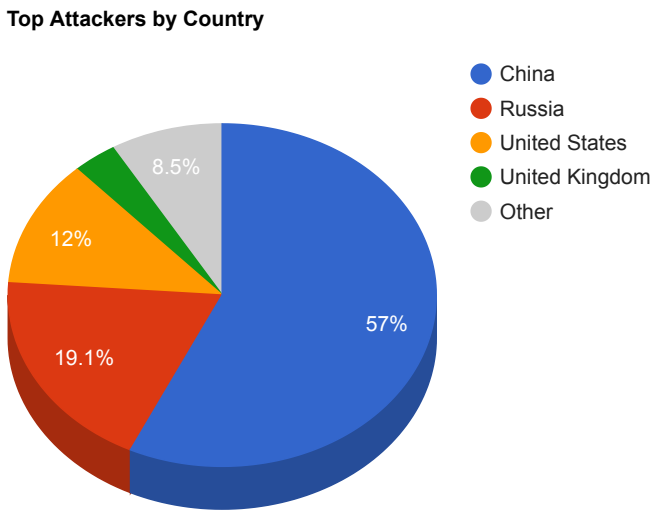
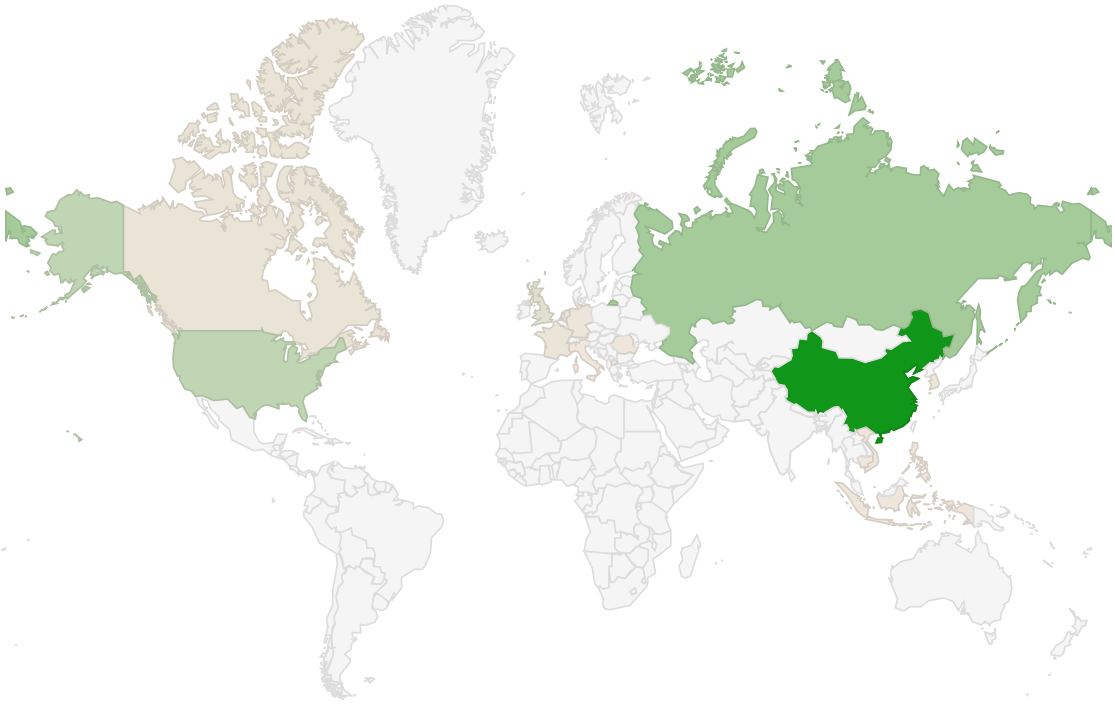
Trends

- The top attacker country was China with 374452 unique attackers (57.04%).
- The top Trojan C&C server detected was TrickBot with 21 instances detected.
- The top phishing campaign detected was against Halifax accounts with 62 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	374452	57.04%
Russia	125315	19.09%
United_States	78703	11.99%
United_Kingdom	21911	3.33%
Netherlands	12894	1.96%
Canada	9506	1.44%
France	8018	1.22%
Germany	6315	0.96%
South_Korea	4911	0.74%
Vietnam	3450	0.52%
Indonesia	3155	0.48%
Romania	2027	0.30%
Cambodia	1463	0.22%
Singapore	1311	0.19%
Italy	1306	0.19%
Philippines	937	0.14%
Macedonia	713	0.10%



