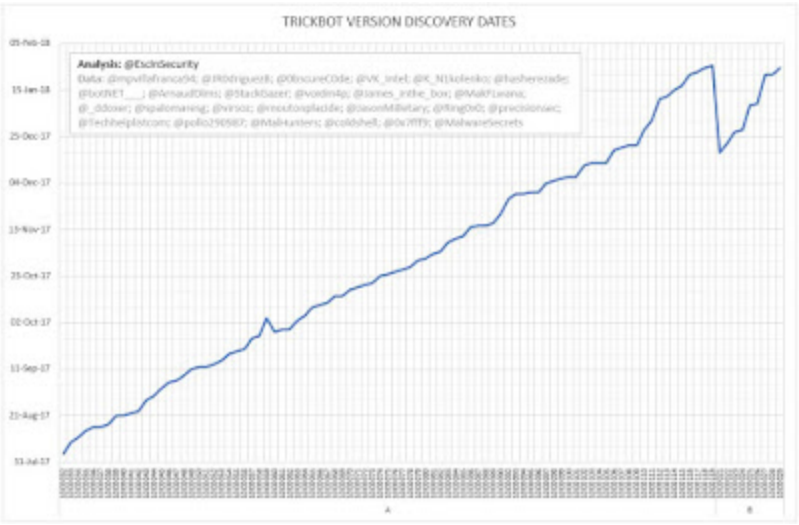
Weekly TrickBot Analysis - End of w/c 22-Jan-2018 to 1000119

escinsecurity.blogspot.de/2018/01/weekly-trickbot-analysis-end-of-wc-22.html

Here are the results of my analysis of TrickBot Banking Trojan mcconfs shared up to the end of the **week commencing 22nd January 2018.** This analysis covers **1,302 unique C2 IP addresses** used in **255 mcconfs** across **118 versions**, with a **highest version of 1000119**.

The following graph shows the rate of discovery of TrickBot versions in the wild, based on shared mcconfs. (Note: The flatter the line, the more frequently versions are discovered.)

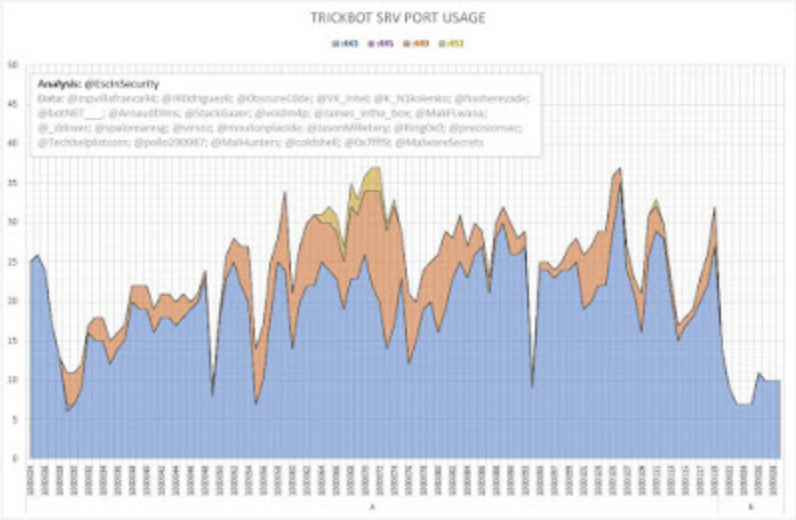
Seven versions were discovered in the week commencing 22th January 2018 (A-1000116, A-1000117, A-1000118, A-1000119, B-1000027, B-1000028, and B-1000029), two the week before, and four the week before that. Four of the discovered versions extend the original iteration of version numbers (which I refer to as iteration A), taking this to 1000119. Three shared versions extend the six repeats from the last two months, where low (1000021 to 1000026) version numbers are reused. (I track these as part of a new, distinct iteration, iteration B, of the version numbers.)



The following graph shows the number of server entries using ports:

- 443 (HTTPS);
- 445 (IBM AS Server Mapper) -- INACTIVE;
- 449 (Cray Network Semaphore Server); and
- 451 (SMB) -- INACTIVE.

This week's iteration A configs increased the count of C2 server entries back to a level last seen at the start of January. The iteration B configs seen continue the low C2 server count which has typified iteration B.



