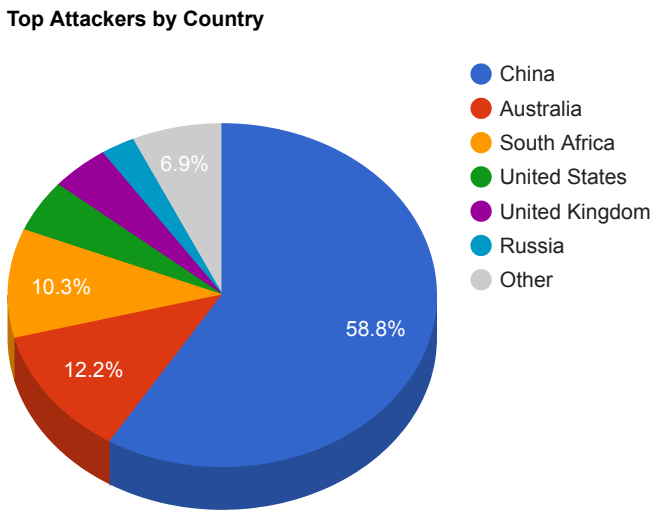
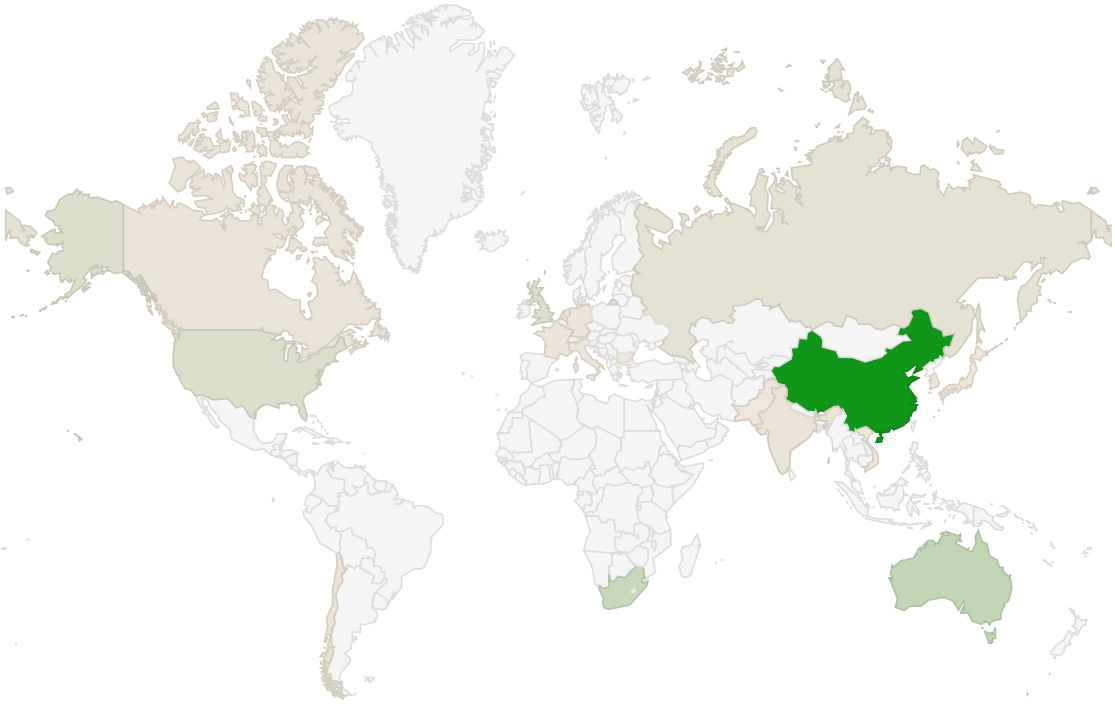
Trends

