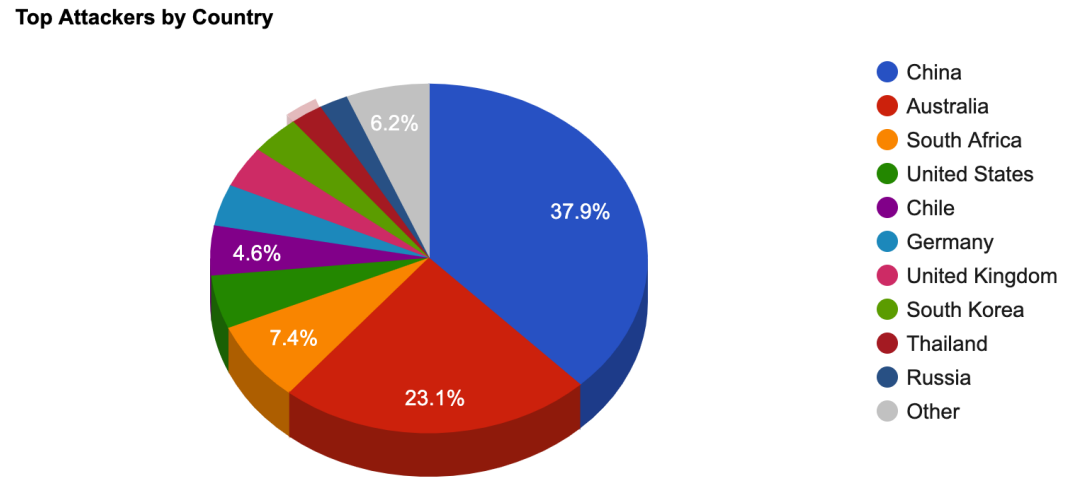
Trends

- The top attacker country was China with 535153 unique attackers (37.00%).
- The top Trojan C&C server detected was TrickBot with 12 instances detected.

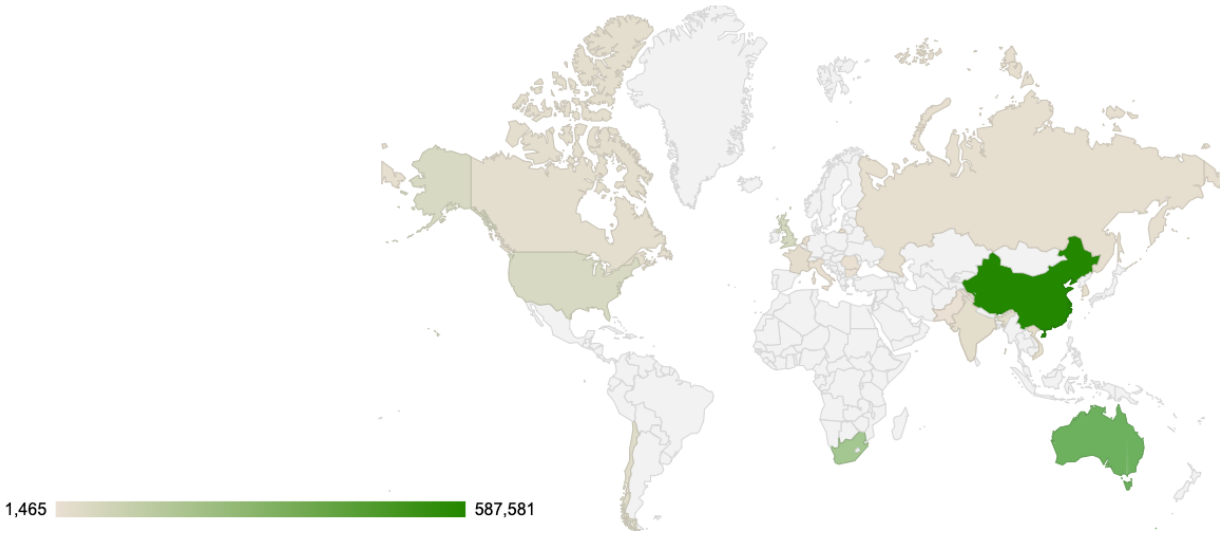
Top Attackers By Country

Country	Occurences	Percentage
China	535153	37.00%
Australia	326654	22.00%
South Africa	105017	7.00%
United States	69770	4.00%
Chile	65136	4.00%
Germany	54433	3.00%
United Kingdom	54097	3.00%
South Korea	51444	3.00%
Thailand	33862	2.00%
Russia	29955	2.00%
Brazil	17159	1.00%
France	17067	1.00%
Vietnam	15215	1.00%
India	13781	0%
Italy	10296	0%
Taiwan	6748	0%
Dominican Republic	2909	0%