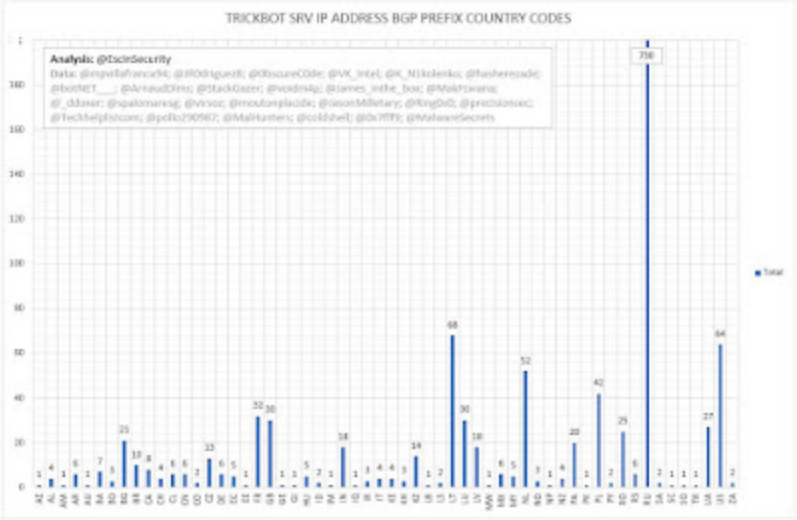
The following table shows the top 25 servers (of 1,302 unique) used within the 118 versions. This table changes for the first time in five weeks with the introduction of 94[.]127[.]111[.]14[:]449 into the top 25 due to its use between versions 1000109 and 1000116.

SRV IP:Port Address	Number of Uses	First Used	Last Used
91.83.88.51:449	17	A-1000058	A-1000063
176.120.126.21:449	17	A-1000065	A-1000081
191.7.30.30:443	15	A-1000024	A-1000038
84.238.198.166:449	14	A-1000030	A-1000046
156.17.92.161:449	14	A-1000068	A-1000081
186.103.161.204:443	12	A-1000024	A-1000035
46.160.165.31:443	11	A-1000025	A-1000035
79.106.41.9:449	11	A-1000092	A-1000102
79.170.7.139:449	11	A-1000064	A-1000074
83.0.245.234:449	11	A-1000080	A-1000090
187.188.162.150:449	11	A-1000080	A-1000090
46.257.117.193:449	10	A-1000059	A-1000068
89.231.13.38:449	10	A-1000058	A-1000063
91.239.249.118:449	10	A-1000065	A-1000074
196.202.194.202:451	10	A-1000065	A-1000074
200.111.97.235:449	10	A-1000101	A-1000110
46.20.56.239:449	8	A-1000065	A-1000072
82.146.48.44:443	8	A-1000100	A-1000107
94.127.111.14:449	8	A-1000109	A-1000116
94.250.253.142:443	8	A-1000100	A-1000107
187.191.0.42:449	8	A-1000076	A-1000083
36.57.176.6:443	7	A-1000002	A-1000012
36.66.107.162:443	7	A-1000012	A-1000019
41.57.103.218:449	7	A-1000064	A-1000070
51.254.164.249:443	7	A-1000038	A-1000044

Analysis: @EsclnSecurity
Data: @mpvillafranca94; @JR0driguezB; @0bscureC0de; @VK_Intel; @K_N1kolenko; @hasherezade; @botNET___; @ArnaudDlms; @StackGazer; @voidm4p; @James_inthe_box; @MakFLwana; @_ddoxer; @spalomaresg; @virsoz; @moutonplacide; @JasonMilletary; @Ring0x0; @precisionsec; @Techhelplistcom; @pollo290987; @MalHunters; @coldshell; @0x7fff9; @MalwareSecrets

The following table shows the breakdown of detected TrickBot campaign 'gtag' (group tags) values used in the 255 mcconfs analysed.

97 C2 servers were used in the mcconfs from this week, of which 84 (87%) were new. The BGP prefix registrations for the C2 server IP addresses continue to be heavily biased to ASN routed through RU (and so the graph below's Y-axis is cut short to allow clearer viewing of other country counts). The new servers' IP addresses are associated with ASN routed to: 64xRU, 10xNL, 3xIN, 3xLU, 2xPL, 1xCH, and 1xUS.



