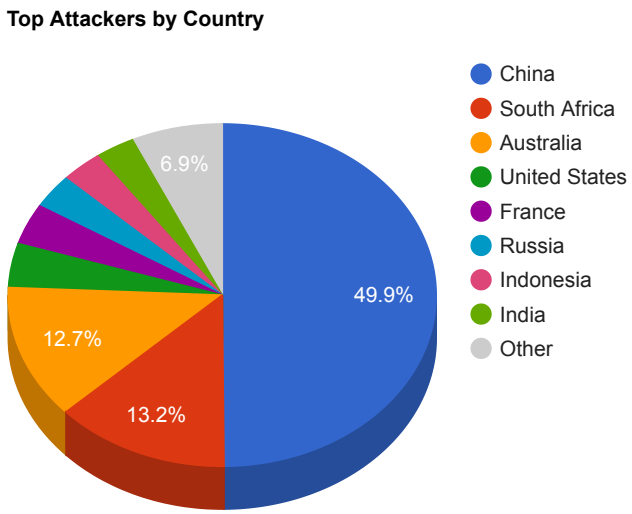
Trends

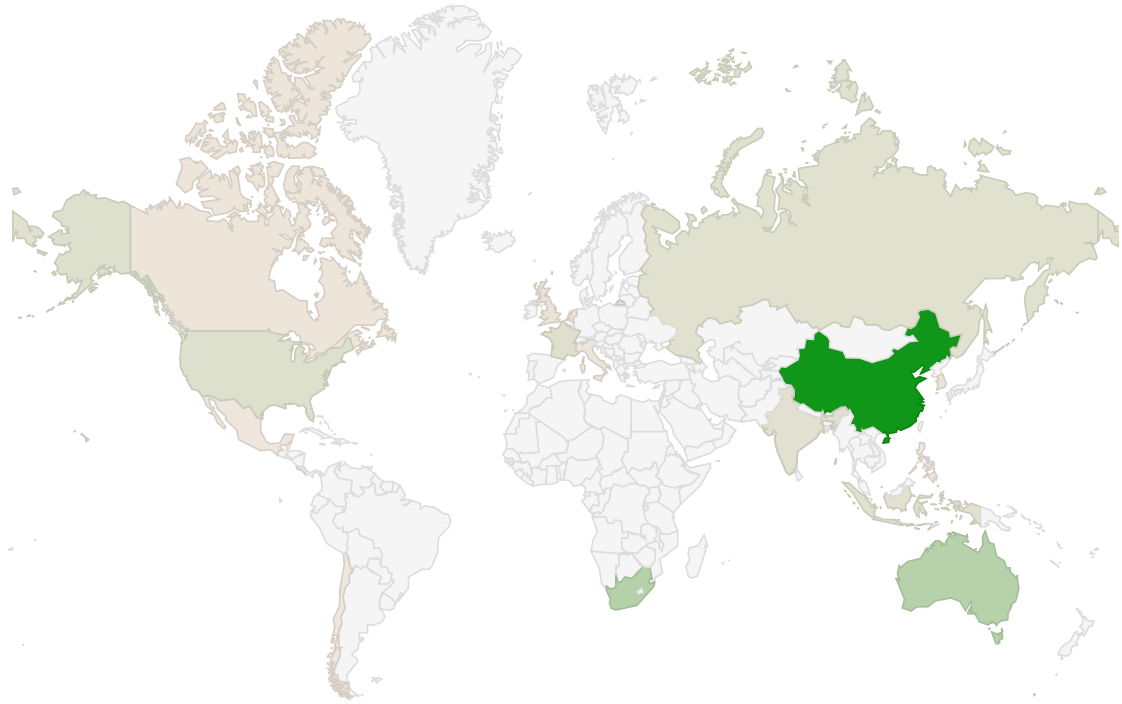
- The top attacker country was China with 217627 unique attackers (46.00%).
- The top Trojan C&C server detected was Heodo with 58 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	217627	46.00%
South Africa	57466	12.00%
Australia	55296	11.00%
United States	18154	3.00%
France	16859	3.00%
Russia	14064	3.00%
Indonesia	13725	2.00%
India	13098	2.00%
United Kingdom	6215	1.00%
South Korea	4898	1.00%
Netherlands	4004	0%
Italy	3222	0%
Canada	2751	0%
Costa Rica	2214	0%
Europe	2004	0%
Hong Kong	1753	0%
Mexico	1213	0%
Philippines	1127	0%
Chile	718	0%