- The top attacker country was China with 488742 unique attackers (57.00%).
- The top Trojan C&C server detected was Trickbot with 38 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	488742	57.00%
Australia	101326	11.00%
South Africa	85389	10.00%
United States	40864	4.00%
United Kingdom	36910	4.00%
Russia	21397	2.00%
India	9656	1.00%
Chile	9554	1.00%
Canada	9120	1.00%
South Korea	6012	0%
Germany	4046	0%
Netherlands	4040	0%
France	3884	0%
Vietnam	3749	0%
Italy	3281	0%
Japan	1186	0%
Hong Kong	1144	0%
Pakistan	816	0%
Bulgaria	774	0%



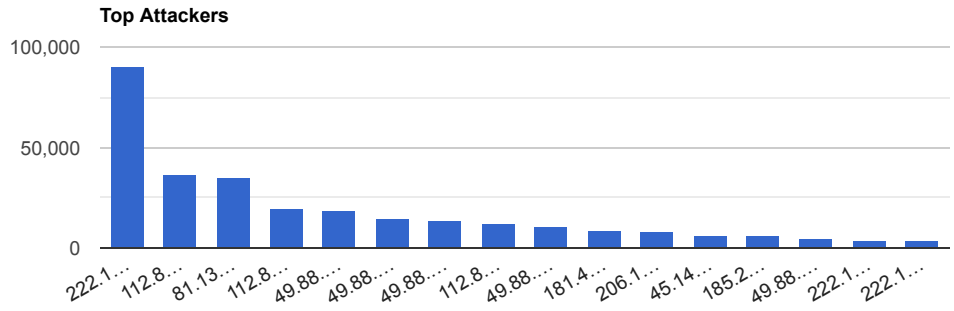


774 488,742

Top Attacking Hosts

Host	Occurrences
222.186.15.33	90445
112.85.42.187	36528
112.85.42.188	19269
49.88.112.75	19035
49.88.112.117	14662
49.88.112.76	13707

112.85.42.88	12025
49.88.112.116	10331
181.43.57.95	9320
206.189.24.67	7796
45.141.86.128	6456
185.211.247.142	6259
49.88.112.112	4888
222.186.175.182	4194
222.186.175.216	4143



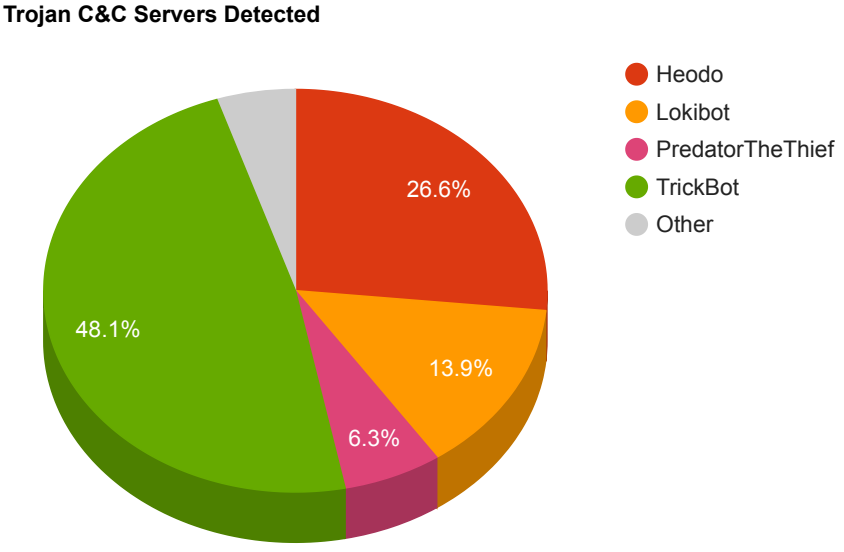
Top Network Attackers

ASN	Country	Name
23650	China	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
2856	United Kingdom	BT-UK-AS BTnet UK Regional network, GB
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
6471	Chile	ENTEL CHILE S.A., CL
206728	Russia	MEDIALAND-AS, RU
202984	Russia	TEAM-HOST AS, RU

