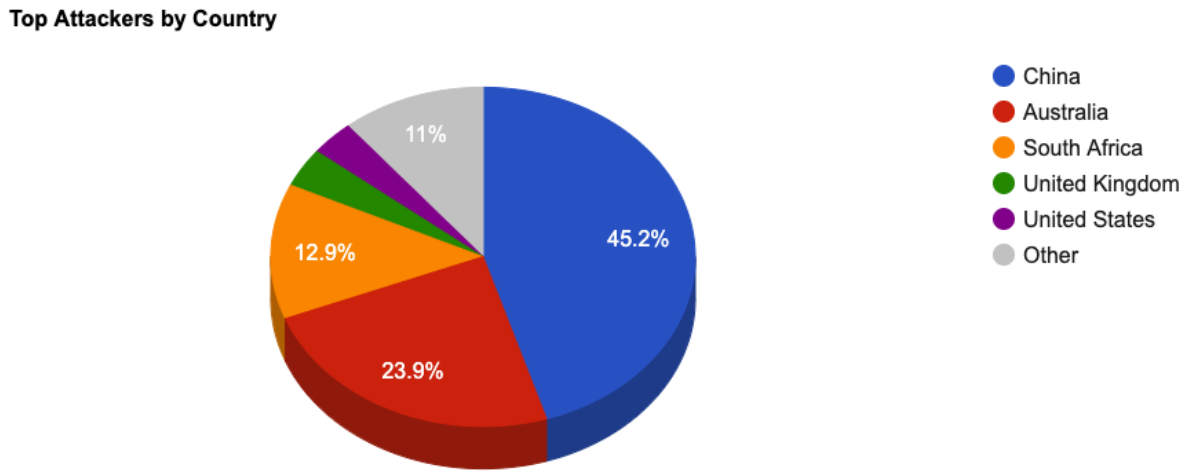
Trends

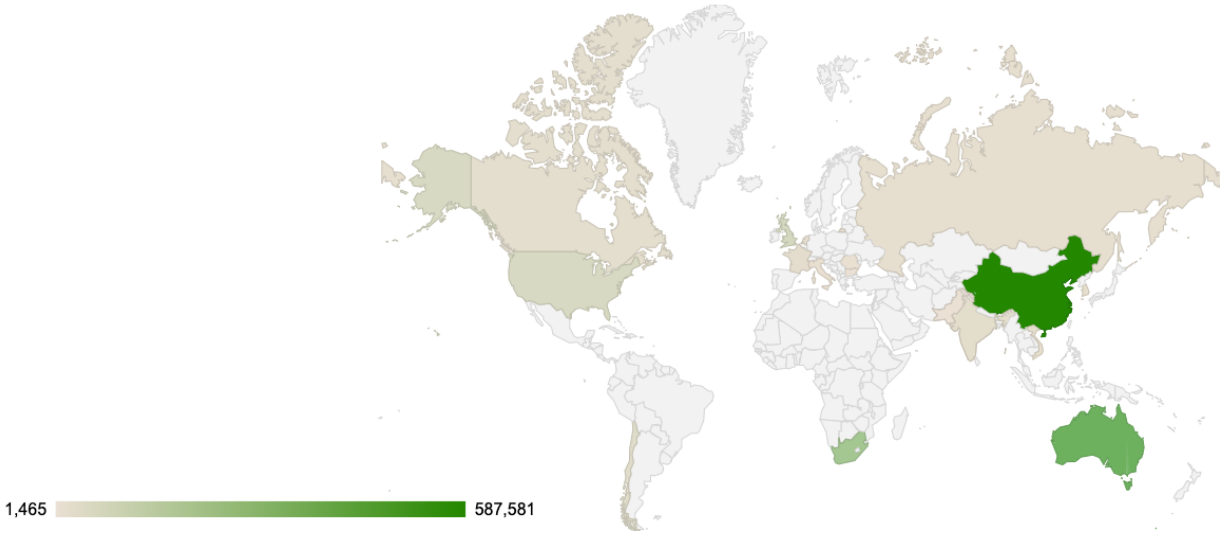
- The top attacker country was China with 587581 unique attackers (44.00%).
- The top Trojan C&C server detected was TrickBot with 34 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	587581	44.00%
Australia	310634	23.00%
South Africa	167513	12.00%
United Kingdom	48487	3.00%
United States	43648	3.00%
Chile	25487	1.00%
India	18271	1.00%
Canada	16057	1.00%
France	13621	1.00%
Hong Kong	12844	0%
South Korea	12146	0%
Vietnam	12016	0%
Russia	11610	0%
Netherlands	8125	0%
Italy	6047	0%
Romania	3284	0%
Bulgaria	1866	0%
Pakistan	1465	0%



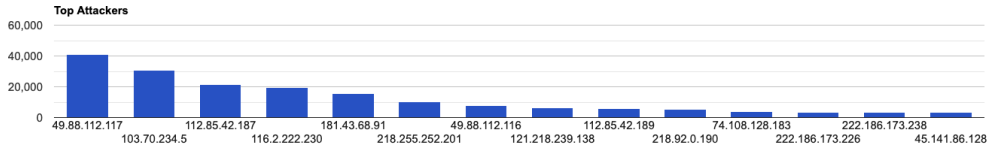
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
49.88.112.117	41144
103.70.234.5	30560
112.85.42.187	21533
116.2.222.230	19271
181.43.68.91	15696
218.255.252.201	10170
49.88.112.116	7975
121.218.239.138	6218
112.85.42.189	5981
218.92.0.190	5234
74.108.128.183	4102
222.186.173.226	3492

