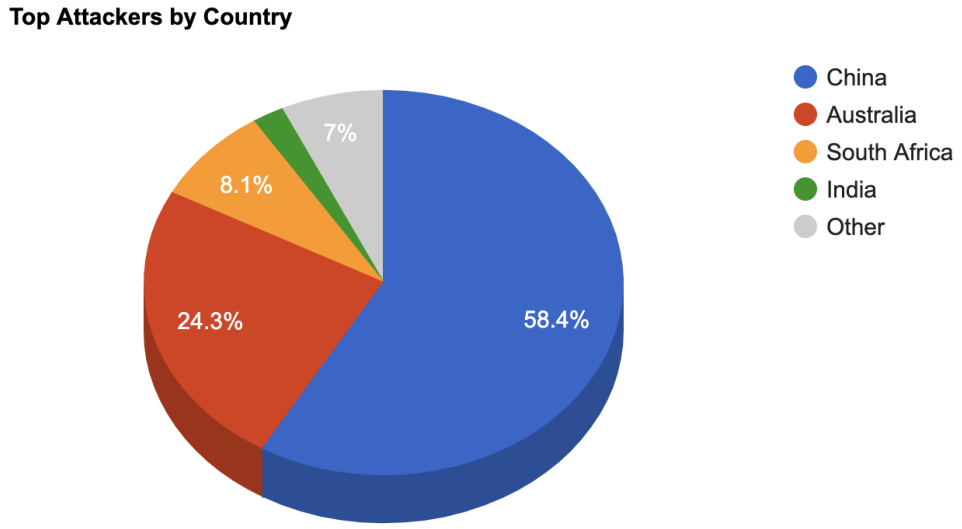
Trends

- The top attacker country was China with 127189 unique attackers (57.00%).
- The top Trojan C&C server detected was Heodo with 44 instances detected.

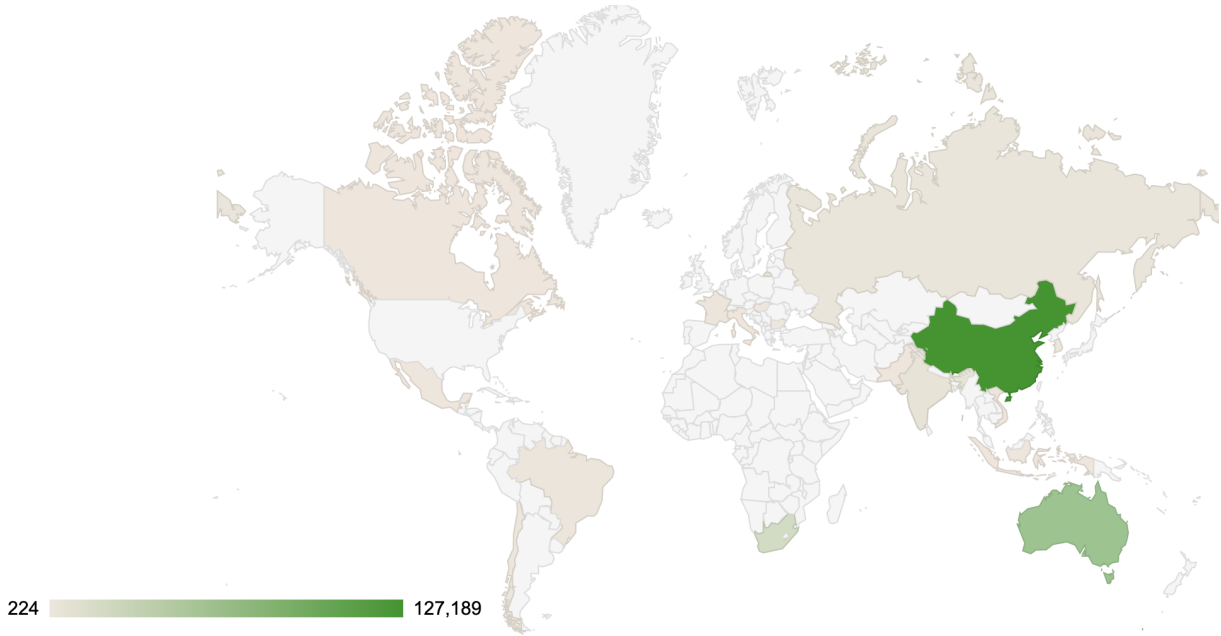
Top Attackers By Country

Country	Occurences	Percentage
China	127189	57.00%
Australia	52974	23.00%
South Africa	17686	7.00%
India	4671	2.00%
Hong Kong	3561	1.00%
Russia	2248	1.00%
Brazil	1578	0%
Vietnam	1547	0%
France	1255	0%
South Korea	950	0%
Chile	800	0%
Bulgaria	520	0%
Hungary	504	0%
Indonesia	486	0%
Italy	481	0%
Mexico	395	0%
Canada	367	0%
Armenia	298	0%