The following map shows the geographical location of 85 (scanned by Shodan) of the 97 IP addresses used in the analysed configs.

Five of these servers are **MikroTik** devices (historically a favourite of TrickBot), one is an **ER-X** and one is a **NanoStation Loco M5**.

49 are running **OpenSSH**, 25 are running **nginx**, 16 are running **Apache**, eight are running **Exim**, eight are running **Postfix**, four are running **MySQL**, four are running **ProFTPD**, one is running ARK, one is running **Dropbear SSH**, one is running **IIS**, one is running **Squid Proxy** -- with some servers running as many as four of these products.

The following table shows the BGP allocations of C2 servers' IP addresses to country by TrickBot version.

Finally, the following table shows the top 25 BGP prefixes used by TrickBot for C2 servers.

BGP Prefix	ASN	AS Name	CC	Allocated	Number of SRV
92.53.64.0/19	49505	SELECTEL, RU	RU	15/02/2008	58
194.87.236.0/22	48347	MTW-AS, RU	RU	01/09/1994	35
194.87.92.0/22	48347	MTW-AS, RU	RU	01/09/1994	35
195.133.144.0/22	48347	MTW-AS, RU	RU	15/04/1997	33
185.80.128.0/22	61053	VPSNET-AS, LT	LT	09/12/2014	30
95.213.128.0/17	49505	SELECTEL, RU	RU	12/08/2009	28
82.146.56.0/21	29182	ISPSYSTEM-AS, LU	RU	18/06/2003	22
195.133.196.0/23	48347	MTW-AS, RU	RU	15/04/1997	20
194.87.144.0/22	48347	MTW-AS, RU	RU	01/09/1994	20
92.63.104.0/22	29182	ISPSYSTEM-AS, LU	RU	07/02/2008	19
194.87.102.0/23	48347	MTW-AS, RU	RU	01/09/1994	19
179.43.128.0/18	51852	PLI-AS, CH	PA	12/11/2013	17
185.158.115.0/24	44812	IPSERVER-RU-NET, UA	RU	05/07/2016	16
82.202.192.0/18	49505	SELECTEL, RU	RU	06/10/2003	15
95.154.192.0/18	20860	IOMART-AS, GB	GB	25/02/2009	15
91.211.244.0/22	61053	VPSNET-AS, LT	LT	02/02/2009	15
178.156.202.0/24	48874	HOSTMAZE HOSTMAZE,	RO	02/06/2010	14
94.250.252.0/23	29182	ISPSYSTEM-AS, LU	NL	12/09/2012	14
149.154.68.0/23	29182	ISPSYSTEM-AS, LU	RU	01/08/2011	14
62.109.16.0/21	29182	ISPSYSTEM-AS, LU	RU	26/09/2008	14
185.125.44.0/22	48096	ITGRAD, RU	KZ	06/11/2015	14
92.63.96.0/21	29182	ISPSYSTEM-AS, LU	RU	07/02/2008	14
78.24.216.0/21	29182	ISPSYSTEM-AS, LU	RU	13/09/2007	14
195.133.48.0/23	48347	MTW-AS, RU	RU	15/04/1997	13
37.230.114.0/23	29182	ISPSYSTEM-AS, LU	LU	12/04/2012	13

Analysis: @EscInSecurity
Data: @mpvillafranca94; @JR0driguezB; @0bscureC0de; @VK_Intel; @K_N1kolenko; @hasherezade; @botNET___; @ArnaudDlms; @StackGazer; @voidm4p; @James_inthe_box; @MakFLwana; @_ddoxer; @spalomaresg; @virsoz; @moutonplacide; @JasonMilletary; @Ring0x0; @precisionsec; @Techhelplistcom; @pollo290987; @MalHunters; @coldshell; @0x7fff9; @MalwareSecrets

Thanks to @mpvillafranca94, @JR0driguezB, @0bscureC0de, @virsoz, @spalomaresg, @VK_Intel, @K_N1kolenko, @hasherezade, @botNET___, @ArnaudDlms, @StackGazer,@voidm4p, @James_inthe_box, @MakFLwana, @_ddoxer, @moutonplacide, @JasonMilletary,@Ring0x0, @precisionsec, @Techhelplistcom, @pollo290987, @MalHunters, @coldshell, @0x7fff9 and @MalwareSecrets for sharing the mcconfs.