Threat Geo-location

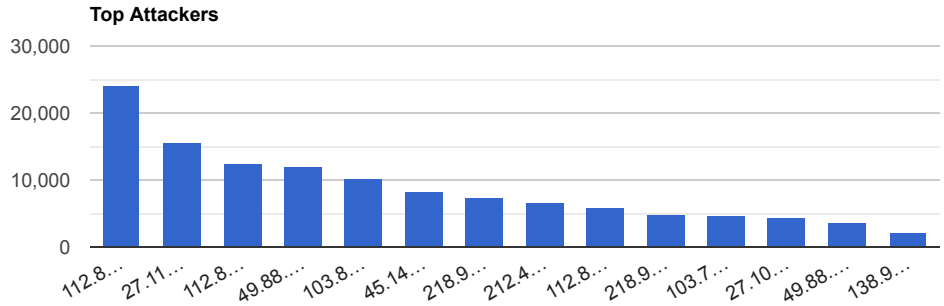


718 217,627

Top Attacking Hosts

Host	Occurrences
112.85.42.187	24082
27.115.13.245	15495
112.85.42.186	12419

49.88.112.117	11865
103.85.63.253	10287
45.141.84.25	8244
218.92.0.190	7230
212.47.244.235	6691
112.85.42.188	5959
218.92.0.192	4877
103.71.76.45	4714
27.106.63.114	4430
49.88.112.116	3579



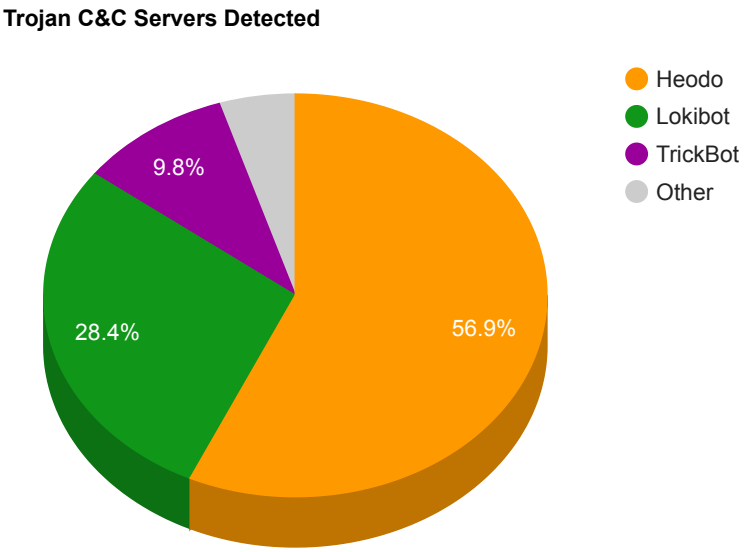
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
17621	China	CNCGROUP-SH China Unicom Shanghai network, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
23947	Indonesia	MORATELINDONAP-AS-ID PT.Mora Telematika Indonesia, ID
206728	Russia	MEDIALAND-AS, RU
12876	France	Online SAS, FR

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	2	185.98.87.59 , 193.32.188.146
BetaBot	1	185.14.31.230

Heodo	58	102.182.229.224 , 103.61.109.13 , 103.77.100.32 , 110.145.77.103 , 113.193.29.98 , 115.160.150.86 , 115.75.6.2 , 116.90.230.98 , 117.7.236.115 , 118.69.70.109 , 120.150.142.241 , 125.99.17.181 , 14.141.203.150 , 14.190.157.56 , 152.169.32.195 , 152.170.196.157 , 153.181.212.155 , 162.255.112.157 , 163.139.237.65 , 173.31.172.11 , 173.79.107.84 , 177.66.190.130 , 181.225.24.251 , 181.52.73.233 , 181.54.245.85 , 182.184.29.137 , 185.10.202.137 , 186.138.210.130 , 187.162.250.23 , 187.188.163.98 , 189.123.239.235 , 189.173.177.96 , 189.220.246.167 , 190.111.215.3 , 190.13.215.114 , 190.2.31.172 , 190.52.207.190 , 198.58.119.85 , 203.153.216.182 , 212.174.19.87 , 24.196.13.216 , 24.249.73.48 , 49.176.162.90 , 59.120.228.67 , 61.195.228.54 , 67.215.46.58 , 68.202.51.4 , 74.105.117.118 , 81.215.14.128 , 82.39.42.86 , 88.249.1.225 , 88.250.201.40 , 89.211.112.137 , 89.216.23.167 , 93.147.157.195 , 94.182.203.158 , 94.206.82.254 , 95.6.84.189
Lokibot	29	103.116.16.173 , 103.21.59.27 , 103.74.123.3 , 104.18.48.122 , 104.18.49.122 , 104.28.16.182 , 107.175.150.73 , 111.118.215.98 , 158.69.39.138 , 165.227.16.98 , 185.126.201.167 , 185.98.87.59 , 192.185.13.60 , 192.185.76.26 , 192.3.182.247 , 192.3.183.226 , 193.142.59.88 , 193.142.59.90 , 198.27.81.31 , 209.127.19.34 , 209.127.19.34 , 35.181.65.162 , 45.10.90.162 , 46.21.147.206 , 89.208.229.55 , 94.100.18.21 , 94.100.18.4 , 95.142.44.87 , ms-owa.host
TrickBot	10	178.156.202.120 , 178.156.202.130 , 178.156.202.143 , 185.183.96.43 , 185.62.188.10 , 195.133.145.31 , 212.80.216.209 , 5.188.168.136 , 5.34.177.97 , 85.143.216.206
Unknown	1	5.188.60.11
ZLoader	1	193.32.188.138



