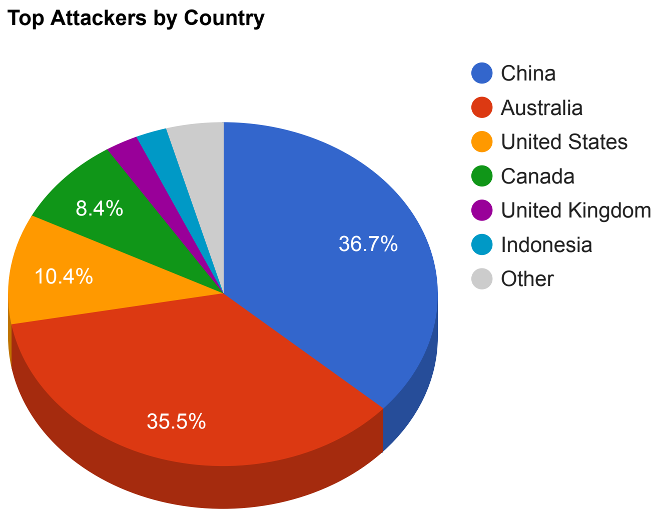
Trends

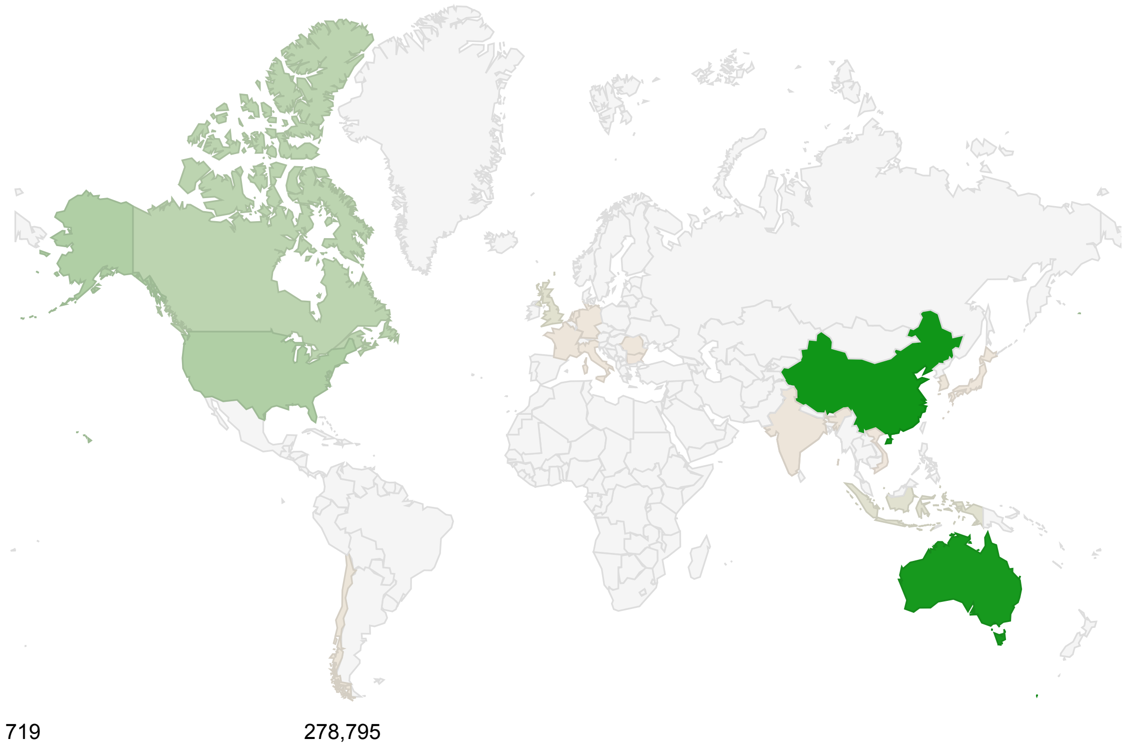
- The top attacker country was China with 278795 unique attackers (35.00%).
- The top Trojan C&C server detected was TrickBot with 15 instances detected.
- The top phishing campaign detected was against Facebook accounts with 65 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	278795	35.00%
Australia	269750	34.00%
United States	79002	10.00%
Canada	63771	8.00%
United Kingdom	18677	2.00%
Indonesia	17761	2.00%
Hong Kong	4963	0%
South Korea	4854	0%
Chile	4334	0%
France	3275	0%
Netherlands	3063	0%
India	3055	0%
Japan	2188	0%
Italy	1959	0%
Germany	1793	0%
Romania	1507	0%
Vietnam	1217	0%
Bulgaria	719	0%



