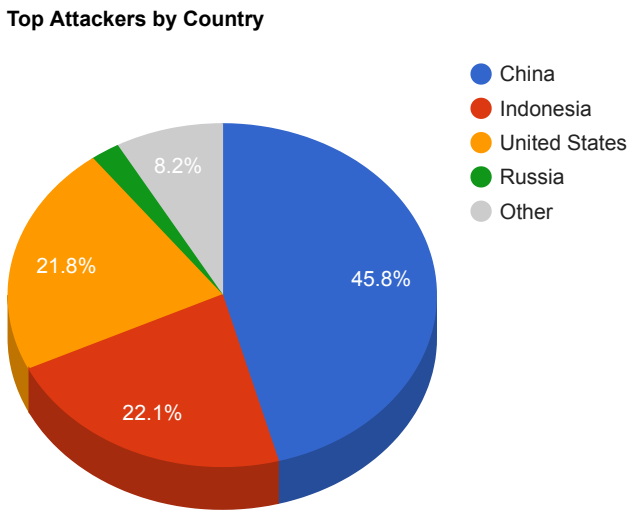
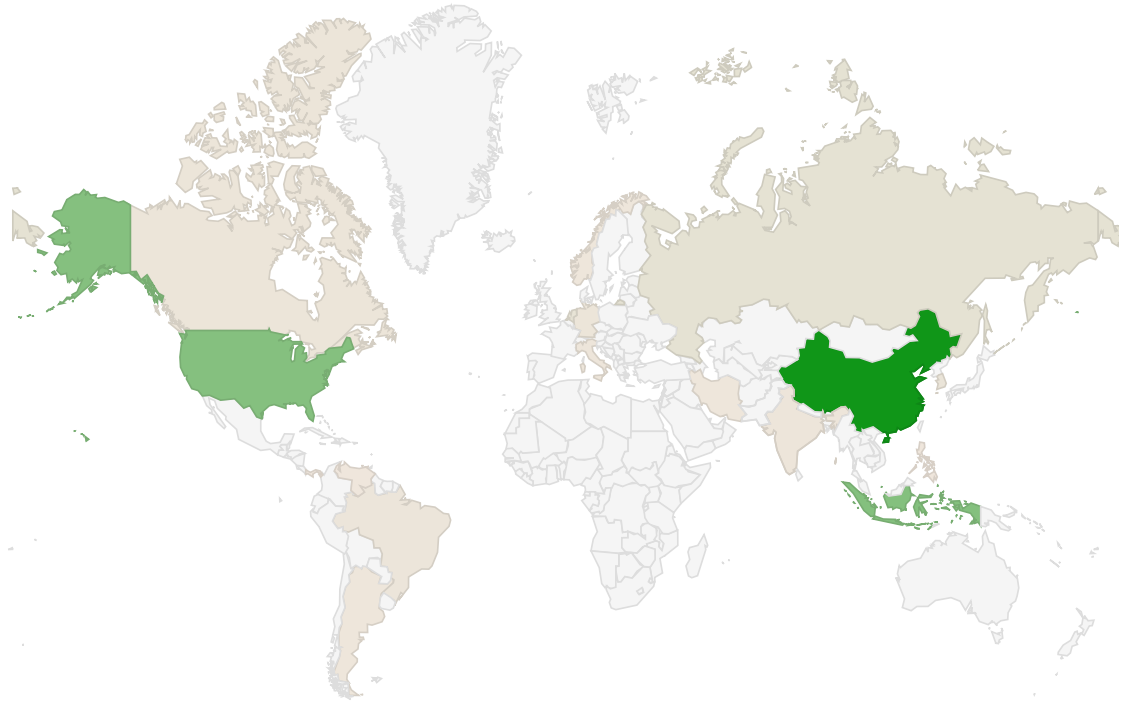
Trends

- The top attacker country was China with 91515 unique attackers (45.80%).
- The top Trojan C&C server detected was Heodo with 65 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	91515	45.80%
Indonesia	44119	22.08%
United States	43487	21.77%
Russia	4386	2.20%
Netherlands	3072	1.54%
South Korea	2351	1.18%
Canada	1767	0.88%
Germany	1626	0.81%
Brazil	1512	0.76%
India	1360	0.68%
Italy	1091	0.55%
Argentina	907	0.45%
Iran	680	0.34%
Norway	674	0.34%
Panama	487	0.24%
Philippines	401	0.20%
Venezuela	358	0.18%



