities as yet to be discussed, including links to Godzilla Loader and the ability to download and execute additional malware packages.

First, when analyzing malware sample (all samples listed by MD5 hash) 3a55fd6b3f969b1324a1942af08e039e, we discovered links back to the somewhat new Godzilla Loader.

In this case, Godzilla Loader (fc431f69760c598098f34eec337c8415) was used to install TrickBot from http://185.14.29[.]13/api.php. The login panel for the Command & Control (C2) server appears at the URL admin.php as follows:



Additional research on Virus Total shows this particular instance to be part of a spam campaign. Threat actors laced an email message with a malicious .scr executable that installed Godzilla Loader. The loader was used to subsequently download TrickBot. The message appears as such:

Subject: You have received a new fax

Attach: fax198-203-9153.scr

Interestingly enough, Godzilla Loader was used as the intermediary for both Bolek and Panda Bankers when threat actors first started distributing them. More information on Godzilla Loader functionality can be found here. **T**

rickBot's Download and Execute Command

As referenced in the malware analyses above, TrickBot has a number of commands that use slightly different URLs. For its "download and execute" functionality, TrickBot uses the following path template: /%s/%s/1/%s/ A completed URL looks something like:

hXXps://138[.]201[.]44[.]28/tmt2/ADMIN-PC_W617601.F2F368CFEBB3F08115DB04EE5697EBBC/1/PB1qOLElSsGUg45wH3JyIKEMGzl60MB/

This path can be broken down into the following pieces:

- “gtag” – group tag
- Client ID
- Command number
- 16 to 32 random letters and digits

The response from the C2 server will look similar to:

```
/42/tmt2/ADMIN-
PC_W617601.F2F368CFEBB3F08115DB04EE5697EBBC/PB1qOLE1SsGUg45
wH3JyIKEMGzl60MB/41274/\r\nAAAAABITWmON7YmzLzAcFn2jj0looA8X
xcYfqQte5O1dab81JgAAAGgAdAB0AHAAOgAvAC8AMQA1ADYAMQA2AC4AbQB
lAHIAYQBoAG8AcwB0AC4AcgB1AC8AOAA1ADEAMwAyADEAMwA2ADUALgBiAG
kAbgCT/OBix1v7jD/hi/8w9D3I9LCYf93qh72eEiPovmcQCB8uL8nz4b9Oq
ja3omAf1v5xR8TDnus4djX37duvEaMHhmxqI1rDcG5Dt1IpFG9Is3SitDDF
hRsGsQuoI9Vtw1s=\r\n1234567890
```

The response can be split into three pieces using “\r\n” as a delimiter. The first piece is a “/” delimited header which echoes back a couple of the request pieces along with a few additional items: /42/tmt2/ADMIN-PC_W617601.23BD67ECD8AEDEC8FEAE8253B2C09D03/XbuepYhfjAwVBawBh1PvDHyHKZmB49/41268/ At the end is a trailer which seems to always be “1234567890”. In the middle is base64-encoded data. Decoding this base64 data results in the following type of output:

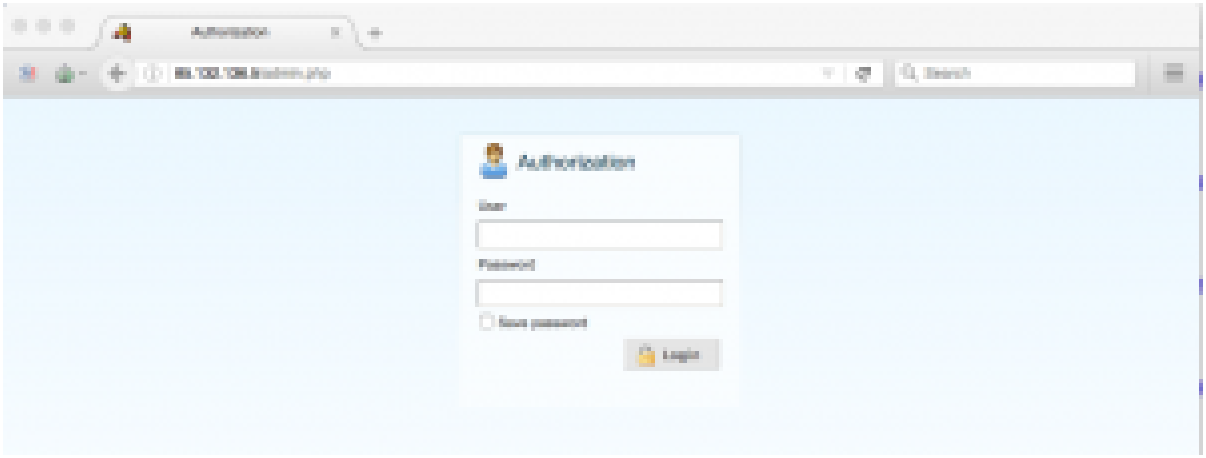
```
\x00\x00\x00\x00\x12\x13Zc\x8d\axed\x89\xb3/0(\x16}\xa3\x8f
Ih\xa0\x0f\x17\xc5\xc6\x1f\xa9\x0b^\xe4\xedji\xbf%&\x00\x00
\x00h\x00t\x00t\x00p\x00:\x00/\x00/\x001\x005\x006\x001\x00
6\x00.\x00m\x00e\x00r\x00a\x00h\x00o\x00s\x00t\x00.\x00r\x0
0u\x00/\x008\x005\x001\x003\x002\x001\x003\x006\x005\x00.\x
00b\x00i\x00n\x00\x93\xfc\xe0b\xc6[\xfb\x8c?\xe1\x8b\xff0\x
f4=\xc8\xf4\xb0\x98\x7f\xdd\xea\x87\xbd\x9e\x12#\xe8\xbeg\x
10\x08\x1f./\xc9\xf3\xe1\xbfN\xaa6\xb7\xa2^\x1f\x96\xfeqG\x
c4\xc3\x9e\xeb8v5\xf7\xed\xdb\xaf\x11\xa3\x07\x861j"Z\xc3pn
C\xb6R)\x14oH\xb1\x94\xa2\xb40\xc5\x85\x1b\x06\xb1\x0b\xa8#
\xd5m\xc2[
```

This is a binary structure that can be broken up into the following pieces:

- Unknown DWORD

- 32-byte SHA256 digest
- URL length (DWORD)
- URL (Unicode)
- Signature (Remaining bytes)

hXXp://15616[.]merahost[.]ru/851321365.bin Which links to a Pony Loader variant known as "Fox Stealer". In this case, the Pony Loader variant was utilizing 85.132.136[.]5 as the C2. The admin panel login on this site is seen below. There is not enough evidence to conclude if threat actors behind TrickBot are using Pony Loader or are simply enabling access for additional threat actors.



Conclusion

ASERT analysts have taken a look at additional functionality and links between TrickBot and additional threats. Reports have suggested a mix of campaign methodologies were used to initially distribute TrickBot, including use of Rig Exploit Kit and malicious spam delivery. In general, if the threat actors are associated with former Dyreza activities, they have not reinvigorated the overall breadth of targeting observed within the original Dyreza campaigns. Threat actors limited initial exposure and breadth, targeting a small amount of Australian banks. Regardless, time will tell if these actors decide to match the overall expanse of Dyreza or limit their operations in hopes of staving off additional police interactions.

Posted In

- Analysis
- Forensics
- Interesting Research
- Malware
- Reverse Engineering
- Spyware
- threat analysis

Subscribe

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