7c1e549cb59bcbf3	7e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	eternalblue-2.2.0.exe	N/A	A5226262.auto.Talos
be52a2a3074a014b163096055df127a0	https://www.virustotal.com/gui/file/97d8ea6cee63296eaf0fa5d97a14898d7cec6fa49fee1bf77c015ca7117a2ba7/details	xme64-553.exe	N/A	Win.Trojan.Coinminer::tpd
d45699f36a79b9d4ef91f5db1980d27b	https://www.virustotal.com/gui/file/9e9d85d9e29d6a39f58f4db3617526b92a5200225d41d0ab679a90c0167321b4/details	profile-6.exe		N/A
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac912661422 66a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	W32.Generic:Gen.22fz.1201

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-2020-0618 Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests. An attacker who successfully exploited this vulnerability could execute code in the context of the Report Server service account. To exploit the vulnerability, an authenticated attacker would need to submit a specially crafted page request to an affected Reporting Services instance.	6.5(AV:N/AC:L/Au:S/C:P/I:P/A:P)	02/11/2020	02/13/2020
CVE-2020-0668 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, aka 'Windows Kernel Elevation of Privilege Vulnerability'	4.6(AV:L/AC:L/Au:N/C:P/I:P/A:P)	02/11/2020	02/20/2020
CVE-2019-18683 Linux kernel vulnerability in the V4L2 subsystem Multi-Vendor	These vulnerabilities are caused by incorrect mutex locking in the vivid driver of the V4L2 subsystem (drivers/media/platform/vivid). This driver doesn't require any special hardware. It is shipped in Ubuntu, Debian, Arch Linux, SUSE Linux Enterprise, and openSUSE as a kernel module (CONFIG_VIDEO_VIVID=m).	6.9(AV:L/AC:M/Au:N/C:C/I:C/A:C)	11/04/2019	12/05/2019

CVE-2020-0601 Microsoft Windows CryptoAPI Spoofing Vulnerability Microsoft	A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source. The user would have no way of knowing the file was malicious, because the digital signature would appear to be from a trusted provider. A successful exploit could also allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.	5.8(AV:N/AC:M/Au:N/C:P/I:P/A:N)	01/14/2020	01/16/2020
CVE-2019-19781 Citrix ADC And Citrix Gateway Arbitrary Code Execution Vulnerability Citrix	A vulnerability has been identified in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution. Successfully exploiting this issue will allow attackers to execute arbitrary code within the context of the application.	7.5(AV:N/AC:L/Au:N/C:P/I:P/A:P)	12/27/2019	01/08/2020

CVE-2020-0683 Microsoft Windows Installer Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links. An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links. An attacker who successfully exploited this vulnerability could bypass access restrictions to add or remove files.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	02/11/2020	02/17/2020
CVE-2020-7247 OpenBSD OpenSMTPD Arbitrary Commands Execution Vulnerability OpenBSD	smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products, allows remote attackers to execute arbitrary commands as root via a crafted SMTP session, as demonstrated by shell metacharacters in a MAIL FROM field. This affects the "uncommented" default configuration. The issue exists because of an incorrect return value upon failure of input validation.	10.0(AV:N/AC:L/Au:N/C:C/I:C/A:C)	01/29/2020	01/31/2020
CVE-2019-11510 Pulse Secure Arbitrary File Disclosure Vulnerability Pulse Secure	Pulse Connect Secure is exposed to arbitrary file disclosure vulnerability. An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, or can send a specially crafted URI to perform an arbitrary file reading vulnerability.	7.5(AV:N/AC:L/Au:N/C:P/I:P/A:P)	05/08/2019	10/03/2019