Trends

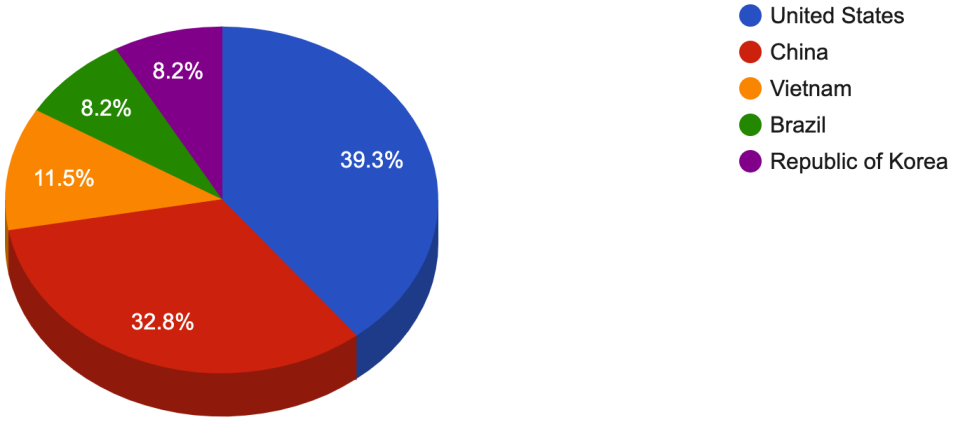
- The top attacker country was China with 195228 unique attackers (33.00%).
- The top Trojan C&C server detected was Lokibot with 33 instances detected.

Top Attackers By Country

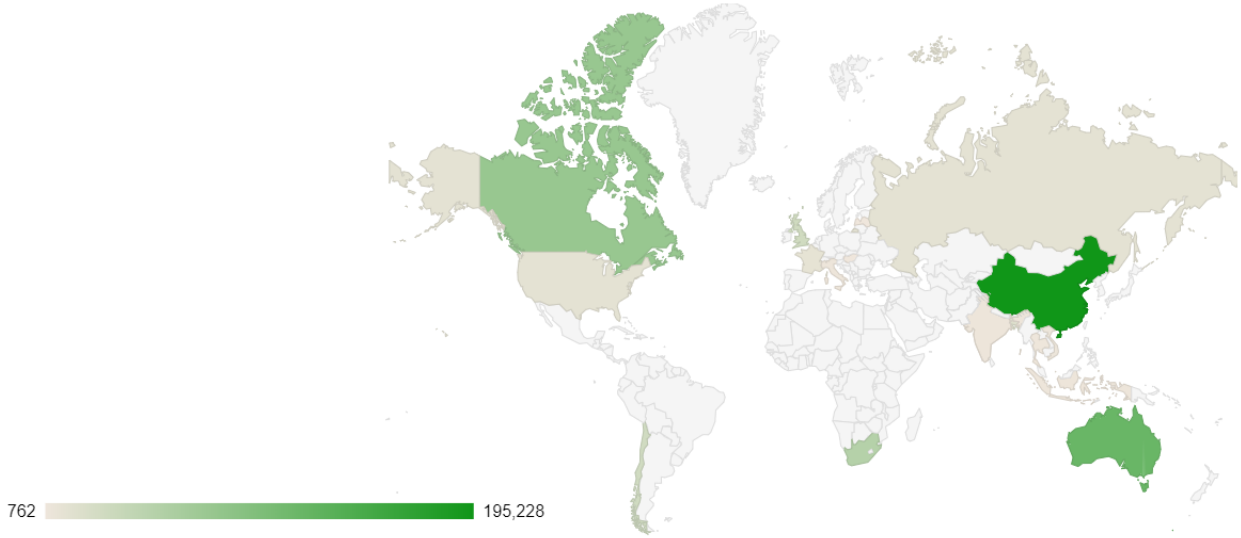
Country	Occurences	Percentage
China	195228	33.00%
Australia	117410	20.00%
Canada	76248	13.00%
South Africa	51483	8.00%
United Kingdom	28068	4.00%
Chile	27916	4.00%
Bangladesh	16684	2.00%
Russia	10059	1.00%
United States	9970	1.00%
France	9033	1.00%
Vietnam	2993	0%
Italy	2491	0%
India	2423	0%
Indonesia	2318	0%
Thailand	1585	0%
Hong Kong	1225	0%
Seychelles	921	0%

