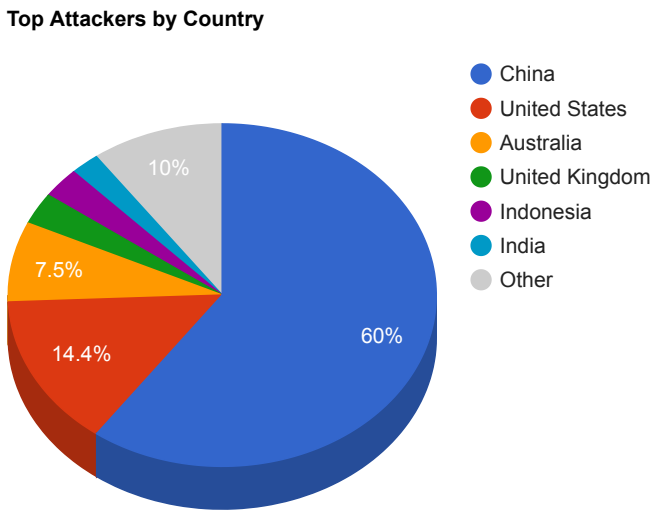
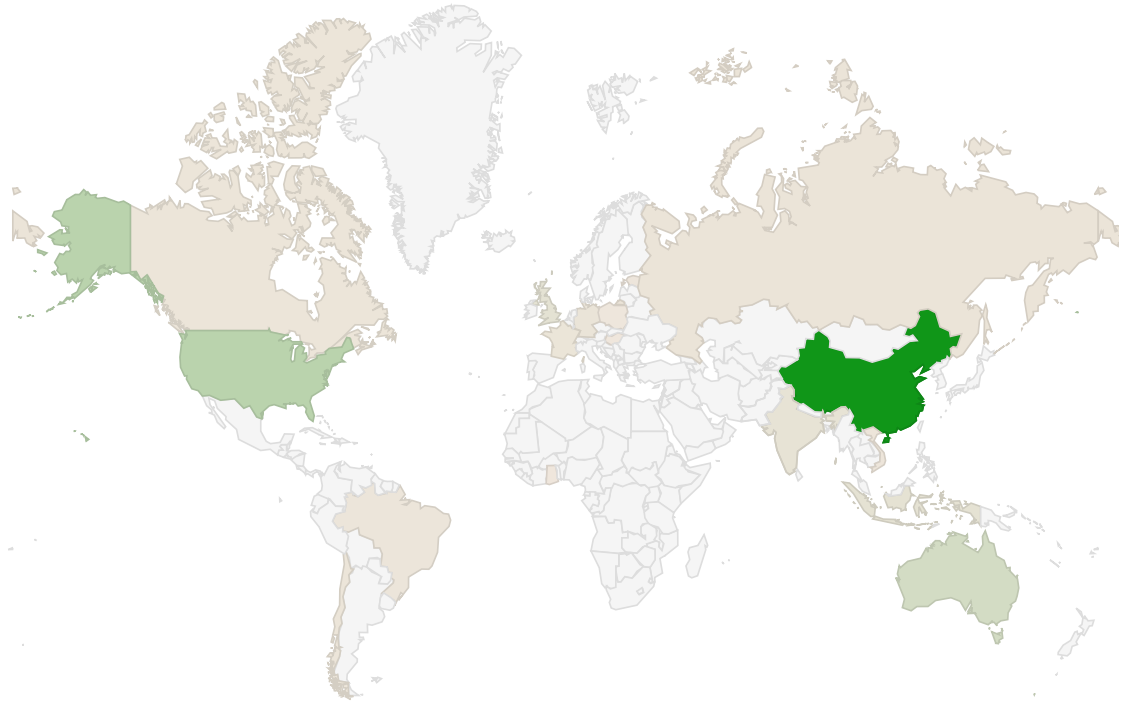
Trends

- The top attacker country was China with 217584 unique attackers (56.00%).
- The top Trojan C&C server detected was Heodo with 14 instances detected.
- The top phishing campaign detected was against Facebook accounts with 56 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	217584	56.00%
United States	52139	13.00%
Australia	27377	7.00%
United Kingdom	10912	2.00%
Indonesia	10431	2.00%
India	7976	2.00%
Germany	5143	1.00%
Russia	4940	1.00%
France	4485	1.00%
Canada	3963	1.00%
Chile	3941	1.00%
Brazil	3165	0%
Vietnam	2357	0%
Estonia	2179	0%
Seychelles	2105	0%
Hong Kong	1708	0%
Poland	1076	0%
Hungary	712	0%
Ghana	562	0%



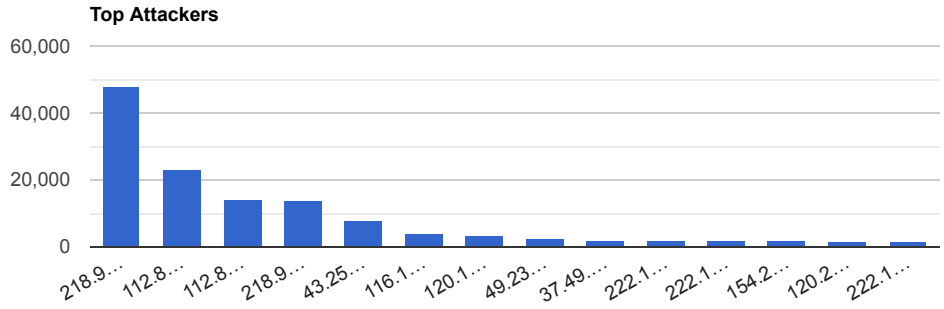


562 217,584

Top Attacking Hosts

Host	Occurrences
218.92.0.210	47670
112.85.42.187	22754
112.85.42.88	14160
218.92.0.190	13724

