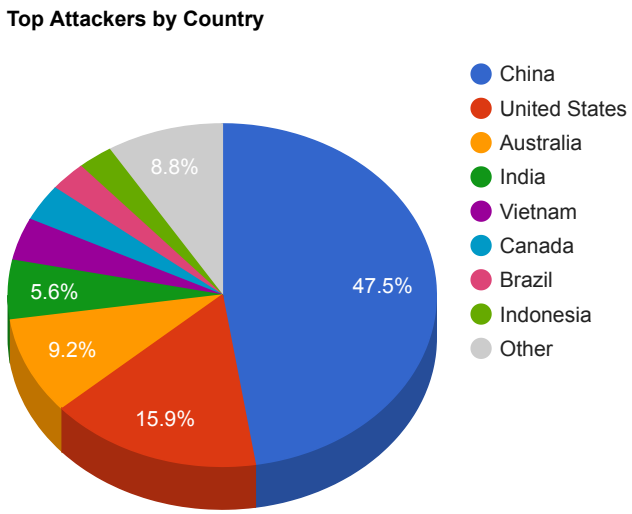
Trends

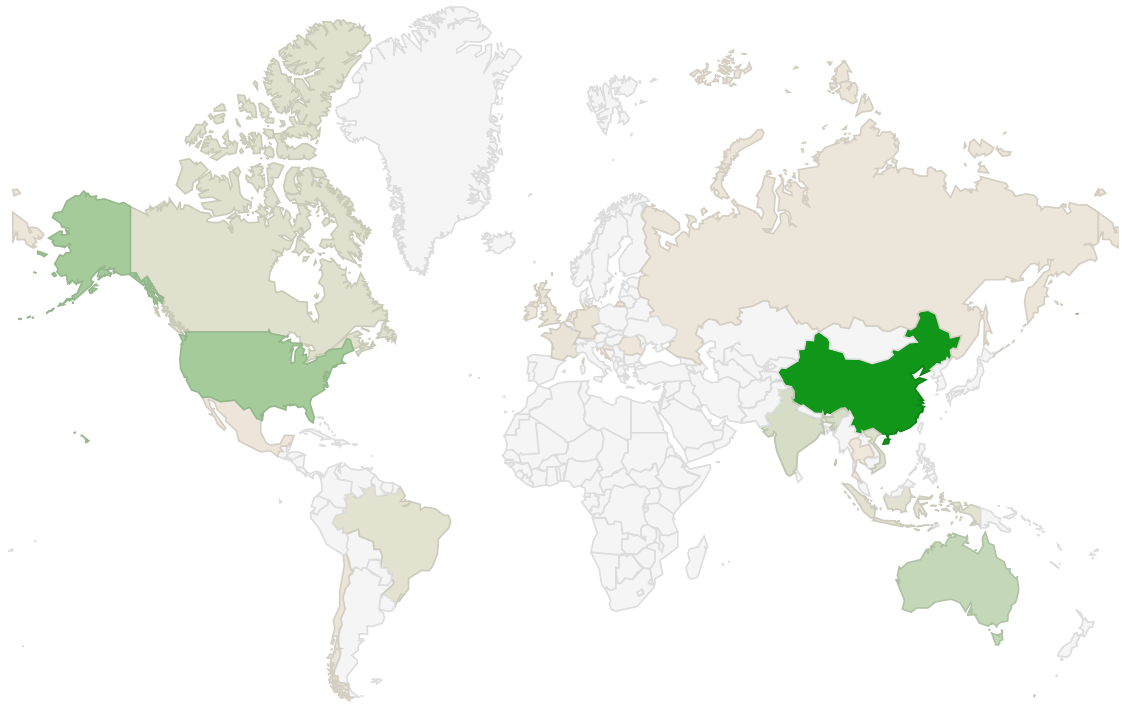
- The top attacker country was China with 105789 unique attackers (45.00%).
- The top Trojan C&C server detected was Heodo with 35 instances detected.
- The top phishing campaign detected was against Facebook accounts with 198 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	105789	45.00%
United States	35415	15.00%
Australia	20507	8.00%
India	12452	5.00%
Vietnam	8925	3.00%
Canada	7697	3.00%
Brazil	6195	2.00%
Indonesia	5896	2.00%
France	3806	1.00%
United Kingdom	3547	1.00%
Netherlands	2509	1.00%
Germany	2354	1.00%
Chile	2087	0%
Russia	2032	0%
Mexico	1188	0%
Romania	670	0%
Thailand	573	0%
Croatia	516	0%
Ireland	379	0%



