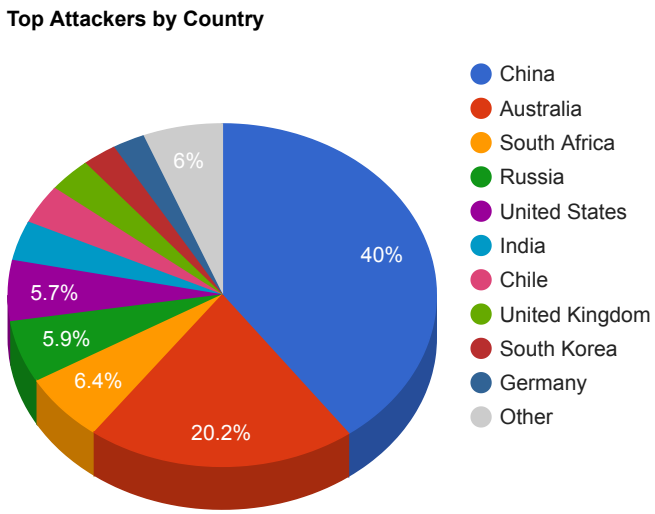
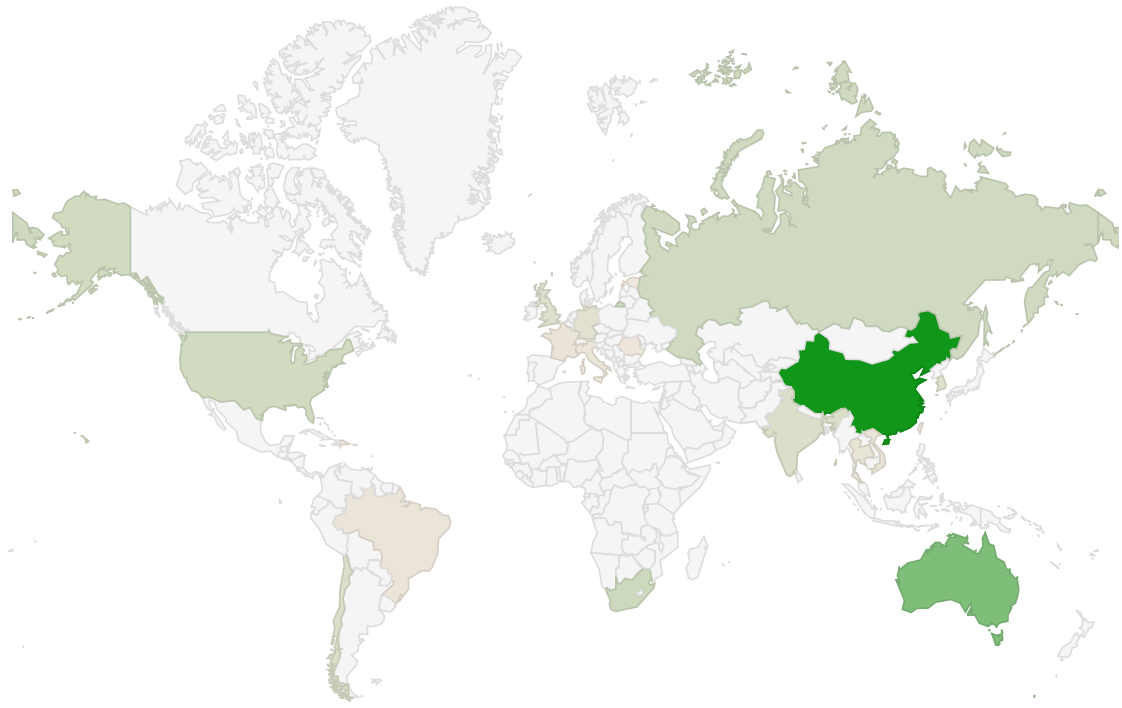
Trends

