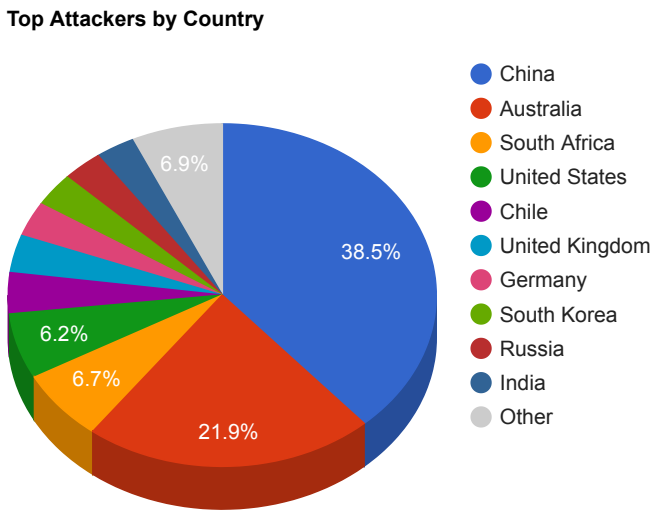
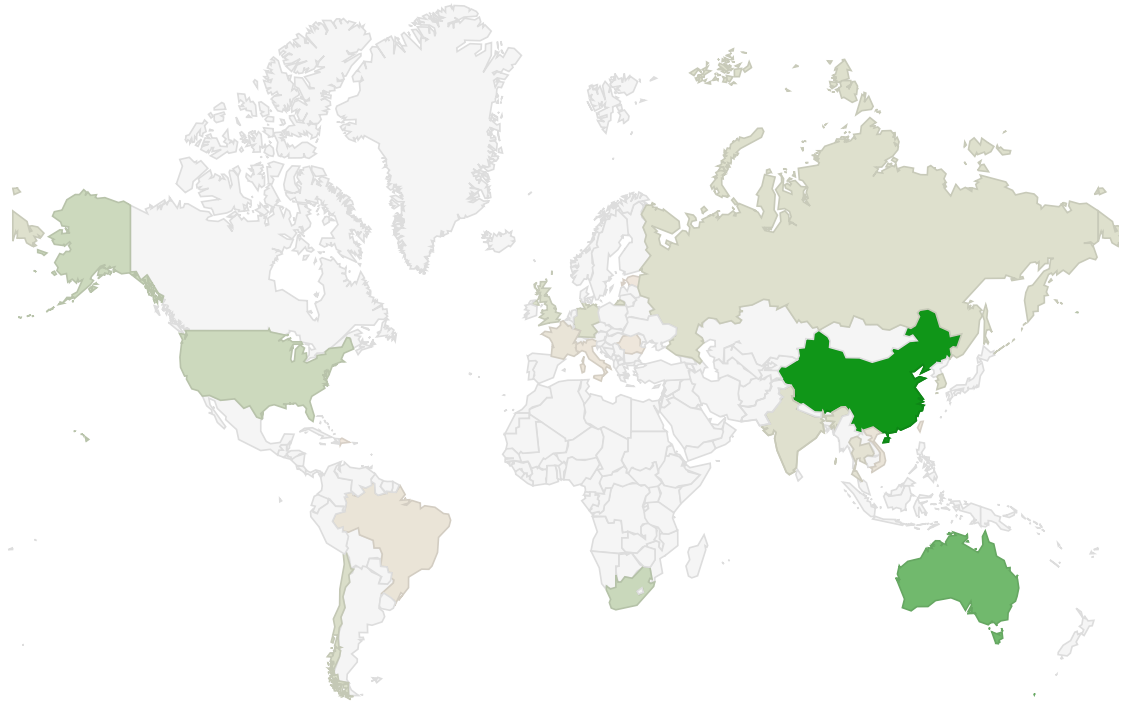
Trends

- The top attacker country was China with 656640 unique attackers (36.00%).
- The top Trojan C&C server detected was TrickBot with 26 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	656640	36.00%
Australia	373252	20.00%
South Africa	114464	6.00%
United States	105652	5.00%
Chile	65878	3.00%
United Kingdom	60798	3.00%
Germany	55888	3.00%
South Korea	54084	2.00%
Russia	51979	2.00%
India	50317	2.00%
Thailand	33862	1.00%
France	19625	1.00%
Brazil	18032	0%
Vietnam	16269	0%
Italy	12253	0%
Taiwan	6748	0%
Romania	4913	0%
Estonia	3276	0%
Dominican Republic	2909	0%