Threat Geo-location

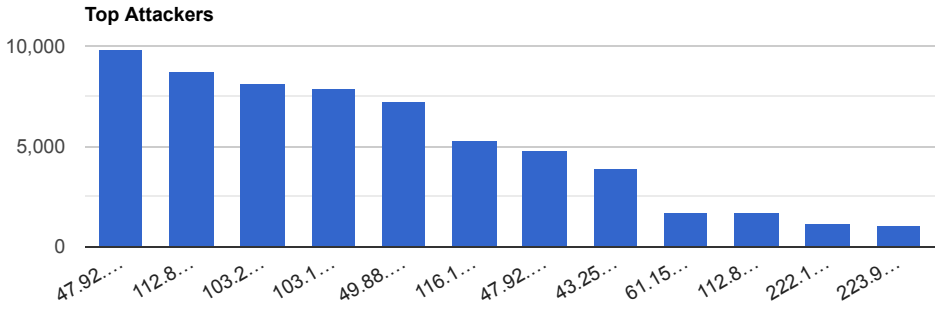


379 105,789

Top Attacking Hosts

Host	Occurrences
47.92.64.185	9864
112.85.42.88	8730

103.214.171.14	8157
103.141.177.175	7916
49.88.112.115	7232
116.153.32.212	5294
47.92.69.155	4792
43.252.145.42	3934
61.153.191.66	1738
112.85.42.187	1731
222.186.175.148	1140
223.99.14.18	1078



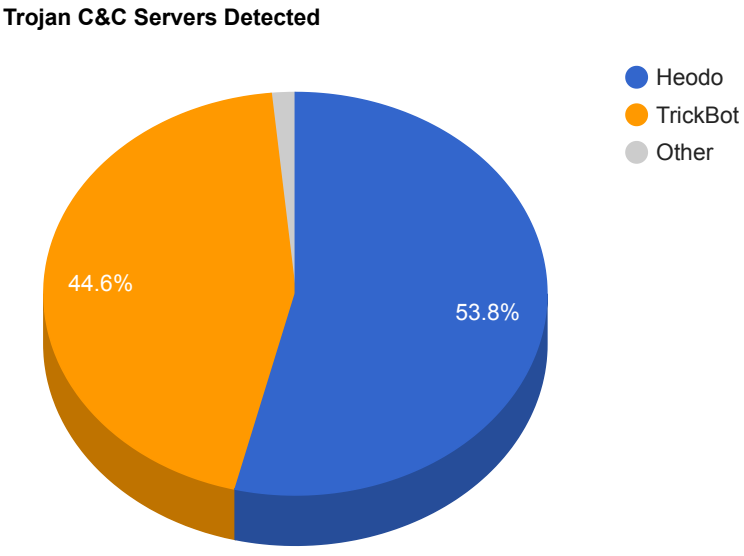
Top Network Attackers

ASN	Country	Name
37963	China	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
137443	Hong Kong SAR China	ANCHGLOBAL-AS-AP Anchnet Asia Limited, HK
63731	Vietnam	TPTECO-AS-VN TIEN PHAT TECHNOLOGY CORPORATION, VN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
56233	Indonesia	ATSINDO-AS-ID PT Asia Teknologi Solusi, ID
58461	China	CT-HANGZHOU-IDC No.288,Fu-chun Road, CN
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN
24444	China	CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location