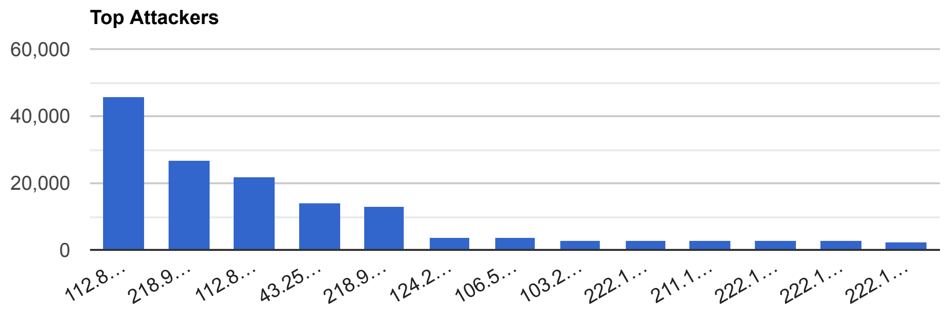
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
112.85.42.187	45782
218.92.0.210	26722

112.85.42.88	21710
43.252.145.42	13990
218.92.0.190	13003
124.225.208.9	4104
106.52.153.230	4055
103.218.242.80	3064
222.186.169.192	2937
211.104.20.145	2890
222.186.180.147	2767
222.186.175.216	2687
222.186.175.154	2650



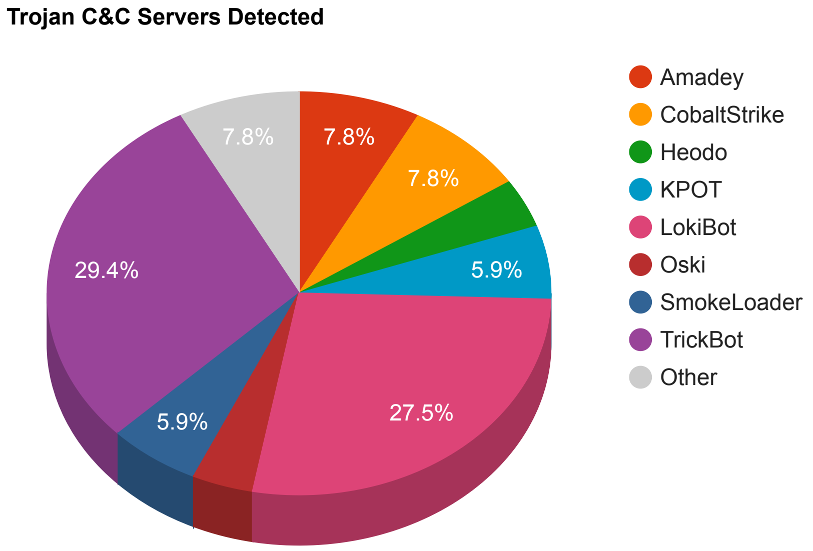
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
56233	Indonesia	ATSINDO-AS-ID PT Asia Teknologi Solusi, ID
45090	China	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
135377	Hong Kong SAR China	UHGL-AS-AP UCloud (HK) Holdings Group Limited, HK
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN
4766	South Korea	KIXS-AS-KR Korea Telecom, KR

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	45.141.84.146
Amadey	4	104.27.174.136 , 172.67.211.220 , 217.8.117.102 , 217.8.117.112
CobaltStrike	4	45.141.84.212 , 45.141.84.233 , 45.141.84.241 , 45.141.84.49
Heodo	2	185.178.10.77 , 219.74.18.66
Keitaro	1	45.141.84.197
KPOT	3	194.180.224.129 , 46.17.98.128 , 78.142.29.185