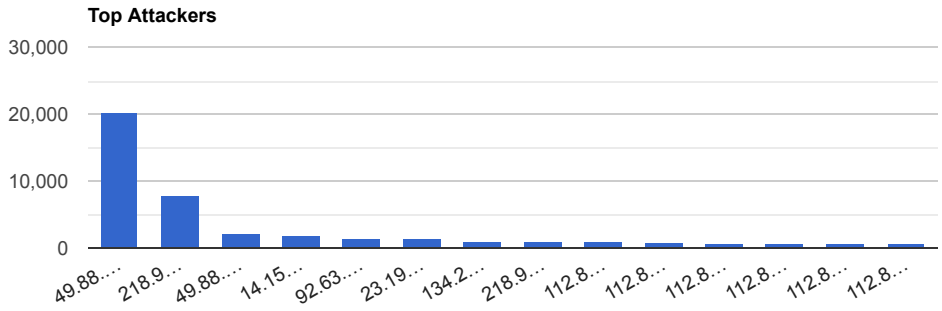


358 91,515

Top Attacking Hosts

Host	Occurrences
49.88.112.72	20224
218.92.0.205	7710
103.100.29.81	4047
49.88.112.116	2283
14.152.73.14	2028
115.85.129.125	1457
92.63.196.13	1374

23.194.132.43	1367
134.209.199.93	1036
218.92.0.250	921
112.85.42.81	915
112.85.42.151	795
112.85.42.172	763
112.85.42.122	746
112.85.42.98	746
112.85.42.47	743



Top Network Attackers

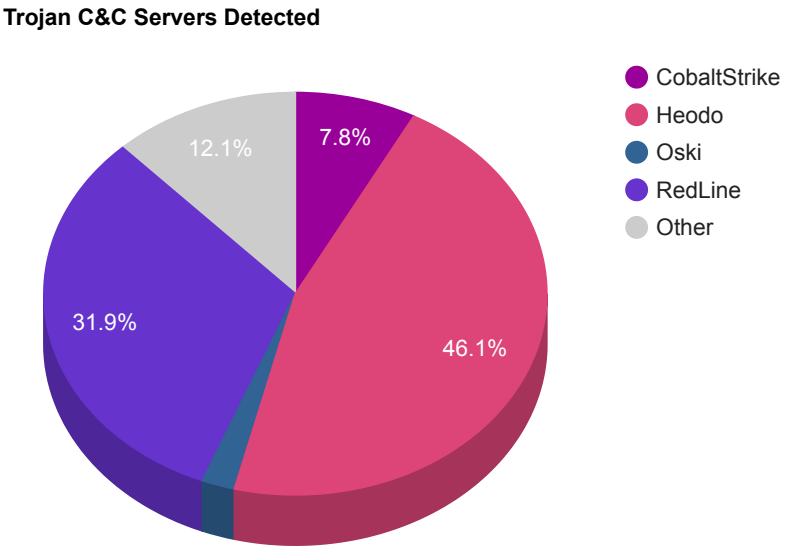
ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
58466	China	CT-GUANGZHOU-IDC CHINANET Guangdong province network, CN
47981	Russia	FOPSERVER, UA
14061	Netherlands	DIGITALOCEAN-ASN, US
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	209.205.206.58
Amadey	1	107.152.39.148
Azorult	2	81.19.215.2 , 91.203.193.242
BetaBot	1	91.203.193.242
CobaltStrike	11	176.123.8.191 , 185.25.51.35 , 193.38.55.91 , 213.252.246.185 , 45.141.84.212 , 45.141.84.34 , 45.142.215.38 , 88.119.170.212 , 88.119.175.100 , 88.119.175.60 , 91.211.246.238
DDosBot	1	45.10.153.186