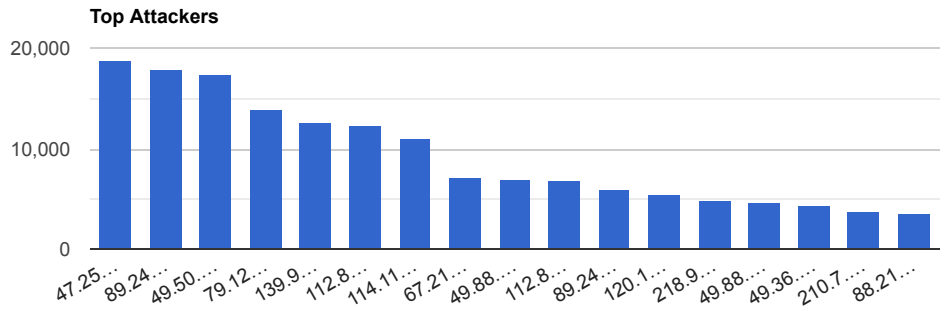


2,909 656,640

Top Attacking Hosts

Host	Occurrences
47.254.21.172	18931
203.82.209.213	18350
89.248.168.221	17945
49.50.69.85	17363
79.124.62.74	13943
139.99.187.23	12741
112.85.42.187	12298
114.116.225.21	11054

67.218.157.95	7216
49.88.112.115	7016
112.85.42.88	6762
89.248.162.136	6003
120.155.9.101	5577
218.92.0.190	4934
49.88.112.110	4677
49.36.128.29	4414
210.7.22.74	3810
88.218.17.15	3568

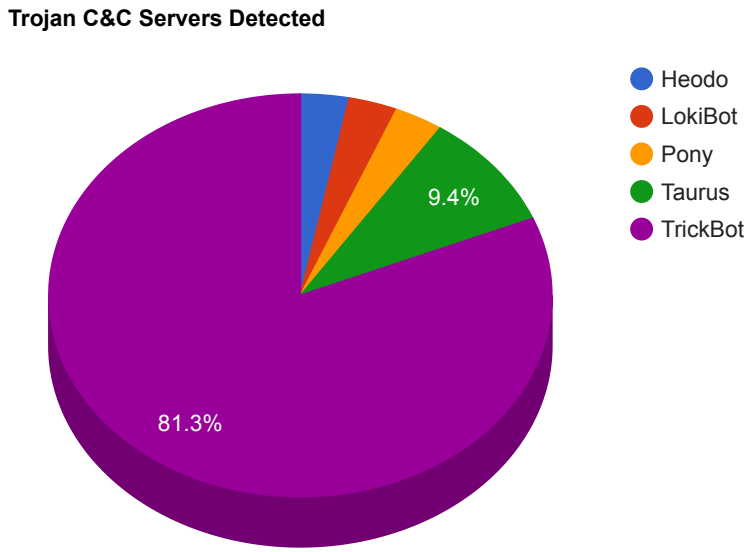


Top Network Attackers

ASN	Country	Name
45102	United States	CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd., CN
202425	Netherlands	INT-NETWORK, SC
55470	India	CYFUTURE-AS-IN Cyfuture India Pvt. Ltd., IN
207812	Bulgaria	DM_AUTO, BG
55990	China	HWCSNET Huawei Cloud Service data center, CN
25820	Canada	IT7NET, CA
55836	India	RELIANCEJIO-IN Reliance Jio Infocomm Limited, IN
4638	Fiji	IS-FJ-AS Telecom Fiji Limited, FJ
50673	Netherlands	SERVERIUS-AS, NL

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	1	193.80.169.64
LokiBot	1	148.66.135.80
Pony	1	162.244.92.35
Taurus	3	104.18.45.216 , 185.141.62.31 , 185.219.83.222
TrickBot	26	104.168.125.105 , 107.155.137.3 , 158.69.133.69 , 172.245.159.191 , 185.14.30.22 , 185.14.30.52 , 185.164.32.114 , 185.17.122.167 , 185.90.61.140 , 185.99.2.133 , 185.99.2.238 , 194.36.189.141 , 194.5.250.96 , 194.87.236.66 , 217.12.209.60 , 31.131.20.244 , 5.1.74.116 , 5.1.81.127 , 5.182.211.215 , 82.146.40.192 , 85.204.116.14 , 85.204.116.16 , 93.189.41.252 , 93.189.41.96 , 93.189.43.61 , 94.250.249.38



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
c6dc7326766f3769575caa3ccab71f63	https://www.virustotal.com/gui/file/fb022bbec694d9b38e8a0e80dd0bfdfe0a462ac0d180965d314651a7bc0614f4/details	wupxarch.exe	N/A	Win.Dropper.Ranumbot::in03.talos
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	W32.AgentWDCR:Gen.21gn.1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	