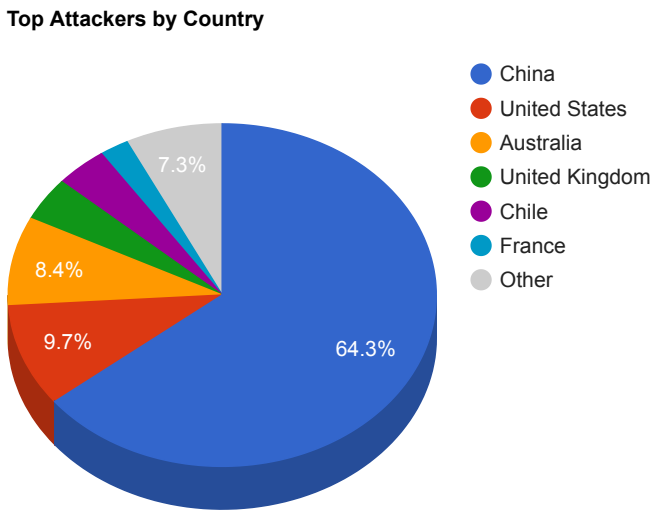
Trends

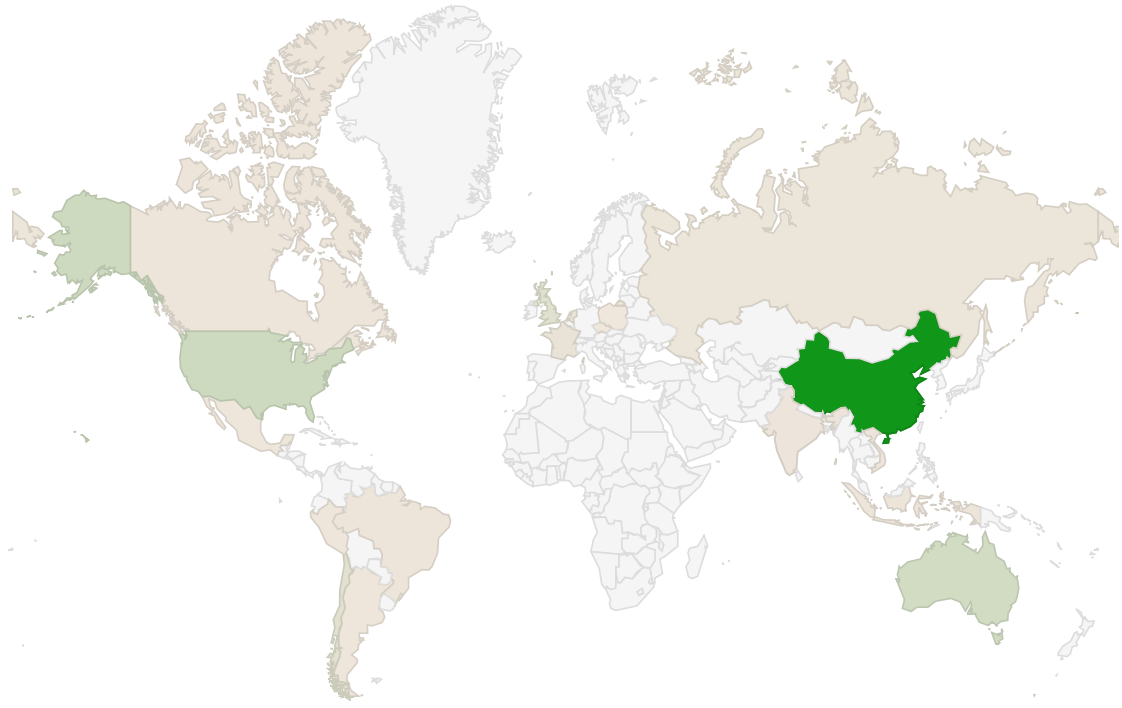
- The top attacker country was China with 263640 unique attackers (62.00%).
- The top Trojan C&C server detected was Heodo with 69 instances detected.
- The top phishing campaign detected was against Facebook accounts with 212 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	263640	62.00%
United States	39698	9.00%
Australia	34385	8.00%
United Kingdom	16916	3.00%
Chile	16170	3.00%
France	9019	2.00%
Netherlands	5394	1.00%
Russia	4496	1.00%
Brazil	3067	0%
Indonesia	3052	0%
Canada	2494	0%
India	2399	0%
Vietnam	2392	0%
Mexico	1954	0%
Peru	1585	0%
Argentina	1516	0%
Poland	674	0%
Europe	653	0%
Czech Republic	454	0%



