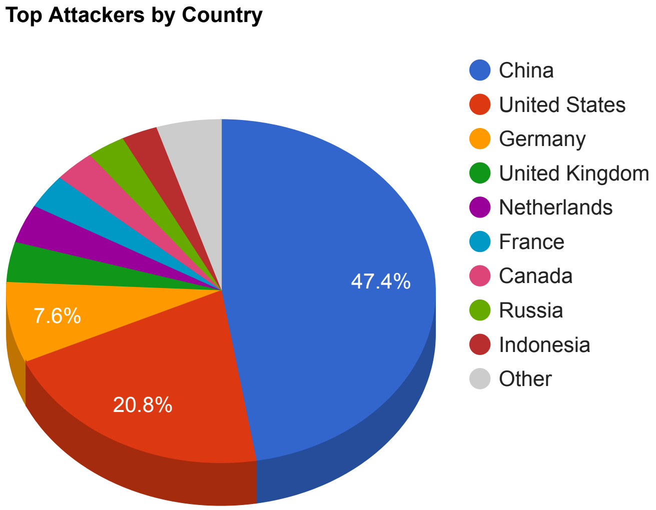
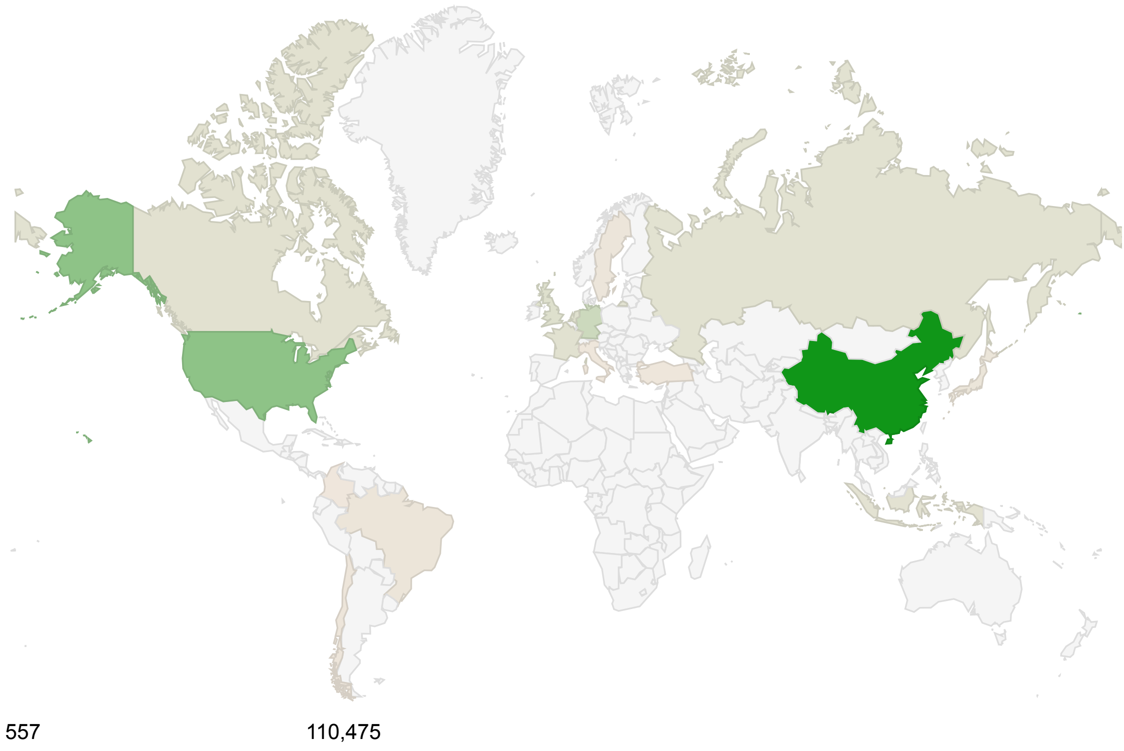
Trends

- The top attacker country was China with 110475 unique attackers (47.40%).
- The top Trojan C&C server detected was Heodo with 53 instances detected.
- The top phishing campaign detected was against Facebook accounts with 29 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	110475	47.40%
United States	48370	20.75%
Germany	17754	7.61%
United Kingdom	8800	3.77%
Netherlands	8465	3.63%
France	7520	3.22%
Canada	7161	3.07%
Russia	6734	2.88%
Indonesia	6308	2.70%
Japan	2293	0.98%
Brazil	1960	0%
Sweden	1910	0%
Chile	1423	0%
Turkey	1186	0%
Singapore	1110	0%
Italy	1022	0%
Colombia	557	0%

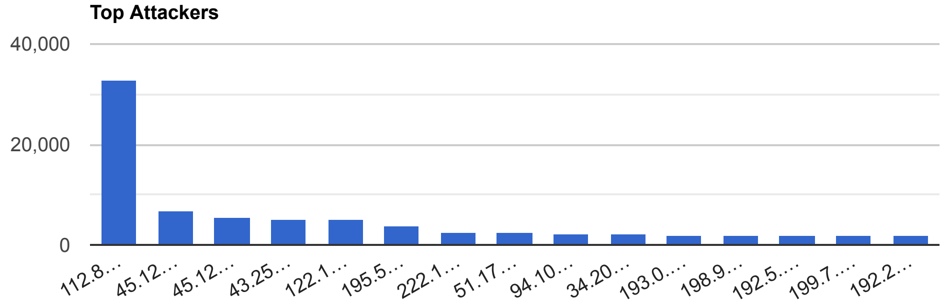




Top Attacking Hosts

Host	Occurrences
112.85.42.188	32916
45.129.33.81	6744
45.129.33.21	5666
43.252.145.42	5350
122.194.229.120	5045
195.54.161.122	3836
222.141.207.246	2555
51.178.184.226	2481