Heodo	35	107.5.122.110 , 110.142.219.51 , 118.101.24.148 , 120.150.60.189 , 134.209.193.138 , 1.54.67.22 , 162.144.42.60 , 162.241.242.173 , 172.91.208.86 , 173.81.218.65 , 174.45.13.118 , 181.122.154.240 , 189.39.32.161 , 190.136.179.102 , 190.96.15.50 , 194.187.133.160 , 197.232.36.108 , 206.15.68.237 , 2.144.244.204 , 216.208.76.186 , 24.26.151.3 , 37.52.87.0 , 45.16.226.117 , 45.182.161.17 , 45.55.219.163 , 45.55.36.51 , 50.81.3.113 , 62.30.7.67 , 68.183.233.80 , 82.239.200.118 , 91.121.54.71 , 91.75.75.46 , 94.102.209.63 , 94.200.114.161 , 97.107.135.148
StealthWorker	1	91.240.118.79
TrickBot	29	104.161.32.108 , 107.155.137.18 , 129.232.133.39 , 139.60.163.45 , 176.31.28.85 , 185.172.129.100 , 185.180.198.58 , 185.234.72.240 , 185.99.2.106 , 194.5.249.221 , 194.87.236.171 , 195.123.240.52 , 195.123.241.175 , 195.123.241.224 , 195.123.241.229 , 195.123.241.68 , 37.220.6.122 , 37.220.6.126 , 45.138.158.33 , 45.138.158.41 , 5.182.211.124 , 51.83.196.234 , 51.89.204.242 , 82.146.37.128 , 85.143.221.85 , 85.204.116.117 , 91.200.100.85 , 93.189.42.225 , 95.171.15.71



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
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201
adad179db8c67696ac24e9e11da2d075	https://www.virustotal.com/gui/file/7f9446709fbd77a21a806d17cf163ba00ce1a70f8b6af1979990aa9924356fd36/details	FlashHelperServices.exe	FlashHelperService	W32.7F9446709F-100.SBX.VIOC
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos

Top Phishing Campaigns

Phishing Target	Count
Other	1579
Facebook	198
PayPal	20
Amazon.com	33
Virustotal	54
Allegro	5
Microsoft	9
Scotiabank	1
Steam	5
RuneScape	9
Americanas.com	1
Netflix	5
Alibaba.com	1
Adobe	8
Twitter	1
Google	3
Orange	1
Blockchain	1
Yahoo	1
LinkedIn	2

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 Microsoft Sharepoint Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the process responsible for deserialization of the XML content.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	07/14/2020	08/20/2020
CVE-2020-6519 Google Chrome Arbitrary Code Execution Vulnerability Google	Policy bypass in CSP in Google Chrome allowed a remote attacker to bypass content security policy via a crafted HTML page. It could allow attackers to bypass the Content Security Policy (CSP) on websites, in order to steal data and execute rogue code.	CVSSv3BaseScore:6.5(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)	07/22/2020	08/09/2020
CVE-2020-3506 Cisco IP Cameras Cisco Discovery Protocol Remote Code Execution and Denial of Service Vulnerabilities Cisco	Multiple vulnerabilities in the Cisco Discovery Protocol implementation for Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP camera. These vulnerabilities are due to missing checks when the IP cameras process a Cisco Discovery Protocol packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to the targeted IP camera.	CVSSv3BaseScore:8.8(V:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	08/26/2020	08/26/2020

CVE-2020-15858 Cinterion Java Modules Vulnerability Cinterion	This security vulnerability could potentially allow attackers with physical access to the device to compromise certain assets stored in the Cinterion modules' flash file system such as: Customer Java MIDlet byte code, TLS credentials or OTAP configuration data	CVSSv3BaseScore:6.2(AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L)	08/21/2020	08/24/2020
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	08/27/2020