Hungary	790	0%
Latvia	762	0%

Top Attackers by Country



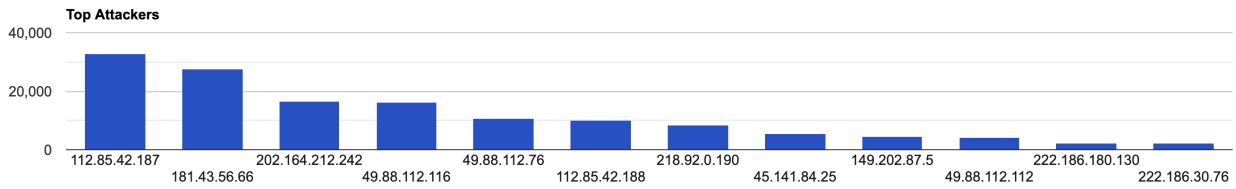
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
112.85.42.187	32773
181.43.56.66	27667
202.164.212.242	16684
49.88.112.116	16193
49.88.112.76	10832
112.85.42.188	10150
218.92.0.190	8553
45.141.84.25	5557
149.202.87.5	4648
49.88.112.112	4303
222.186.180.130	2370

222.186.30.76	2316



Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
6471	Chile	ENTEL CHILE S.A., CL
38026	Bangladesh	MNBL-TRANSIT-AS-AP MetroNet Bangladesh Limited, Fiber Optic Based Metropolitan Data, BD
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
206728	Russia	MEDIALAND-AS, RU
16276	France	OVH, FR
23650	China	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN

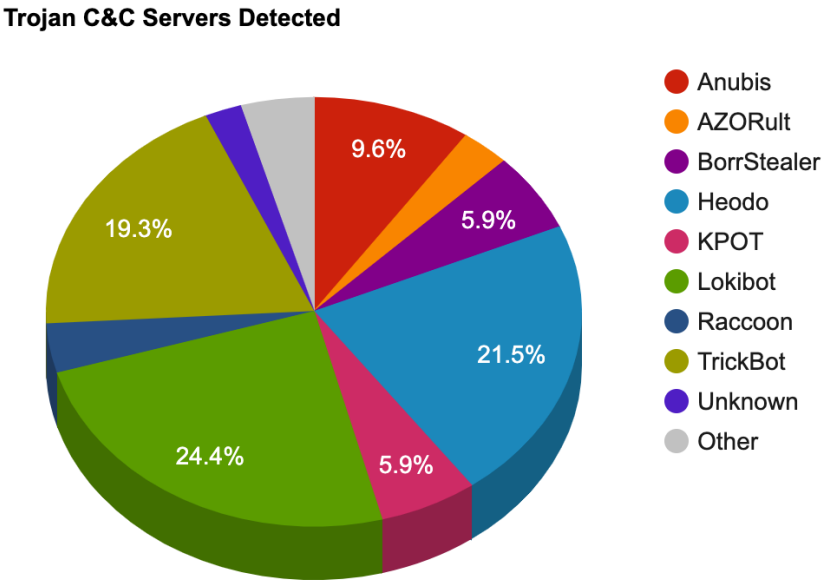
Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	95.163.248.15
Anubis	13	185.31.163.148 , 198.54.117.244 , 1.pestola.online , 69.com , 72.18.132.133 , borjomi-ge.club , doktorlar.com , elka929.club , pinpong.top , rxetcryvtubyinurxetcryvtubyinumcryvetucaybnu.com , vitel.top , www.newtest456678.top , yourdarkside.club
AZORult	4	20.36.46.115 , 217.160.59.64 , 45.143.138.38 , 95.163.214.100
Betabot	1	170.106.50.37

BorrStealer	8	141.8.192.46 , 176.57.69.214 , 185.178.208.176 , 209.182.217.85 , 212.86.115.244 , 45.132.105.97 , 45.14.14.38 , gwujbwnug381u2hgb22hg172.fun
Heodo	29	101.141.5.17 , 110.232.188.29 , 129.205.201.163 , 149.210.171.237 , 152.169.31.120 , 173.24.68.195 , 174.53.195.88 , 182.71.222.187 , 187.162.248.237 , 189.235.233.119 , 213.107.110.252 , 213.60.19.245 , 24.167.122.146 , 37.211.90.253 , 42.115.22.145 , 45.118.133.154 , 47.155.214.239 , 50.251.171.165 , 5.32.84.54 , 64.207.176.4 , 70.187.114.147 , 71.126.247.90 , 71.197.197.100 , 71.222.233.135 , 76.86.17.1 , 78.188.33.71 , 85.100.115.92 , 91.74.88.6 , 98.15.121.180
KPOT	8	104.24.125.192 , 111.90.142.112 , 161.117.184.53 , 176.57.217.21 , 190.97.166.142 , 192.64.119.14 , 8.208.26.77 , 89.105.202.59