Threat Geo-location

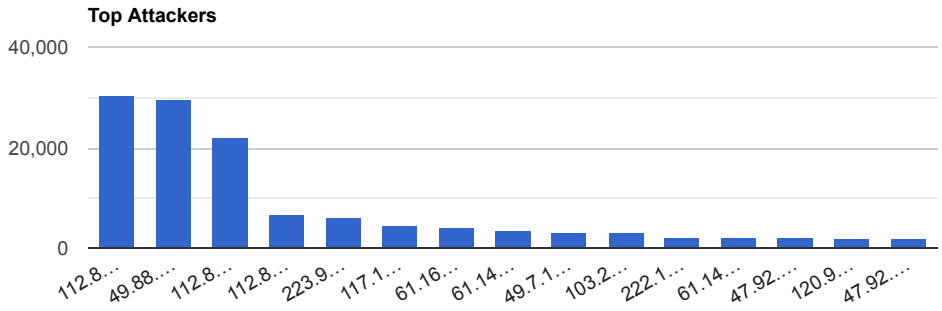


454 263,640

Top Attacking Hosts

Host	Occurrences
112.85.42.187	30611
49.88.112.115	29475
112.85.42.88	22187
112.85.42.189	6728

223.99.14.18	6020
117.139.143.123	4466
61.164.52.180	4198
61.147.70.96	3528
49.7.12.171	3173
103.214.171.18	3115
222.186.180.41	2217
61.149.137.142	2143
47.92.81.116	2127
120.92.159.83	2111
47.92.79.10	2003



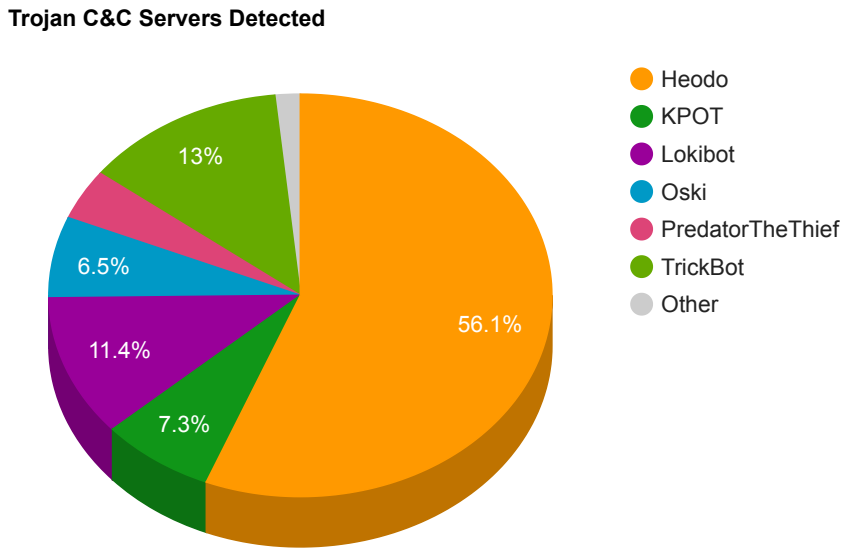
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
24444	China	CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited, CN
9808	China	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
137697	China	CHINATELECOM-JIANGSU-YANGZHOU-IDC CHINATELECOM JiangSu YangZhou IDC networkdescr: YangZhouJiangsu Province, P.R.China., CN
23724	China	CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation, CN
137443	Hong Kong SAR China	ANCHGLOBAL-AS-AP Anchnet Asia Limited, HK
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN
4808	China	CHINA169-BJ China Unicom Beijing Province Network, CN
37963	China	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN
4812 17621	China	CHINANET-SH-AP China Telecom (Group), CN CNCGROUP-SH China Unicom Shanghai network, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Amadey	1	217.8.117.52
AZORult	1	185.183.98.244