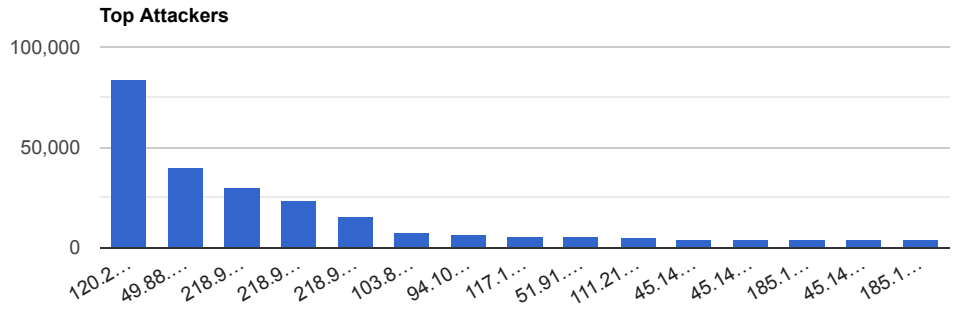


713 374,452

Top Attacking Hosts

Host	Occurrences
120.210.208.137	83620
49.88.112.68	39687
218.92.0.204	30129
218.92.0.190	23540
218.92.0.210	15690
103.85.25.227	7369
94.102.51.95	6131
117.185.95.122	5846

51.91.116.150	5525
111.21.208.204	4608
45.146.167.219	3919
45.146.167.183	3914
185.193.90.182	3906
45.146.167.201	3891
185.193.90.38	3864

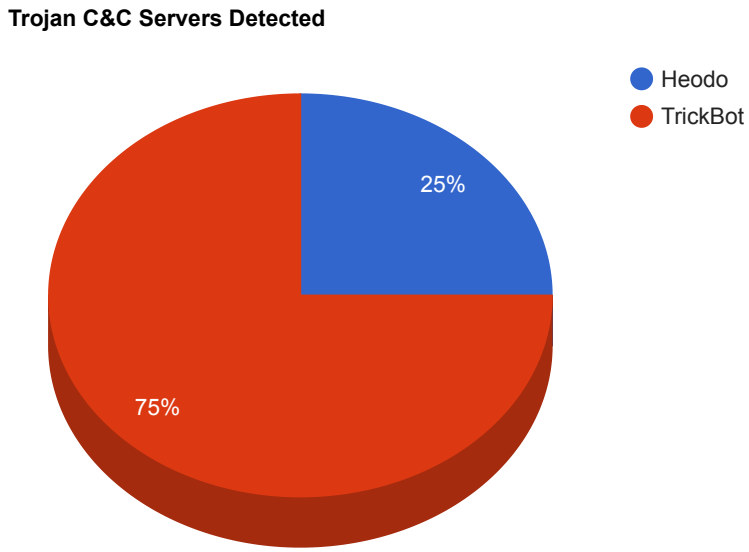


Top Network Attackers

ASN	Country	Name
9808		CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
4134		CHINANET-BACKBONE No.31,Jin-rong Street, CN
134835		SNL-HK Starry Network Limited, HK
202425	Netherlands	INT-NETWORK, SC
24400		CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd., CN
16276		OVH, FR
49505		SELECTEL, RU
204428		SS-NET, BG

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	7	120.150.218.241 , 162.241.140.129 , 186.74.215.34 , 191.191.23.135 , 192.232.229.54 , 46.101.58.37 , 72.143.73.234
TrickBot	21	185.117.73.190 , 185.14.30.247 , 185.99.2.176 , 194.5.249.126 , 194.5.249.136 , 194.5.249.216 , 194.5.249.224 , 195.123.240.130 , 35.164.230.208 , 37.220.6.115 , 45.89.127.118 , 45.89.127.119 , 45.89.127.128 , 51.77.112.255 , 51.89.177.8 , 62.108.35.29 , 62.108.35.36 , 80.85.156.116 , 82.146.54.254 , 85.99.2.140 , 92.242.40.12



29e6f0dfd3983956	0d7233e358392382bfb3db81ca4f28d74f415a5/details	wupxarch.exe	N/A	6.in03.Talos
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
88781be104a4dcb13846189a2b1ea055	https://www.virustotal.com/gui/file/1a8a17b615799f504d1e801b7b7f15476ee94d242affc103a4359c4eb5d9ad7f/details	UltraSearchApp	N/A	Win.Trojan.Generic::sso.talos

Top Phishing Campaigns

Phishing Target	Count
Halifax	62
Other	1417
PayPal	37
Facebook	34

Virustotal	26
Amazon.com	33
DocuSign	1
Microsoft	16
Apple	1
Bradesco	3
Orange	2
Instagram	2
Special	2
VKontakte	1
DHL	4
Three	3
Netflix	3
Adobe	1
RuneScape	3
Google	4
Steam	1
Vodafone	3
Caixa	2
Binance	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-2020-1350 Microsoft Windows DNS Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	07/14/2020	07/23/2020

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-2020-0688 Microsoft Exchange Validation Key Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time. Knowledge of a the validation key allows an authenticated user with a mailbox to pass arbitrary objects to be deserialized by the web application, which runs as SYSTEM.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	02/11/2020	02/20/2020