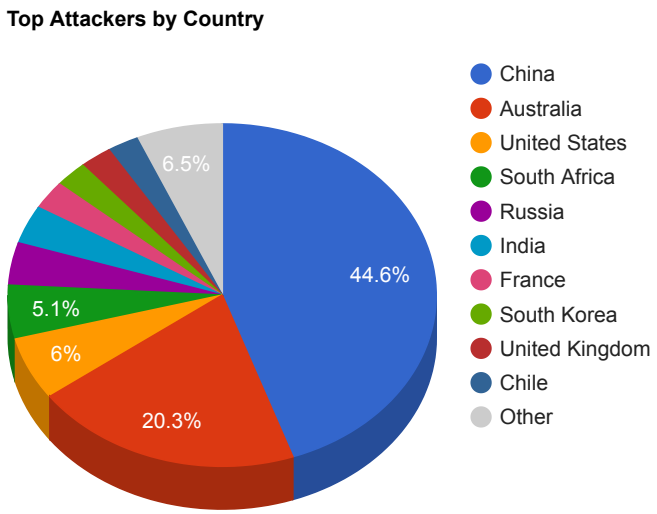
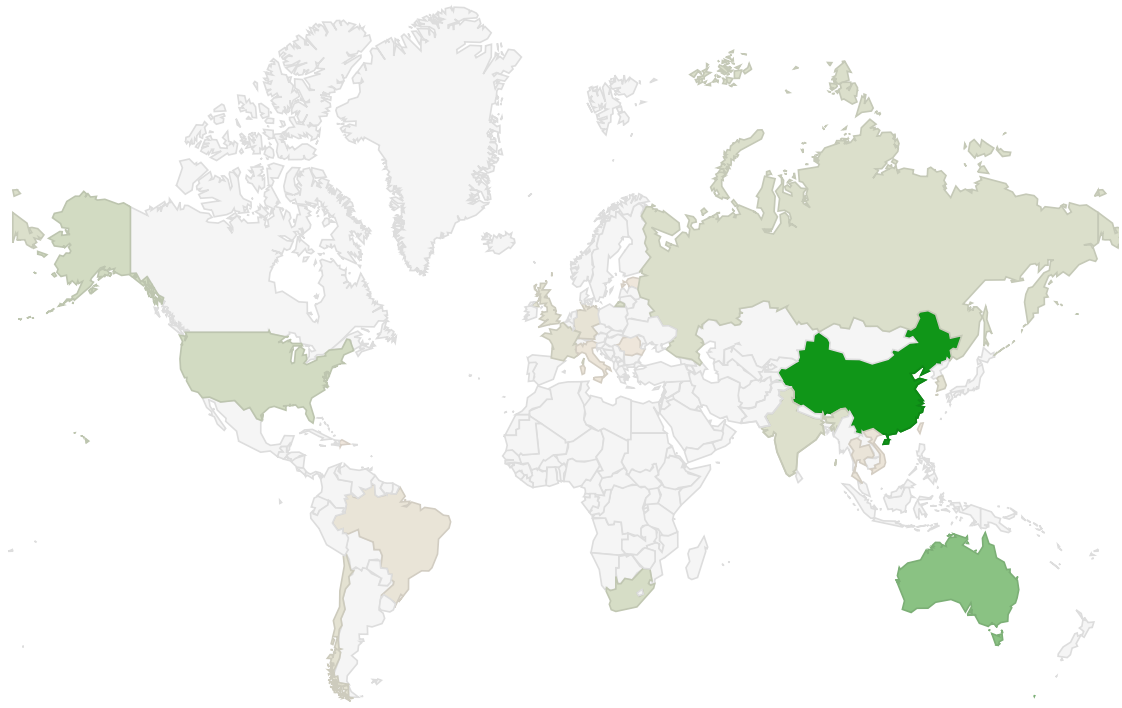
Trends

- The top attacker country was China with 1706706 unique attackers (44.00%).
- The top Trojan C&C server detected was TrickBot with 26 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	1706706	44.00%
Australia	774471	20.00%
United States	227625	5.00%
South Africa	193416	5.00%
Russia	153137	3.00%
India	138252	3.00%
France	102801	2.00%
South Korea	93817	2.00%
United Kingdom	92600	2.00%
Chile	89730	2.00%
Germany	62231	1.00%
Brazil	49809	1.00%
Thailand	41275	1.00%
Vietnam	35740	0%
Italy	28356	0%
Romania	12828	0%
Estonia	8455	0%
Taiwan	7876	0%
Dominican Republic	3302	0%