Pakistan	224	0%

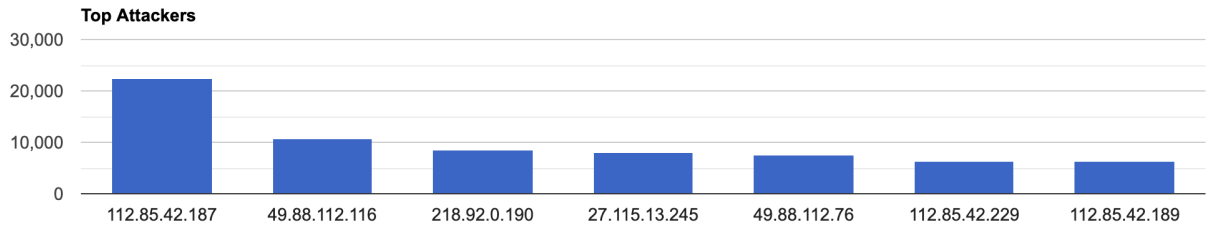


Threat Geo-location



Top Attacking Hosts

Host	Occurrences
112.85.42.187	22477
49.88.112.116	10676
218.92.0.190	8617
27.115.13.245	8075
49.88.112.76	7517
112.85.42.229	6297
112.85.42.189	6273



Top Network Attackers

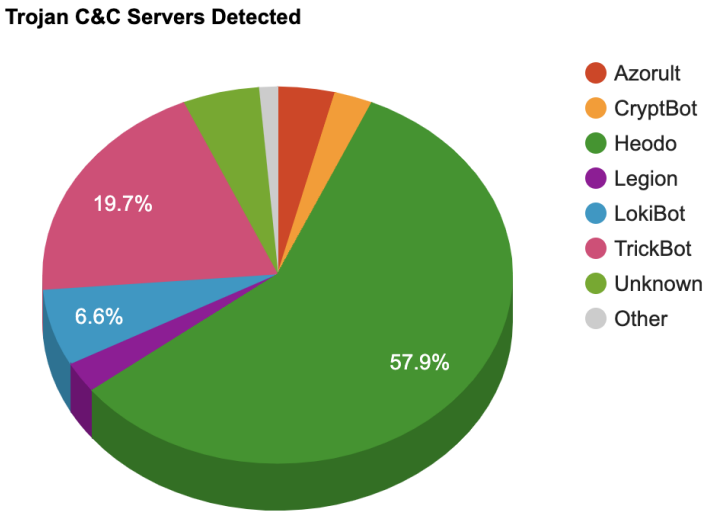
ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
17621	China	CNCGROUP-SH China Unicom Shanghai network, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	95.163.212.79
Azorult	3	176.32.33.157 , 209.127.19.34 , 45.143.138.14
CryptBot	2	176.32.33.157 , 45.143.138.14

Heodo	44	101.100.137.135 , 104.131.41.185 , 104.236.161.64 , 104.236.28.47 , 105.27.155.182 , 108.190.109.107 , 110.44.113.2 , 113.52.123.226 , 125.207.127.86 , 136.243.205.112 , 146.255.96.214 , 154.70.158.97 , 162.154.175.215 , 174.83.116.77 , 175.139.209.3 , 177.188.121.26 , 178.62.75.204 , 181.60.244.48 , 184.162.115.11 , 184.172.27.82 , 186.10.92.114 , 186.6.245.26 , 190.70.1.69 , 198.211.121.27 , 200.69.224.73 , 207.177.72.129 , 210.213.85.43 , 218.255.173.106 , 23.243.215.4 , 31.16.195.72 , 45.55.179.121 , 5.34.158.102 , 60.151.66.216 , 65.184.222.119 , 68.183.18.169 , 70.127.155.33 , 70.60.238.62 , 74.208.45.104 , 74.50.51.115 , 85.96.49.152 , 89.19.20.202 , 91.72.179.214 , 94.76.247.61 , 95.66.182.136
Legion	2	35.228.215.155 , 47.241.1.210
LokiBot	5	103.116.16.173 , 103.74.123.3 , 108.163.221.2 , 209.127.19.34 , 78.128.76.165

TrickBot	15	104.193.252.168 , 185.66.12.59 , 194.99.21.137 , 195.123.240.197 , 198.8.91.25 , 212.109.195.100 , 212.109.195.175 , 212.109.220.222 , 212.80.217.162 , 83.220.168.254 , 85.143.220.73 , 85.217.170.137 , 92.38.171.11 , 93.189.41.185 , 95.181.198.236
Unknown	4	163.172.20.152 , 5.188.60.21 , 5.188.60.58 , 5.188.60.59



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
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
7c38a43d2ed9af80932749f6e80fea6f	https://www.virustotal.com/gui/file/c0cdd2a671195915d9ffb5c9533337db935e0cc2f4d7563864ea75c21ead3f94/details	xme64-520.exe	N/A	PUA.Win.File.Coinminer::1201
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f		N/A
a917d39a8ef125300f2f38ff1d1ab0db	https://www.virustotal.com/gui/file/d91abcd024d4172fadc5aa82750a18796a549207b76f624b8a9d165459379258/details	FFChromeSetters	N/A	PUA.Osx.Adware.Macsearch::agent.tht.talos