Lokibot	14	103.253.212.225 , 103.27.62.62 , 142.11.195.130 , 192.185.185.16 , 192.236.199.171 , 193.142.59.80 , 195.22.153.121 , 195.69.140.147 , 40.71.100.104 , 45.143.138.128 , 5.56.134.77 , 79.124.8.8 , 95.181.172.13 , 95.181.172.13
Nexus	1	162.213.253.54
Oski	2	188.127.249.228 , 194.87.237.143
SmokeLoader	3	148.251.72.21 , 95.215.108.15 , vot552.com
TrickBot	15	185.172.129.67 , 188.225.9.82 , 195.123.240.196 , 195.123.241.124 , 195.123.241.134 , 195.123.241.194 , 195.123.241.58 , 23.95.8.136 , 37.220.6.101 , 37.220.6.98 , 85.143.221.6 , 85.204.116.158 , 91.200.103.111 , 93.189.43.80 , 93.189.46.41
Uadmin	1	45.11.19.246


Trojan C&C Servers Detected

Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
adad179db8c67696ac24e9e11da2d075	https://www.virustotal.com/gui/file/7f9446709fbd77a21a806d17cf163ba00ce1a70f8b6af197990aa9924356fd36/details	FlashHelperServices.exe	FlashHelperService	W32.7F9446709F-100.SBX.VIOC

73d1de319c7d61e0333471c82f2fc104	https://www.virustotal.com/gui/file/32155b070c7e1b9d6bdc021778c5129edfb9cf7e330b8f07bb140dedb5c9aae7/details	SAntivirusService.exe	AntivirusService	Win.Dropper.Segurazo::tpd
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg

Top Phishing Campaigns

Phishing Target	Count
Other	1640
Facebook	65
PayPal	13
Amazon.com	12
Google	8
Microsoft	8
Virustotal	8
RuneScape	4
Adobe	3
ZML	2
Apple	2
Three	2
Halifax	2
AT&T	1
Vodafone	1
Orange	1
Caixa	1
Netflix	1
Instagram	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-2020-3495 Cisco Jabber for Windows Message Handling Arbitrary Code Execution Vulnerability Cisco	A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code. The vulnerability is due to improper validation of message contents. An attacker could exploit this vulnerability by sending specially crafted Extensible Messaging and Presence Protocol messages to the affected software. A successful exploit could allow the attacker to cause the application to execute arbitrary programs on the targeted system with the privileges of the user account that is running the Cisco Jabber client software, possibly resulting in arbitrary code execution.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	09/03/2020	09/09/2020
CVE-2020-0986 Microsoft Windows Kernel Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application to take control of an affected system.	CVSSv3BaseScore:7.8(V:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/12/2020

CVE-2020-9715 Adobe Reader and Acrobat Arbitrary Code Execution Vulnerability Adobe	Adobe Reader and Acrobat are applications for handling PDF files. Adobe Reader and Acrobat have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. An attacker could exploit this vulnerability to compromise Confidentiality, Integrity and/or Availability.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	08/19/2020	08/19/2020
CVE-2020-17496 vBulletin Remote Code Execution Vulnerability vBulletin	vBulletin allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request. vBulletin is vulnerable to a remote code execution vulnerability caused by incomplete patching of the previous "CVE-2019-16759" remote code execution vulnerability.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	08/12/2020	08/17/2020
CVE-2020-8218 Pulse Connect Secure Arbitrary Code Execution Vulnerability PulseSecure	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)	07/30/2020	09/01/2020

CVE-2020-1247 Microsoft Win32k Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	CVSSv3BaseScore:7.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/11/2020
CVE-2020-3398 PAN-OS Management Interface Command Injection Vulnerability PAN-OS	An OS Command Injection vulnerability exists in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue affects some unknown processing of the component Management Interface. The manipulation with an unknown input leads to a privilege escalation vulnerability.	CVSSv3BaseScore:7.2(V:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	08/27/2020	09/03/2020