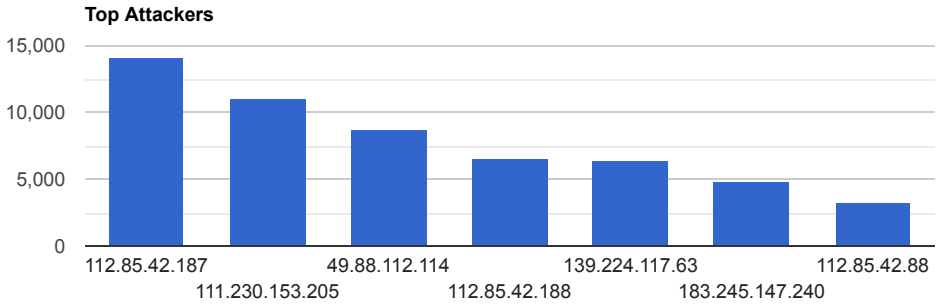




3,302 1,706,706

Top Attacking Hosts

Host	Occurrences
112.85.42.187	14166
111.230.153.205	11137
49.88.112.114	8797
112.85.42.188	6546
139.224.117.63	6416
183.245.147.240	4877
112.85.42.88	3344



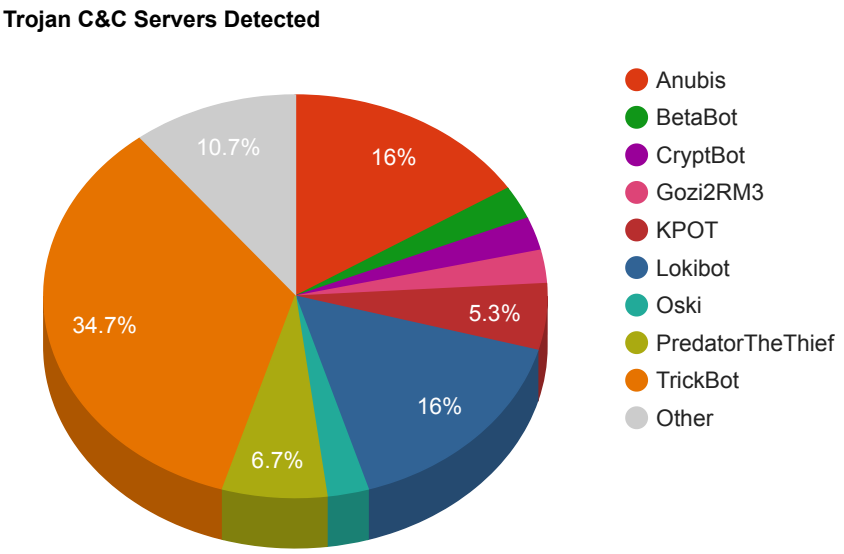
Top Network Attackers

ASN	Country	Name
37963	China	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN
56041	China	CMNET-ZHEJIANG-AP China Mobile communications corporation, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Amadey	1	8.208.89.219
Anubis	12	185.157.76.112 , 217.8.117.80 , 34.105.152.77 , 5.101.153.87 , 5.101.50.153 , 5.206.224.239 , 8.208.10.238 , 8.208.19.246 , 8.208.28.246 , 8.209.112.8 , 91.210.104.81 , 91.211.247.69
Azorult	1	104.237.252.54
BetaBot	2	5.101.50.99 , 84.38.181.21
CryptBot	2	77.220.205.154 , 95.181.198.176
Flexnet	1	47.252.0.20
Gozi2RM3	2	185.236.203.196 , 8.208.25.99
Heodo	1	213.60.96.117
KPOT	4	172.86.75.232 , 199.192.16.192 , bumboxik.casa , hjmthgb45df.lib
Lokibot	12	104.237.252.54 , 104.27.168.243 , 104.27.169.243 , 185.159.153.117 , 31.41.45.199 , 37.120.145.171 , 81.29.134.61 , 84.38.181.21 , 88.99.150.216 , 89.208.222.22 , 91.215.216.54 , lmpulsefashion.net
MassLogger	1	66.152.176.61
Oski	2	185.178.208.148 , 185.209.22.86
PredatorTheThief	5	141.8.193.236 , 185.18.52.177 , 185.27.134.142 , 81.177.140.221 , 81.177.141.241
Taurus	1	185.141.62.161

