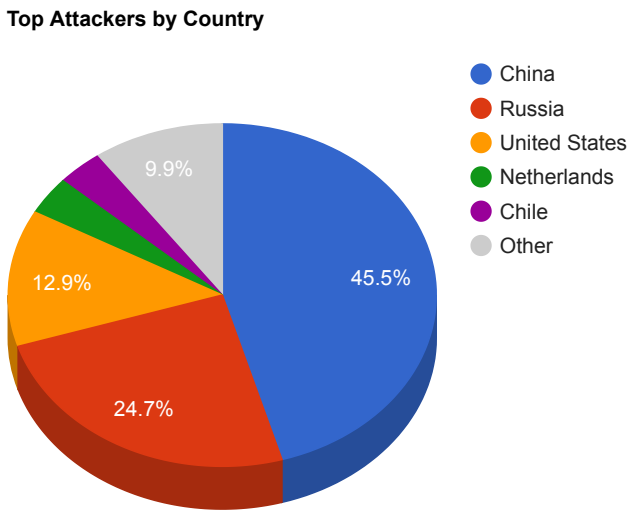
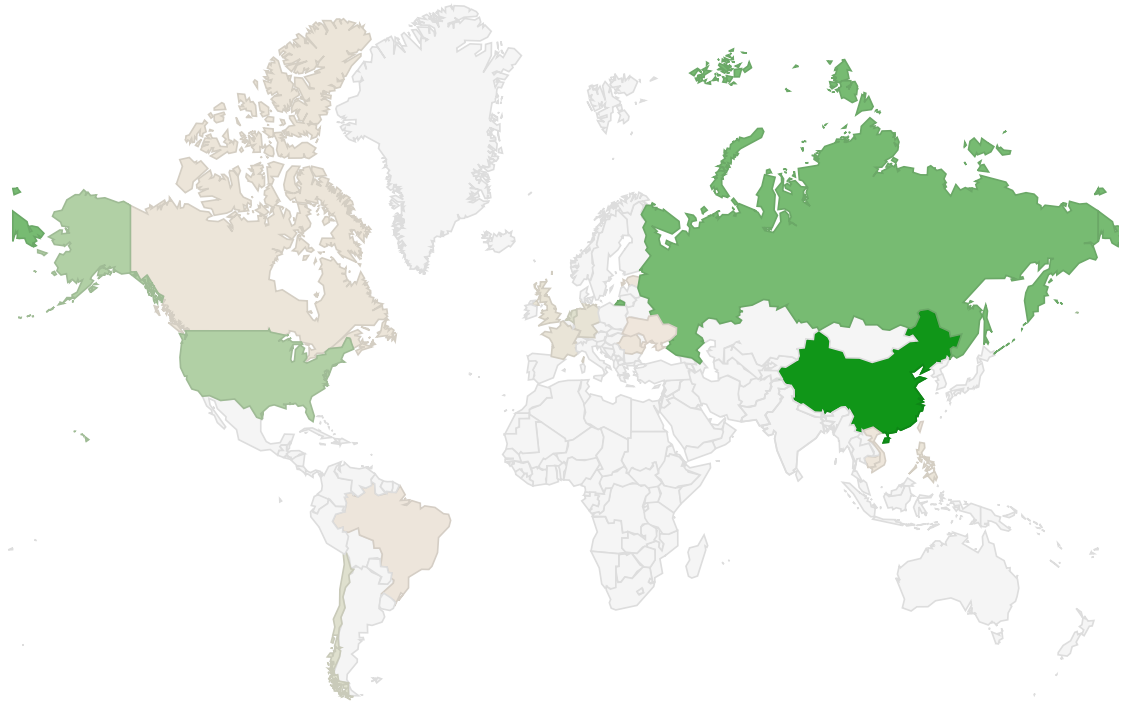
Trends

- The top attacker country was China with 299392 unique attackers (45.50%).
- The top Trojan C&C server detected was Heodo with 49 instances detected.
- The top phishing campaign detected was against Halifax accounts with 75 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	299392	45.50%
Russia	162190	24.65%
United States	84822	12.89%
Netherlands	23601	3.58%
Chile	22514	3.42%
Germany	11967	1.81%
United Kingdom	10025	1.52%
France	9616	1.46%
Philippines	6324	0.96%
Canada	5511	0.83%
Romania	4492	0.68%
Estonia	4136	0.62%
Brazil	3816	0.58%
Cambodia	3015	0.45%
Vietnam	2863	0.43%
Taiwan	2100	0.31%
Ukraine	1573	0.23%



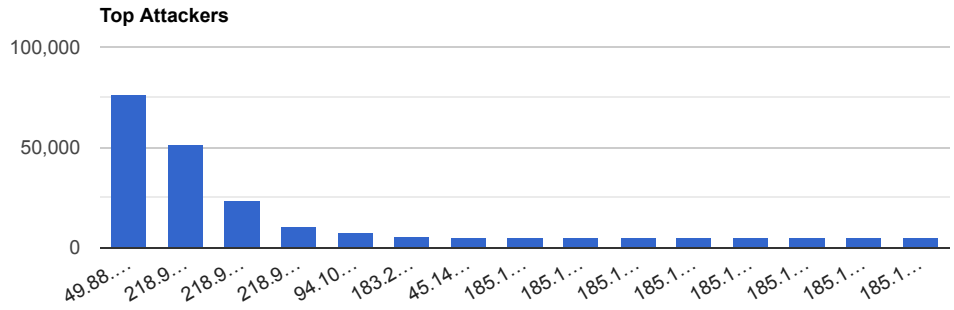


1,573 299,392

Top Attacking Hosts

Host	Occurrences
49.88.112.68	76423
218.92.0.204	51203
218.92.0.210	23201
218.92.0.190	10518
94.102.51.29	7622
183.201.252.68	5904
45.146.167.208	4855
185.193.90.222	4780