Heodo	69	104.131.103.128 , 105.213.67.88 , 107.185.211.16 , 115.78.11.155 , 139.99.157.213 , 147.91.184.91 , 159.203.232.29 , 167.86.90.214 , 173.62.217.22 , 174.100.27.229 , 174.102.48.180 , 176.10.250.88 , 176.216.226.44 , 176.9.93.82 , 177.32.8.85 , 179.62.238.49 , 181.114.114.203 , 181.211.11.242 , 182.176.95.147 , 182.187.139.200 , 185.208.226.142 , 186.32.90.103 , 188.166.25.84 , 188.2.217.94 , 188.83.220.2 , 190.190.15.20 , 190.212.140.6 , 190.53.144.120 , 192.187.99.90 , 192.210.135.126 , 197.83.232.19 , 201.171.150.41 , 201.213.177.139 , 202.5.47.71 , 203.117.253.142 , 207.144.103.227 , 209.126.6.222 , 209.143.35.232 , 212.93.117.170 , 213.176.36.147 , 24.135.198.218 , 24.137.76.62 , 24.148.98.177 , 24.233.112.152 , 37.70.8.161 , 41.106.96.12 , 5.153.250.14 , 51.75.33.120 , 58.171.153.81 , 66.228.49.173 , 66.61.94.36 , 67.205.85.243 , 67.247.242.247 , 69.30.203.214 , 71.57.180.213 , 74.120.55.163 , 81.198.69.61 , 85.105.140.135 , 85.152.162.105 , 85.66.181.138 , 87.98.218.33 , 88.217.172.164 , 91.222.77.105 , 92.24.51.238 , 94.206.45.18 , 95.85.151.205 , 95.9.180.128 , 96.8.113.4 , 97.82.79.83
KPOT	9	172.67.206.85 , 185.193.126.198 , 194.187.249.88 , 198.54.117.197 , 84.38.180.187 , 89.249.67.27 , 94.177.123.102 , files-get.pw , github-download.com
Lokibot	14	103.129.98.18 , 103.129.98.58 , 103.27.62.62 , 162.241.3.30 , 172.67.185.131 , 185.34.216.210 , 194.180.224.87 , 195.69.140.147 , 3.17.153.68 , 45.143.138.26 , 79.124.8.8 , 84.38.180.247 , polysolcomx.com , sanfrm.xyz
Oski	8	104.27.183.143 , 176.119.156.8 , 194.87.101.31 , 213.159.203.231 , 217.8.117.77 , 5.101.153.15 , 91.245.227.131 , daymnebtc.site
PredatorTheThief	5	141.8.192.58 , 141.8.193.236 , 217.107.34.61 , 81.177.139.161 , 95.216.64.168
TrickBot	16	185.164.32.216 , 185.198.57.108 , 194.5.249.197 , 195.123.237.241 , 195.123.239.193 , 45.148.10.164 , 45.148.10.182 , 46.17.107.148 , 62.108.35.90 , 64.44.133.61 , 83.220.171.175 , 83.220.171.193 , 85.143.220.121 , 86.104.194.24 , 86.104.194.28 , 91.200.103.236



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eter.exe	N/A	Win.Exploit.Shadowbrokers::5A5226262.auto.talos
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
34560233e751b7e95f155b6f61e7419a	https://www.virustotal.com/gui/file/8b4216a7c50599b11241876ada8ae6f07b48f1abe6590c2440004ea4db5becc9/details	SAService.exe	SAService	PUA.Win.Dropper.Segurazo::tpd
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201

Top Phishing Campaigns

Phishing Target	Count
Other	1241
Facebook	212
Microsoft	10
RuneScape	9
Scotiabank	1
Sparkasse	2
Google	1
PayPal	4
Apple	2
Adobe	5
Steam	3
Amazon.com	27
Virustotal	6
Orange	55
Caixa	1
Three	5
Netflix	2
Blockchain	1
DocuSign	1
DHL	1

CVEs with Recently Discovered Exploits

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

CVE, Title, Vendor	Description	CVSS v3.1 Base Score	Date Created	Date Updated
CVE-2020-1464 Microsoft Windows Spoofing Vulnerability Microsoft	A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files. In an attack scenario, an attacker could bypass security features intended to prevent improperly signed files from being loaded	CVSSv3BaseScore:5.3(AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)	08/17/2020	08/17/2020

CVE-2020-3382 Pi-hole Remote Code Execution Cisco	Pi-Hole is a DNS server specialized in content-filtering and is affected by a remote code execution vulnerability. An authenticated user of the Web portal can execute arbitrary commands with the underlying server with the privileges of the local user executing the service.	CVSSv3BaseScore:7.2(AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	07/30/2020	08/05/2020
CVE-2020-3187 Cisco ASA Software and FTD Software Web Services Path Traversal Vulnerability Cisco	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences.	CVSSv3BaseScore:9.1(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)	05/06/2020	07/29/2020

CVE-2020-3452 Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability Cisco	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	07/22/2020	07/29/2020
CVE-2020-1380 Microsoft Scripting Engine Memory Corruption Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine.	CVSSv3BaseScore:7.5(AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)	08/17/2020	08/17/2020

CVE-2020-3698 Qualcomm Out-Of-Bounds Memory Corruption Vulnerability Qualcomm	An Out of bound write happens in the component QoS DSCP when mapping due to improper input validation for data received from association response frame in Qualcomm Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music and Snapdragon Wearables	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/30/2020	07/30/2020
CVE-2020-1339 Microsoft Windows Media Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when Windows Media Audio Codec improperly handles objects. An attacker who successfully exploited the vulnerability could take control of an affected system. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit a malicious webpage.	CVSSv3BaseScore:7.3(AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N)	08/17/2020	08/17/2020