TrickBot	26	103.111.83.246 , 107.175.72.141 , 110.50.84.5 , 134.119.191.11 , 134.119.191.21 , 182.253.113.67 , 185.14.31.104 , 185.14.31.34 , 185.99.2.137 , 185.99.2.65 , 185.99.2.66 , 192.3.247.123 , 200.107.35.154 , 23.95.8.123 , 36.66.218.117 , 36.89.182.225 , 36.89.243.241 , 36.92.19.205 , 51.81.112.144 , 62.108.34.34 , 78.108.216.47 , 80.210.32.67 , 85.204.116.100 , 85.204.116.216 , 91.200.103.232 , 91.235.129.20
UAdmin	1	8.209.104.170
Zloader	1	5.101.50.240



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
42143a53581e0304b08f61c2ef8032d7	https://www.virustotal.com/gui/file/64f3633e009650708c070751bd7c7c28cd127b7a65d4ab4907dbe8ddaa01ec8b/details	JPMorganChase	Instructions	SMG
82749206.pdf	N/A	Pdf.Phishing.Phishing::malicious.tht.talos		
3409ff801cb177f6df26cfec8f4528ae	https://www.virustotal.com/gui/file/dddbfa95401a3f2d9999055b976a0b4ae963e128f7f0d5b043efae29e4306c4a/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.Adware.Flashserv::100.sbx.vioc

8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.Adware.Flashserv::100.sbx.vioc
b065af93b5fd551526705b5968d0ca10	https://www.virustotal.com/gui/file/28c33a9676f04274b2868c1a2c092503a57d38833f0f8b964d55458623b82b6e/details	vscekgp.exe	NTLMSharedFunctionality	W32.28C33A9676-100.SBX.TG
5d34464531ddbdc7b0a4dba5b4c1cfea	https://www.virustotal.com/gui/file/a545df34334b39522b9cc8cc0c11a1591e016539b209ca1d4ab8626d70a54776/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.Adware.Flashserv::in03.talos

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-2020-1048 Microsoft Windows Print Spooler Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/21/2020	05/26/2020

CVE-2020-3153 Cisco AnyConnect Secure Mobility Client Vulnerability Cisco	A vulnerability in the installer component of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated local attacker to copy user-supplied files to system level directories with system level privileges. The vulnerability is due to the incorrect handling of directory paths. An attacker could exploit this vulnerability by creating a malicious file and copying the file to a system directory. An exploit could allow the attacker to copy malicious files to arbitrary locations with system level privileges.	CVSSv3BaseScore:6.5(AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N)	02/19/2020	04/21/2020
CVE-2020-0674 Microsoft Windows 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)	02/11/2020	05/08/2020
CVE-2019-0685 Microsoft Windows Win32k Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	04/09/2019	04/10/2019

CVE-2020-11022 jQuery Cross Site Scripting Vulnerability Multi-Vendor	In jQuery, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information or addition or modification of data.	CVSSv3BaseScore:6.1(AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	04/29/2020	05/22/2020
CVE-2020-5837 Symantec Endpoint Protection Elevation of Privilege Vulnerability Symantec	Symantec Endpoint Protection, may not respect file permissions when writing to log files that are replaced by symbolic links, which can lead to a potential elevation of privilege.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/11/2020	05/14/2020
CVE-2020-1015 Microsoft Windows Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in the way that the User-Mode Power Service (UMPS) handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	04/15/2020	04/21/2020
CVE-2019-0887 Microsoft Remote Desktop Services Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Remote Desktop Servicesformerly known as Terminal Serviceswhen an authenticated attacker abuses clipboard redirection. An attacker who successfully exploited this vulnerability could execute arbitrary code on the victim system.	CVSSv3BaseScore:7.2(AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)	07/15/2019	08/08/2019