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
DiamondFox	1	192.99.34.204
Heodo	21	101.187.104.105 , 137.25.7.112 , 142.105.151.124 , 170.82.195.50 , 177.230.81.0 , 180.222.165.169 , 186.188.152.177 , 186.208.123.210 , 190.108.228.62 , 190.181.235.46 , 190.229.148.144 , 190.251.235.239 , 201.214.229.79 , 201.91.28.210 , 221.133.46.86 , 46.214.11.172 , 61.197.37.169 , 65.24.85.214 , 82.223.70.24 , 94.130.171.231 , 95.180.25.146

Lokibot	11	103.143.173.20 , 104.223.170.93 , 136.243.90.101 , 162.213.253.111 , 185.159.153.129 , 192.3.202.210 , 35.246.219.215 , 45.252.248.29 , 50.31.174.86 , 89.38.241.83 , 91.215.169.52
Nexus	1	193.109.84.165
ParasiteStealer	1	104.24.107.129
Pony	1	103.143.173.20
PredatorTheThief	5	104.27.173.77 , 141.8.192.151 , 185.178.208.129 , 190.97.162.37 , 51.38.140.2
TrickBot	38	103.69.216.86 , 107.155.137.10 , 107.175.87.113 , 109.94.110.79 , 139.60.163.56 , 146.185.219.29 , 146.185.253.157 , 151.80.212.114 , 178.157.82.127 , 185.105.1.187 , 185.11.146.101 , 185.14.29.63 , 185.161.211.215 , 185.186.77.216 , 185.203.119.173 , 185.68.93.105 , 185.90.61.62 , 185.98.87.70 , 185.99.2.53 , 195.123.239.194 , 195.133.196.151 , 195.54.162.120 , 23.227.206.170 , 31.131.20.159 , 45.142.215.235 , 5.1.74.249 , 51.81.113.25 , 5.182.210.178 , 5.182.211.24 , 51.89.115.104 , 5.2.78.118 , 62.109.28.101 , 62.109.30.83 , 64.44.133.153 , 81.177.3.88 , 85.204.116.139 , 91.235.129.60 , 93.189.44.131



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
5fb477098fc975fd1b314c8fb0e4ec06	https://www.virustotal.com/gui/file/8e0aea169927ae791dbafe063a5674853315419 8cd539ee7efcd81a734ea325/details	upxarch.exe	N/A	Win.Dropper.Ranumbot::in07.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	W32.AgentWDCR:Gen.21gn.1201
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
42143a53581e0304b08f61c2ef8032d7	https://www.virustotal.com/gui/file/64f3633e009650708c070751bd7c7c28cd127b7a65d4ab4907dbe8ddaa01ec8b/details	myfile.exe	N/A	Pdf.Phishing.Phishing::malicious.tht.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-2020-0796 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-2020-0041 Google Android Privilege Escalation Vulnerability Android	In binder_transaction of binder.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	03/10/2020	03/11/2020

CVE-2020-7982 OpenWrt's opkg Man In The Middle Attack Vulnerability OpenWrt	A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification).	CVSSv3BaseScore:8.1(AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	03/16/2020	03/25/2020
CVE-2019-13495 Zyxel Cross Site Scripting Vulnerability Zyxel	In firmware version of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.	CVSSv3BaseScore:5.4(AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)	03/31/2020	04/01/2020
CVE-2020-10189 Zoho ManageEngine Desktop Central Remote Code Execution Vulnerability zohocorp	An issue was discovered in Zoho ManageEngine Desktop Central. Remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. This is related to the CewolfServlet and MDMLogUploaderServlet servlets. An attacker could exploit this vulnerability to escalate privilege on the target system.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	03/06/2020	03/09/2020

CVE-2019-18634 Sudo Buffer Overflow Vulnerability Multi-Vendor	In Sudo versions, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS however, it is NOT the default for up stream and many other packages, and would exist only if enabled by anadministrator.) The attacker needs to deliver along string to the stdin of get ln()int get pass.c.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	01/29/2020	02/07/2020