Lokibot	33	103.21.59.27 , 103.74.123.3 , 104.223.170.113 , 104.24.100.123 , 104.27.156.253 , 104.31.70.73 , 104.31.78.250 , 104.31.89.164 , 107.175.150.73 , 111.90.156.119 , 162.241.6.97 , 170.106.50.37 , 173.247.252.61 , 176.107.160.198 , 176.126.201.11 , 176.32.33.34 , 192.185.119.161 , 192.185.88.246 , 192.185.92.174 , 192.185.92.183 , 193.142.59.96 , 198.23.200.241 , 207.174.213.181 , 45.143.138.38 , 45.252.248.29 , 46.165.223.4 , 66.85.173.45 , 68.183.42.186 , 89.208.196.16 , 89.208.84.96 , 89.37.226.146 , 95.163.212.79 , noniwire7.website
Pony	1	107.175.150.73
Raccoon	5	34.65.176.45 , 34.77.125.60 , 35.204.238.220 , 35.228.28.245 , 35.246.8.131
SmokeLoader	1	45.141.86.24
Tables	1	45.141.86.52

TrickBot	26	107.172.165.149 , 146.185.253.181 , 185.11.146.86 , 185.186.77.222 , 185.65.202.240 , 185.99.2.52 , 188.227.84.209 , 193.26.217.243 , 194.5.250.52 , 195.123.219.69 , 195.123.220.154 , 23.95.231.164 , 45.148.120.13 , 45.148.120.31 , 46.229.213.27 , 51.254.164.240 , 51.89.73.154 , 5.2.77.18 , 5.2.78.70 , 5.2.78.77 , 5.34.177.40 , 64.44.133.39 , 66.85.173.20 , 81.177.180.254 , 85.204.116.84 , 88.99.112.87
Unknown	3	217.29.57.164 , 45.80.68.4 , 5.8.88.189
Vidar	1	185.99.133.188



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name

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
88cbadec77cf90357f46a3629b6737e6	https://www.virustotal.com/gui/file/1460fd00cb6addf9806a341fee9c5ab0a793762d1d97dca05fa17467c8705af7/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.File.2144flashplayer::tpd
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/c3e530cc0055583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc0055583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f		N/A

CVEs with Recently Discovered Exploits

This is a list of recent vulnerabilities for which exploits are available.

CVE, Title, Vendor	Description	CVSS v2 Base Score	Date Created	Date Updated

CVE-2019-18426 whatsapp Cross-Site Scripting Vulnerability whatsapp	A vulnerability in WhatsApp Desktop versions when paired with WhatsApp for iPhone versions allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.	5.8(AV:N/AC:M/Au:N/C:P/I:P/A:N)	01/21/2020	01/29/2020

CVE-2019-16027 Cisco IOS XR Software Intermediate System-to-Intermediate System Denial of Service Vulnerability Cisco	A vulnerability in the implementation of the Intermediate System-to-Intermediate System (IS-IS) routing protocol functionality in Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service condition in the IS-IS process. The vulnerability is due to improper handling of a SNMP request for specific Object Identifiers OIDs by the IS-IS process. An attacker could exploit this vulnerability by sending a crafted SNMP request to the affected device.	4.0(AV:N/AC:L/Au:S/C:N/I:N/A:P)	01/26/2020	01/31/2020

CVE-2019-16516 ConnectWise Control User Enumeration Information Disclosure Vulnerability ConnectWise	An issue was discovered in ConnectWise Control (formerly known as ScreenConnect). ConnectWise Control is vulnerable to a user enumeration vulnerability, allowing an unauthenticated attacker to determine with certainty if an account exists for a given username.	5.0(AV:N/AC:L/Au:N/C:P/I:N/A:N)	01/23/2020	01/28/2020
CVE-2020-8417 WordPress Code Snippets Plugin Remote Code Execution Vulnerability WordPress	WordPress plugin code snippets is vulnerable to cross site request forgery. Plugin's import function does not provide protection against CSRF. This vulnerability leads to Remote Code Execution. An attacker could possibly exploit this vulnerability and gain access to sensitive information.	7.5(AV:N/AC:M/Au:S/C:C/I:P/A:P)	01/28/2020	02/06/2020

CVE-2012-6114 pyrad Password Hash Information Disclosure Vulnerability and Packet Spoofing Vulnerability pyrad	pyrad is prone to an information disclosure vulnerability and a packet spoofing vulnerability. An attacker can exploit these issue to obtain sensitive information through man in the middle attacks and spoof packet IDs that may lead to further attacks.	4.3(AV:N/AC:M/Au:N/C:P/I:N/A:N)	01/28/2020	02/07/2020