43.252.145.42	7863
116.153.32.211	3715
120.194.195.92	3218
49.232.170.155	2488
37.49.225.131	2179
222.186.169.194	1800
222.186.180.147	1753
154.220.96.130	1729
120.240.95.157	1702
222.186.175.167	1696



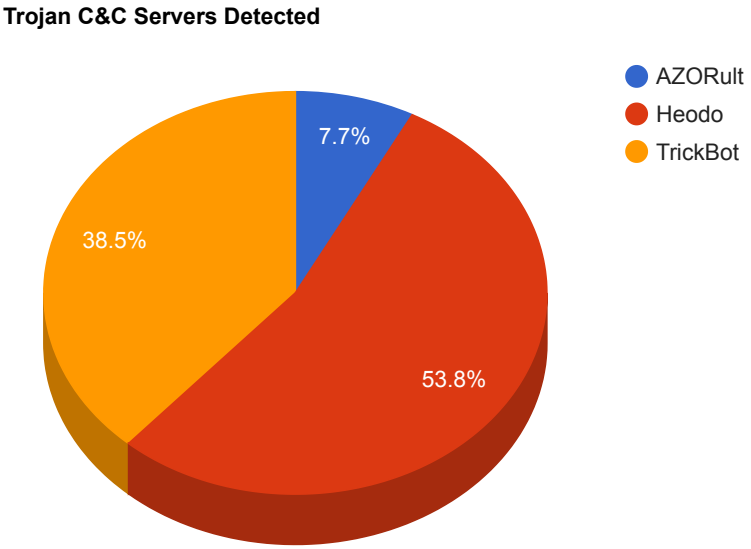
Top Network Attackers

ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
56233	Indonesia	ATSINDO-AS-ID PT Asia Teknologi Solusi, ID
24445	China	CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd, CN
45090	China	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
213371	Netherlands	SQUITTER-NETWORKS, NL
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN
133201	Hong Kong SAR China	COMING-AS ABCDE GROUP COMPANY LIMITED, HK
56040	China	CMNET-GUANGDONG-AP China Mobile communications corporation, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AZORult	2	104.28.24.76 , 68.66.200.213
Heodo	14	101.50.232.218 , 149.202.5.139 , 153.92.4.96 , 175.139.144.229 , 179.191.239.255 , 190.225.150.234 , 222.159.240.58 , 223.17.215.76 , 50.121.220.50 , 51.75.163.68 , 51.75.33.122 , 54.37.42.48 , 68.69.155.181 , 73.84.105.76

TrickBot	10	185.234.72.114 , 194.5.249.214 , 194.5.249.215 , 194.5.249.225 , 194.87.94.14 , 195.123.240.93 , 195.123.242.119 , 5.182.211.138 , 51.89.215.186 , 91.200.100.71



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201
adad179db8c67696ac24e9e11da2d075	https://www.virustotal.com/gui/file/7f9446709fbd77a21a806d17cf163ba00ce1a70f8b6af197990aa9924356fd36/details	FlashHelperServices.exe	FlashHelperService	W32.7F9446709F-100.SBX.VIOC

47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos

Top Phishing Campaigns

Phishing Target	Count
Other	1416
Facebook	56
Amazon.com	14
Microsoft	7
Apple	5
Yahoo	3
EE	3
Caixa	3
Google	2
Twitter	2
RuneScape	2
Vodafone	2
Adobe	1
Halifax	1
DocuSign	1
Virustotal	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-2020-1147 Pulse Connect Secure Arbitrary Code Injection Vulnerability Pulse Secure	A code injection vulnerability exists in Pulse Connect Secure that allows an attacker to crafted a URI to perform an arbitrary code execution via the admin web interface.	CVSSv3BaseScore:7.2(AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	07/14/2020	08/20/2020

CVE-2020-8913 Google Android Play Core Library Arbitrary Code Execution Vulnerability Google	A local, arbitrary code execution vulnerability exists in the SplitCompat.install endpoint in Android's Play Core Library. A malicious attacker could create an app which targets a specific application, and if a victim were to install this app, the attacker could perform a directory traversal, execute code as the targeted application and access the targeted application's data on the Android device.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	08/12/2020	08/31/2020
CVE-2020-2674 Oracle VM VirtualBox Arbitrary Code Execution Vulnerability Oracle	Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox.	CVSSv3BaseScore:8.2(AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)	01/15/2020	02/07/2020
CVE-2020-4589 IBM WebSphere Application Server Remote Code Execution Vulnerability IBM	IBM WebSphere Application Server could allow a remote attacker to execute arbitrary code on the system with a specially crafted sequence of serialized objects from untrusted sources.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	08/13/2020	08/21/2020

CVE-2020-3398 Cisco NX-OS Software Border Gateway Protocol Multicast VPN Session Denial of Service Vulnerability Cisco	A vulnerability in the Border Gateway Protocol (BGP) Multicast VPN (MVPN) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a BGP session to repeatedly reset, causing a partial denial of service condition due to the BGP session being down. The vulnerability is due to incorrect parsing of a specific type of BGP MVPN update message. An attacker could exploit this vulnerability by sending this BGP MVPN update message to a targeted device. A successful exploit could allow the attacker to cause the BGP peer connections to reset, which could lead to BGP route instability and impact traffic.	CVSSv3BaseScore:8.6(AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)	08/27/2020	09/03/2020