222.186.173.238	3448
45.141.86.128	3434



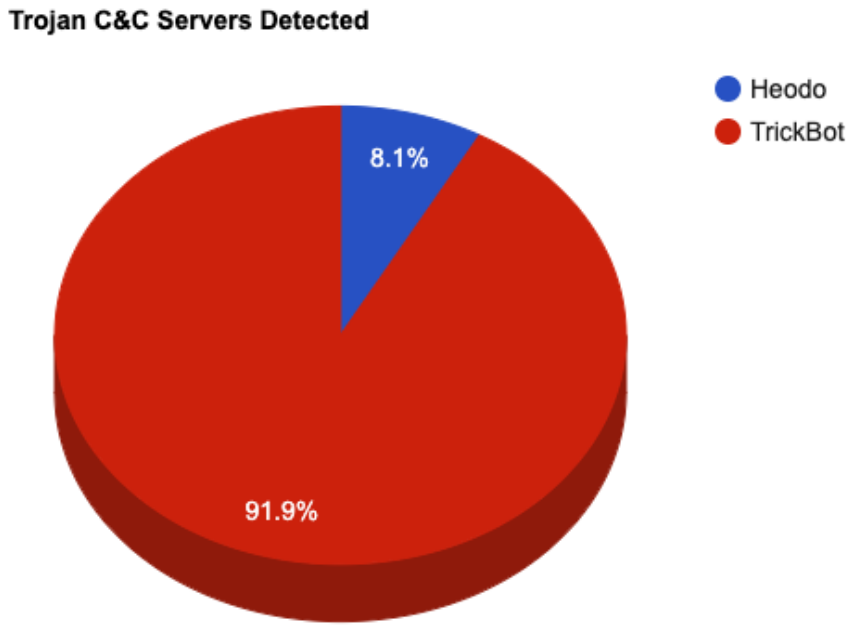
Top Network Attackers

ASN	Country	Name
9381	Hong Kong SAR China	HKBNES-AS-AP HKBN Enterprise Solutions HK Limited, HK
1221	Australia	ASN-TELSTRA Telstra Corporation Ltd, AU
701	United States	UUNET, US

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	3	170.81.48.2 , 46.30.175.11 , 70.48.238.90

TrickBot	34	103.5.231.188 , 107.155.137.23 , 110.232.76.39 , 110.93.15.98 , 122.50.6.122 , 176.119.159.147 , 178.156.202.251 , 185.141.61.101 , 185.14.30.45 , 185.99.2.142 , 185.99.2.152 , 185.99.2.68 , 188.119.113.114 , 190.136.178.52 , 194.5.250.46 , 194.5.250.47 , 194.5.250.69 , 200.171.101.169 , 217.12.209.170 , 217.12.209.244 , 31.131.26.31 , 36.91.45.10 , 45.153.185.187 , 45.6.16.68 , 5.1.74.124 , 51.89.115.121 , 5.196.247.14 , 79.137.101.2 , 85.204.116.191 , 85.204.116.195 , 85.204.116.57 , 91.200.100.84 , 93.189.42.81 , 96.9.77.56



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
5d34464531ddbdc7b0a4dba5b4c1cfea	https://www.virustotal.com/gui/file/a545df34334b39522b9cc8cc0c11a1591e016539b209ca1d4ab8626d70a54776/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::in03.talos
bf1d79fad6471fcf50e38a9ea1f646a5	https://www.virustotal.com/gui/file/589d9977a5b0420d29acc0c1968a2ff48102ac3ddc0a1f3188be79d0a4949c82/details	wupxarch.exe	N/A	W32.Auto:589d99.in03.Talos
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos

9b47b9f19455bf56138ddb81c93b6c0c	https://www.virustotal.com/gui/file/518a8844dae953d7f2510d38ba916f1c4ccc01cfba58f69290938b6ddde8b472/details	updateprofile.exe	N/A	Win.Dropper.Generic::tpd
c2406fc0fce67ae79e625013325e2a68	https://www.virustotal.com/gui/file/1c3ed460a7f78a43bab0ae575056d00c629f35cf7e72443b4e874ede0f305871/details	SegurazoIC.exe	SegurazoIC	PUA.Win.Adware.Ursu::95.sbx.tg

CVEs with Recently Discovered Exploits

This is a list of recent vulnerabilities for which exploits are available.

CVE, Title, Vendor	Description	CVSS v2 Base Score	Date Created	Date Updated
CVE-2020-0760 Microsoft Office Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when Microsoft Office improperly loads arbitrary type libraries. An attacker could then install programs	view,change,ordeletedata	04/15/2020	04/17/2020
CVE-2020-1027 Microsoft Windows Kernel Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/15/2020	04/15/2020

CVE-2020-1020 Microsoft Adobe Font Manager Library Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/15/2020	04/15/2020
CVE-2020-0687 Microsoft Graphics Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/15/2020	04/17/2020

CVE-2019-1381 Microsoft Windows Information Disclosure Vulnerability Microsoft	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations. An attacker who successfully exploited the vulnerability could potentially access unauthorized files.	CVSSv3BaseScore:9.9(AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)	11/12/2019	11/14/2019
CVE-2020-0968 Microsoft Scripting Engine Memory Corruption Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.	CVSSv3BaseScore:7.5(AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/15/2020	04/17/2020

CVE-2020-0939 Microsoft Media Foundation Information Disclosure Vulnerability Microsoft	An information disclosure vulnerability exists when Media Foundation improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/15/2020	04/15/2020