Heodo	65	100.37.240.62 , 103.13.224.53 , 104.131.92.244 , 107.170.146.252 , 109.101.137.162 , 109.242.153.9 , 109.99.146.210 , 117.2.139.117 , 118.69.11.81 , 118.7.227.42 , 120.72.18.91 , 152.32.75.74 , 153.204.122.254 , 154.91.33.137 , 159.203.16.11 , 168.197.45.36 , 169.1.39.242 , 173.173.254.105 , 173.212.214.235 , 179.15.102.2 , 179.222.115.170 , 181.120.29.49 , 186.193.229.123 , 189.123.103.233 , 189.34.181.88 , 190.162.215.233 , 190.164.104.62 , 190.180.65.104 , 190.202.229.74 , 190.45.24.210 , 190.64.88.186 , 192.198.91.138 , 194.190.67.75 , 197.221.227.78 , 200.24.255.23 , 201.163.74.203 , 201.171.244.130 , 201.241.127.190 , 217.123.207.149 , 24.133.106.23 , 24.135.69.146 , 27.114.9.93 , 2.82.75.215 , 2.84.12.98 , 49.12.113.171 , 5.12.246.155 , 51.89.199.141 , 5.2.164.75 , 58.94.58.13 , 60.249.78.226 , 61.118.67.173 , 64.207.182.168 , 67.170.250.203 , 68.115.186.26 , 70.39.251.94 , 72.186.136.247 , 74.40.205.197 , 78.101.224.151 , 78.206.229.130 , 80.227.52.78 , 83.103.179.156 , 87.230.25.43 , 88.153.35.32 , 91.121.200.35 , 94.23.62.116
KeitaroTDS	1	45.141.84.197
Lokibot	2	45.252.248.12 , 91.203.193.242
Oski	3	185.206.214.130 , 45.12.215.204 , 45.141.84.184
Predator	2	141.8.192.31 , 141.8.193.236
PredatorTheThief	1	141.8.193.236
Redirected	1	207.154.210.66

RedLine	45	109.234.35.30 , 135.181.45.121 , 138.124.180.103 , 138.124.180.17 , 138.124.180.4 , 159.69.249.205 , 172.67.137.23 , 178.20.40.83 , 185.120.57.211 , 185.147.80.211 , 185.191.32.174 , 185.244.217.126 , 185.248.101.89 , 185.87.50.113 , 195.201.128.244 , 195.2.85.147 , 205.185.117.192 , 208.115.109.99 , 209.141.43.21 , 2.56.212.242 , 37.1.213.110 , 45.142.212.10 , 45.150.67.34 , 45.150.67.47 , 45.153.231.200 , 45.67.229.13 , 45.67.229.182 , 45.67.231.194 , 45.84.0.155 , 45.88.3.143 , 46.249.62.250 , 51.38.219.14 , 5.34.180.163 , 78.47.251.182 , 81.29.143.6 , 86.105.252.12 , 87.251.71.88 , 89.223.124.122 , 89.223.25.184 , 91.235.129.67 , 93.114.128.121 , 93.115.18.189 , 94.130.170.71 , 95.179.148.51 , 95.181.172.34
UAdmin	2	45.139.236.12 , 45.141.84.178
Zloader	2	217.8.117.17 , 91.203.193.163



CVEs with Recently Discovered Exploits

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

CVE, Title, Vendor	Description	CVSS v3.1 Base Score	Date Created	Date Updated

CVE-2020-14181 Atlassian Jira Server and Data Center User Enumeration Vulnerability Atlassian	Atlassian Jira Server and Data Center allow an unauthenticated user to enumerate users via an Information Disclosure vulnerability in the /ViewUserHover.jspa endpoint.	CVSSv3BaseScore:5.3(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	09/16/2020	09/18/2020
CVE-2020-16938 Microsoft Windows Kernel Information Disclosure Vulnerability Microsoft	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.	CVSSv3BaseScore:5.5(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	10/16/2020	10/20/2020

CVE-2020-3118 Cisco IOS XR Software Cisco Discovery Protocol Format String Vulnerability Cisco	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device.	CVSSv3BaseScore:8.8(AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	02/05/2020	02/10/2020
CVE-2020-1472 Microsoft Netlogon Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	08/17/2020	10/05/2020

CVE-2020-14882 Oracle Weblogic Remote Code Execution Vulnerability Oracle	A critical vulnerability exists in Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP 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)	10/21/2020	10/29/2020
CVE-2020-16898 Microsoft Windows TCP/IP Stack Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	10/16/2020	10/23/2020

CVE-2020-1013 Microsoft Windows Group Policy Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when Microsoft Windows processes group policy updates. An attacker who successfully exploited this vulnerability could potentially escalate permissions or perform additional privileged actions on the target machine. To exploit this vulnerability, an attacker would need to launch a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine. An attacker could then create a group policy to grant administrator rights to a standard user.	CVSSv3BaseScore:8.1(AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	09/11/2020	09/17/2020