185.193.90.182	4768
185.193.90.38	4748
185.193.90.170	4733
185.193.90.246	4733
185.193.90.26	4700
185.193.90.226	4693
185.193.90.218	4685



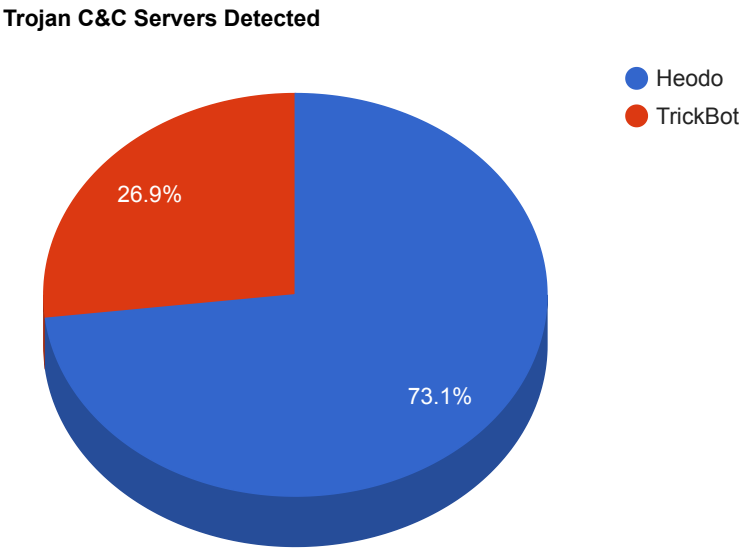
Top Network Attackers

ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
202425	Netherlands	INT-NETWORK, SC
132510	China	SHANXIMCC-IDC IDC ShanXi China Mobile communications corporation, CN
49505	Russia	SELECTEL, RU
204428	Netherlands	SS-NET, BG

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	49	103.236.179.162 , 104.161.32.111 , 109.190.249.106 , 167.114.153.111 , 169.50.76.149 , 172.86.186.21 , 175.143.12.123 , 177.23.7.151 , 183.176.82.231 , 184.180.181.202 , 186.222.250.115 , 188.157.101.114 , 188.166.220.180 , 189.223.16.99 , 190.108.228.27 , 190.117.101.56 , 190.164.135.81 , 190.190.219.184 , 192.175.111.214 , 200.127.14.97 , 208.180.207.205 , 209.54.13.14 , 213.52.74.198 , 218.147.193.146 , 24.232.228.233 , 2.45.176.233 , 37.179.145.105 , 42.200.96.63 , 45.89.127.140 , 45.89.127.182 , 45.89.127.92 , 46.105.114.137 , 47.154.85.229 , 47.36.140.164 , 49.50.209.131 , 5.2.72.199 , 5.89.33.136 , 61.33.119.226 , 69.206.132.149 , 74.135.120.91 , 74.214.230.200 , 75.143.247.51 , 76.171.227.238 , 79.118.74.90 , 81.215.230.173 , 86.104.194.30 , 94.212.52.40 , 95.85.33.23 , 96.245.227.43

TrickBot	18	104.161.32.112 , 107.174.254.216 , 131.153.22.145 , 148.251.27.76 , 185.117.73.50 , 185.125.46.53 , 194.5.249.241 , 194.5.250.113 , 195.123.237.37 , 198.8.91.44 , 212.80.217.69 , 37.228.117.217 , 45.141.103.31 , 46.30.42.239 , 5.101.51.112 , 85.204.116.204 , 86.104.194.102 , 93.189.43.168



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
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201

01a607b4d69c549629e6f0dfd3983956	https://www.virustotal.com/gui/file/1eef72aa566ba6c76b33f9d430d7233e358392382bfb3db81ca4f28d74f415a5/details	wupxarch.exe	N/A	W32.Auto:1eef72aa56.in03.Talos
88781be104a4dcb13846189a2b1ea055	https://www.virustotal.com/gui/file/1a8a17b615799f504d1e801b7b7f15476ee94d242affc103a4359c4eb5d9ad7f/details	UltraSearchApp	N/A	Win.Trojan.Generic::sso.talos

Top Phishing Campaigns

Phishing Target	Count
Other	1736
Facebook	22
Amazon.com	27
Instagram	2
DHL	1
Adobe	3
Three	1
Mastercard	25
Microsoft	4
PayPal	6
Bradesco	1
Halifax	75
Netflix	6
Google	8
Alibaba.com	2
RuneScape	2
Apple	1
Virustotal	5

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-2020-16898 Microsoft Windows TCP/IP Stack Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	10/16/2020	10/16/2020
CVE-2020-1472 Microsoft Netlogon Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	08/17/2020	10/05/2020

CVE-2020-3452 Cisco ASA and FTD 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	10/12/2020
CVE-2020-13943 Apache Tomcat Unexpected Resource Response Vulnerability Apache	If an HTTP/2 client exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.	CVSSv3BaseScore:5.3(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	10/12/2020	10/16/2020

CVE-2020-9746 Adobe Flash Player Arbitrary Code Execution Vulnerability Adobe	Adobe Flash Player is affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution. Exploitation of this issue requires an attacker to insert malicious strings in an HTTP response that is by default delivered over TLS/SSL.	CVSSv3BaseScore:7.0(AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)	10/14/2020	10/14/2020
CVE-2020-16951 Microsoft SharePoint Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account. Exploitation of this vulnerability requires that a user uploads a specially crafted SharePoint application package to an affected version of SharePoint.	CVSSv3BaseScore:8.6(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L)	10/16/2020	10/16/2020