Estonia	2869	0%
Romania	1422	0%



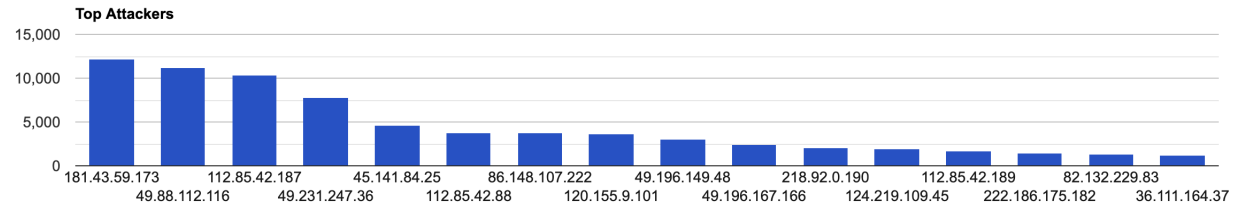
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
181.43.59.173	12186
49.88.112.116	11206
112.85.42.187	10399
49.231.247.36	7781
45.141.84.25	4662
112.85.42.88	3800
86.148.107.222	3762
120.155.9.101	3629
49.196.149.48	3059

49.196.167.166	2470
218.92.0.190	2034
86.131.23.36	1996
124.219.109.45	1945
112.85.42.189	1677
222.186.175.182	1411
82.132.229.83	1382
36.111.164.37	1271

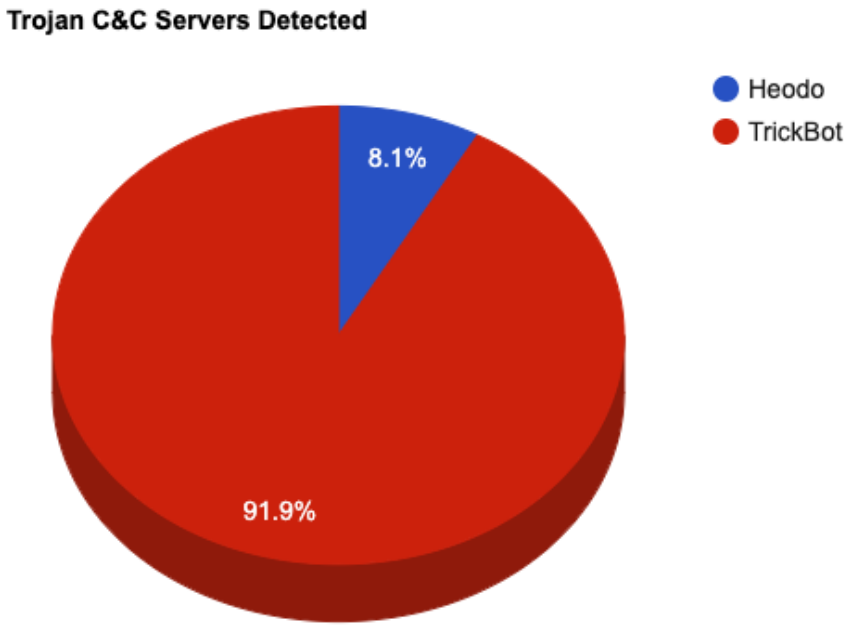


Top Network Attackers

ASN	Country	Name
24154	Taiwan	APBT-AS-TW Asia Pacific Broadband Fixed Lines Co., Ltd., TW
35228	United Kingdom	O2BROADBAND, GB
58519	China	CHINATELECOM-CTCLOUD Cloud Computing Corporation, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Kpot	1	63.250.39.193
TrickBot	12	107.155.137.25 , 107.155.137.28 , 107.175.87.128 , 185.14.31.87 , 185.14.31.97 , 185.164.32.115 , 194.5.250.80 , 195.54.32.40 , 45.67.231.62 , 45.83.192.152 , 5.188.168.87 , 85.204.116.58



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
5d34464531ddbdc7b0a4dba5b4c1cfea	https://www.virustotal.com/gui/file/a545df34334b39522b9cc8cc0c11a1591e016539b209ca1d4ab8626d70a54776/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::in03.talos
c6dc7326766f3769575caa3ccab71f63	https://www.virustotal.com/gui/file/fb022bbec694d9b38e8a0e80dd0bfdfe0a462ac0d180965d314651a7bc0614f4/details	wupxarch.exe	N/A	Win.Dropper.Ranumbot::in03.talos
4202e589899ec68bc2d4fa6fb1218e2f	https://www.virustotal.com/gui/file/9cc2b845bdee4774e45143e00dc82c673bf940c764b687c976f8d27d9f48b704/details	app171.exe	N/A	Win.Dropper.Ranumbot::sbmt.talos

8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	W32.AgentWDCR:Gen.21gn.1201