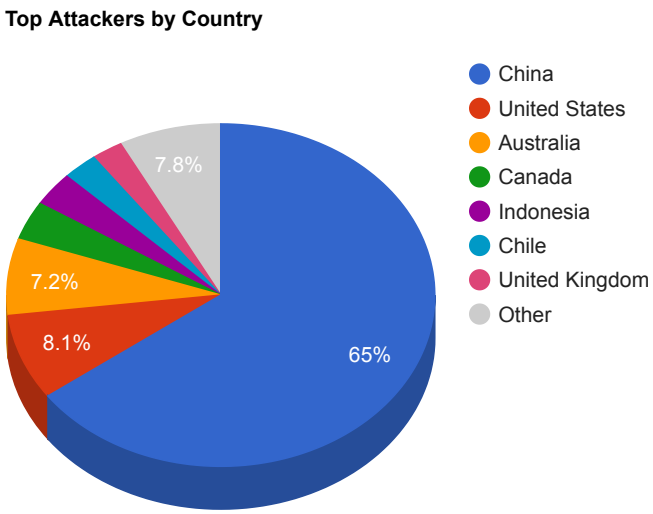
Trends

- The top attacker country was China with 491021 unique attackers (62.00%).
- The top Trojan C&C server detected was TrickBot with 57 instances detected.
- The top phishing campaign detected was against Facebook with 108 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	491021	62.00%
United States	61407	7.00%
Australia	54500	6.00%
Canada	27789	3.00%
Indonesia	24427	3.00%
Chile	20152	2.00%
United Kingdom	17918	2.00%
Russia	11222	1.00%
France	10373	1.00%
Brazil	7831	1.00%
Vietnam	4485	0%
India	4272	0%
Taiwan	4246	0%
Hong Kong	3946	0%
Germany	2860	0%
Netherlands	2765	0%
Italy	2662	0%
Spain	2176	0%
Romania	1761	0%



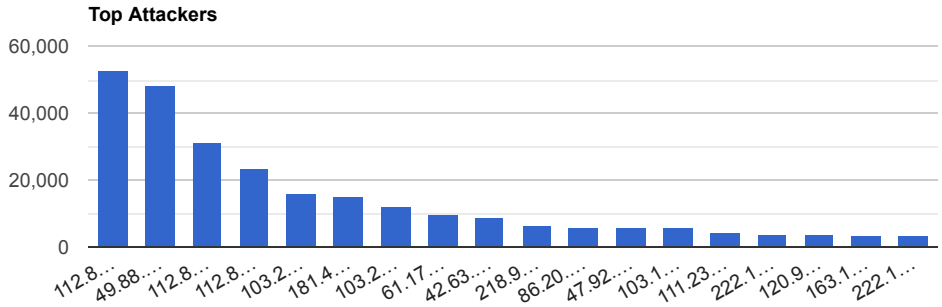
Threat Geo-location

1,761 491,021

Top Attacking Hosts

Host	Occurrences
112.85.42.187	52656
49.88.112.115	48193
112.85.42.88	31360
112.85.42.189	23573

103.253.2.185	16095
103.24.177.99	12336
61.177.172.13	9944
42.63.14.194	8800
218.92.0.190	6454
47.92.64.185	6046
103.108.242.26	5801
111.230.40.195	4164
222.186.173.154	4128
120.92.159.83	3764
163.172.75.41	3636
222.186.175.215	3549



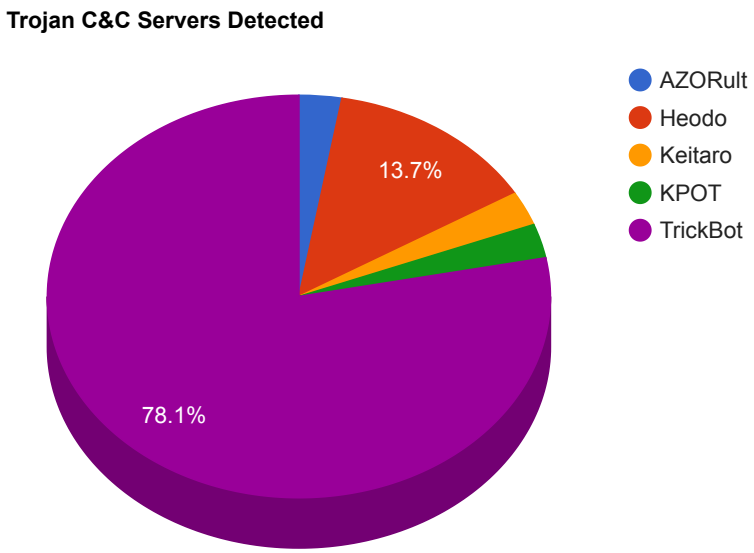
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
59139	Indonesia	WIFIKU-AS-ID PT Wifiku Indonesia, ID
59072	China	ESINNET Shenzhen ESIN Technology Co., Ltd, CN
5089	United Kingdom	NTL, GB