- The top attacker country was China with 941679 unique attackers (37.00%).
- The top Trojan C&C server detected was TrickBot with 18 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	941679	37.00%
Australia	476439	19.00%
South Africa	151548	6.00%
Russia	138560	5.00%
United States	135021	5.00%
India	88266	3.00%
Chile	87342	3.00%
United Kingdom	76755	3.00%
South Korea	60910	2.00%
Germany	57410	2.00%
Thailand	36265	1.00%
France	28993	1.00%
Vietnam	22892	0%
Brazil	18867	0%
Italy	14919	0%
Taiwan	6748	0%
Romania	6384	0%
Estonia	4285	0%
Dominican Republic	2909	0%



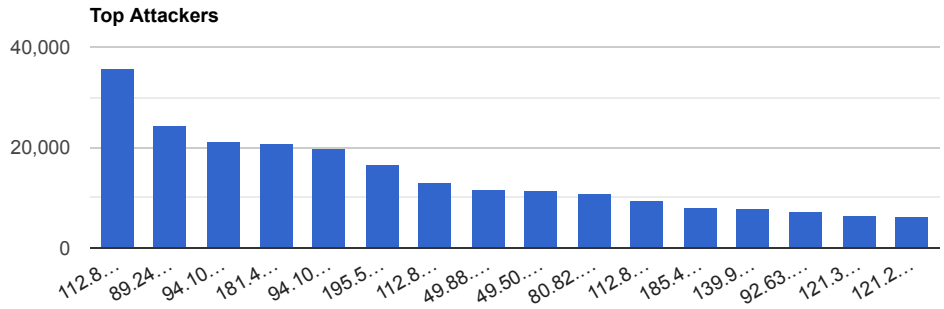


2,909 941,679

Top Attacking Hosts

Host	Occurrences
112.85.42.187	35686
89.248.168.221	24353
94.102.53.112	21105
181.43.214.78	20855
94.102.49.159	19988
195.54.166.29	16528
112.85.42.88	13132

49.88.112.114	11827
49.50.69.85	11359
80.82.65.60	10854
112.85.42.188	9569
185.40.4.116	8034
139.99.187.23	7711
92.63.196.3	7139
121.36.44.62	6564
121.218.128.50	6044



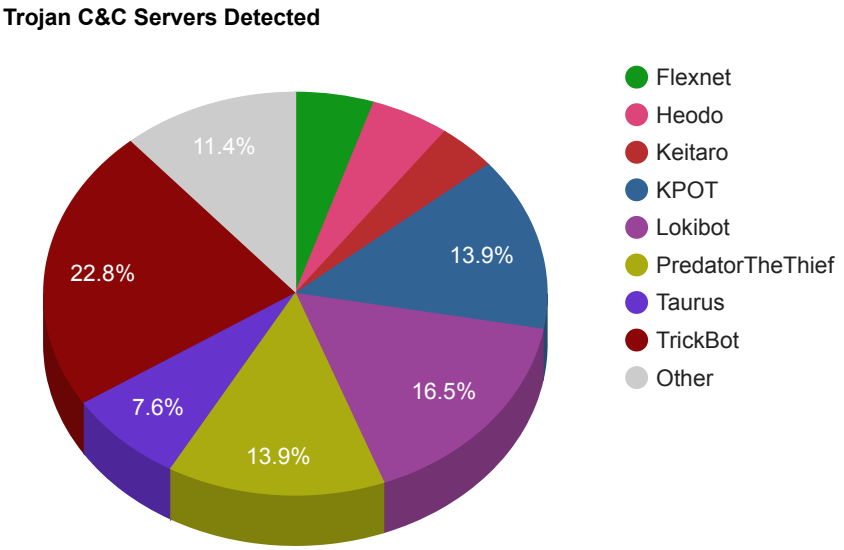
Top Network Attackers

ASN	Country	Name
49505	Russia	SELECTEL, RU
50113	Russia	SUPERSERVERSDATACENTER, RU
35582	Russia	CHISTYAKOV, RU