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AZORult	2	185.183.98.244 , 38.117.105.162
Heodo	10	114.173.201.110 , 116.125.120.88 , 145.236.8.174 , 157.147.76.151 , 190.190.148.27 , 190.31.53.131 , 204.197.146.48 , 47.146.32.175 , 72.12.127.184 , 97.104.107.190
Keitaro	2	88.119.171.152 , 88.119.171.153
KPOT	2	5.101.51.51 , 84.38.183.121

TrickBot	57	103.130.114.106 , 103.221.254.102 , 103.36.48.103 , 103.87.169.150 , 107.174.196.242 , 110.232.249.13 , 112.109.19.178 , 121.101.185.130 , 158.181.155.153 , 162.216.0.189 , 162.244.32.198 , 177.190.69.162 , 180.211.170.214 , 180.211.95.14 , 183.81.154.113 , 185.164.32.214 , 185.164.32.215 , 185.205.209.241 , 186.159.8.218 , 187.109.119.99 , 192.52.167.104 , 194.5.249.174 , 194.5.249.193 , 195.123.240.252 , 195.123.241.187 , 195.123.241.90 , 195.123.241.94 , 198.46.198.139 , 200.116.159.183 , 200.116.232.186 , 212.22.70.65 , 217.12.209.54 , 220.247.174.12 , 23.92.93.230 , 27.147.173.227 , 36.94.33.102 , 37.220.6.108 , 45.127.222.8 , 45.138.158.32 , 45.148.120.195 , 46.30.41.160 , 51.210.135.34 , 5.149.253.99 , 51.83.165.31 , 51.89.177.20 , 51.89.177.9 , 51.89.202.103 , 5.34.178.126 , 62.108.35.194 , 62.108.35.9 , 64.44.133.137 , 82.146.46.220 , 86.104.194.113 , 86.104.194.116 , 88.247.212.56 , 91.200.102.149 , 92.62.65.163



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name

f0fdc17674950a4eaa4bbaafce5007f6	https://www.virustotal.com/gui/file/e66d6d13096ec9a62f5c5489d73c0d1dd113ea466850202107530349 5fd9ff82/details	FlashHelperServices.exe	FlashHelperService	W32.Auto:e66d6d1309.in03.Talos
73d1de319c7d61e0333471c82f2fc104	https://www.virustotal.com/gui/file/32155b070c7e1b9d6bdc021778c5129edfb9cf7e330b8f07bb140dedb5c9aae7/details	SAntivirusService.exe	SAService	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**
RuneScape	6
Facebook	108
Other	1703
Microsoft	4
Three	6
Allegro	1
Amazon.com	14
PayPal	15
Itau	2
Americanas.com	1
Netflix	4
UniCredit	2
DHL	1
EE	4

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-2020-3382 Cisco Data Center Network Manager Authentication Bypass Vulnerability Cisco	The vulnerability is due to insufficient validation of user input on the web management interface. An attacker could exploit this vulnerability by submitting a malicious request to an affected system. An exploit could allow the attacker to gain administrative-level privileges on the system. The attacker needs a valid username to exploit this vulnerability.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/30/2020	08/05/2020
CVE-2020-10713 GRUB2 bootloader Buffer Overflow Vulnerability Multi-Vendor	A flaw was found in grub2, where an attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	CVSSv3BaseScore:6.7(AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	07/30/2020	08/08/2020

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-2020-8163 Ruby On Rails Remote Code Execution Vulnerability Ruby On Rails	The is a code injection vulnerability that would allow an attacker who controlled the "locals" argument of a "render" call to perform a remote code execution vulnerability.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	07/02/2020	07/27/2020
CVE-2020-4534 IBM WebSphere Application Server Remote Code Execution Vulnerability IBM	IBM WebSphere Application Server could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges.	CVSSv3BaseScore:8.8(AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)	08/03/2020	08/04/2020
CVE-2020-8607 Trend Micro Rootkit Driver Input Validation Vulnerability Trend Micro	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability.	CVSSv3BaseScore:6.7(AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	08/05/2020	08/05/2020

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 (ChipSoftware).	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