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Amadey	1	217.8.117.89
BetaBot	1	193.38.54.155
BlackBot	1	193.38.54.155
Flexnet	4	45.141.84.31 , 45.141.84.32 , 45.141.86.209 , 45.141.86.79
Guadox	1	193.38.54.155
H1N1	1	193.38.54.155
Heodo	4	186.188.222.3 , 195.76.232.114 , 196.179.249.218 , 85.94.170.73
KatyushaPro	1	45.141.86.143
Keitaro	3	46.249.62.206 , 46.249.62.253 , 91.219.239.183
KPOT	11	101.99.75.21 , 104.27.156.242 , 162.0.230.107 , 172.105.3.120 , 192.64.115.242 , 213.226.100.185 , 5.101.50.191 , 5.53.125.153 , 8.208.77.208 , 8.208.89.38 , gatehub.services
Lokibot	13	103.21.59.27 , 104.237.252.50 , 104.24.109.135 , 104.27.144.219 , 104.27.154.111 , 104.28.12.250 , 157.52.211.247 , 162.215.255.4 , 185.55.225.217 , 190.61.250.140 , 45.143.138.142 , 92.42.34.215 , rnarport.com
Oski	1	195.133.147.113

PredatorTheThief	11	141.8.193.236 , 177.55.116.76 , 185.178.208.137 , 185.50.25.17 , 5.23.50.132 , 5.23.50.190 , 81.177.141.121 , 81.177.141.22 , 8.209.73.155 , 92.53.96.169 , nelujan.beget.tech
Taurus	6	104.18.44.216 , 104.27.152.168 , 104.28.17.29 , 185.141.62.31 , 185.219.83.222 , bit-browser.gq
TeamViewerBot	1	193.38.54.155
TrickBot	18	144.91.64.194 , 144.91.76.208 , 158.69.133.68 , 185.105.1.225 , 185.164.32.164 , 185.164.32.167 , 185.205.209.101 , 193.38.54.106 , 194.5.250.211 , 194.5.250.214 , 45.148.120.176 , 5.101.50.173 , 51.89.177.14 , 5.9.178.74 , 62.108.35.45 , 79.137.100.4 , 85.204.116.18 , 85.204.116.182
ZyklonHTTP	1	193.38.54.155



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
c6dc7326766f3769575caa3ccab71f63	https://www.virustotal.com/gui/file/fb022bbec694d9b38e8a0e80dd0bfdfe0a462ac0d180965d314651a7bc0614f4/details	wupxarch.exe	N/A	Win.Dropper.Ranumbot::in03.talos

47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	W32.AgentWDCR:Gen.21gn.1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	W32.Generic:Gen.22fz.1201

Top Phishing Campaigns

Phishing Target	Count

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-2020-11651 Saltstack Remote Code Execution Vulnerability Multi-Vendor	An issue was discovered in SaltStack Salt where, the salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	04/30/2020	05/08/2020

CVE-2020-0932 Microsoft SharePoint Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the SharePoint application pool and the SharePoint server farm account.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	04/15/2020	04/17/2020
CVE-2020-2883 Oracle WebLogic Server T3 Protocol Deserialization of Untrusted Data Remote Code Execution Vulnerability Oracle	Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core) is vulnerable to an easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	04/15/2020	04/16/2020
CVE-2020-9294 FortiMail Authentication Bypass Vulnerability Fortiguard	An improper authentication vulnerability in FortiMail may allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	04/27/2020	05/04/2020
CVE-2020-0558 Intel Wi-Fi Products Denial of Service Vulnerability Intel	Improper buffer restrictions in kernel mode driver for Intel PROSet/Wireless WiFi products on Windows 10 may allow an unprivileged user to potentially enable denial of service via adjacent access.	CVSSv3BaseScore:6,5(AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	04/15/2020	04/23/2020

CVE-2020-0796 Microsoft Windows SMBv3 Client/Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	03/12/2020	03/31/2020
CVE-2020-0674 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)	02/11/2020	05/08/2020