94.102.51.95	2203
34.200.247.158	2157
193.0.14.129	1959
198.97.190.53	1957
192.5.5.241	1950
199.7.91.13	1925
192.203.230.10	1924



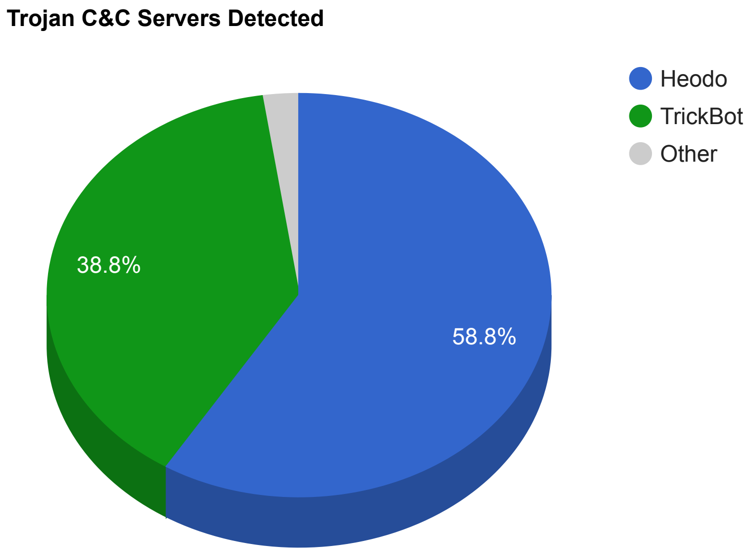
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
202425	Netherlands	INT-NETWORK, SC
2856	United Kingdom	BT-UK-AS BTnet UK Regional network, GB
56233	Indonesia	ATSINDO-AS-ID PT Asia Teknologi Solusi, ID
49505	Russia	SELECTEL, RU
16276	Romania	OVH, FR
14618	United States	AMAZON-AES, US
25152	Netherlands	K-ROOT-SERVER Reseaux IP Europeens Network Coordination Centre (RIPE NCC), EU

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location

Heodo	50	104.251.33.179 , 108.46.29.236 , 109.206.139.119 , 110.142.236.207 , 111.89.241.139 , 115.79.59.157 , 116.202.23.3 , 118.33.121.37 , 118.83.154.64 , 119.106.216.84 , 12.163.208.58 , 121.7.31.214 , 142.112.10.95 , 153.229.219.1 , 159.203.116.47 , 173.249.6.108 , 174.106.122.139 , 175.103.38.146 , 177.129.17.170 , 180.148.4.130 , 181.169.235.7 , 185.232.182.218 , 185.80.172.199 , 190.117.79.209 , 190.191.171.72 , 192.81.38.31 , 195.7.12.8 , 202.4.58.197 , 216.139.123.119 , 220.106.127.191 , 223.135.30.189 , 27.73.70.219 , 2.84.135.163 , 37.157.196.117 , 38.111.46.46 , 45.177.120.36 , 45.33.35.74 , 51.75.33.127 , 60.108.144.104 , 60.93.23.51 , 66.65.136.14 , 67.10.155.92 , 68.252.26.78 , 70.116.143.84 , 73.55.128.120 , 76.168.54.203 , 78.186.65.230 , 85.96.199.93 , 93.20.157.143 , 94.124.59.22
Lokibot	1	185.209.1.124
Taurus	1	195.2.78.152
TrickBot	33	103.76.169.213 , 117.222.63.145 , 117.252.214.138 , 125.165.20.104 , 148.251.185.165 , 179.127.88.41 , 179.97.246.23 , 181.143.186.42 , 185.172.129.173 , 185.234.72.35 , 185.99.2.243 , 190.99.97.42 , 194.5.249.143 , 194.87.110.144 , 195.123.240.104 , 195.123.240.113 , 195.123.241.242 , 200.24.67.161 , 213.32.84.27 , 36.91.87.227 , 45.224.213.234 , 45.237.241.97 , 45.67.231.68 , 45.89.125.148 , 5.152.210.188 , 5.182.210.156 , 51.89.163.40 , 85.204.116.173 , 86.104.194.38 , 86.104.194.77 , 88.150.180.32 , 88.150.197.172 , 89.223.126.186



73d1de319c7d61e0333471c82f2fc104	VirusTotal:https://www.virustotal.com/gui/file/32155b070c7e1b9d6bdc021778c5129edfb9cf7e330b8f07bb140dedb5c9aae7/details	SAntivirusService.exe	AntivirusService	Win.Dropper.Segurazo::tpd
e2ea315d9a83e7577053f52c974f6a5a	VirusTotal:https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201
bc26fd7a0b7fe005e116f5ff2227ea4d	VirusTotal:https://www.virustotal.com/gui/file/60b6d7664598e6a988d9389e6359838be966dfa54859d5cb1453cbc9b126ed7d/details	svchost.exe	N/A	Win.Dropper.Python::1201

Top Phishing Campaigns

Phishing Target (Users)	Count
Other	1299
Facebook	29
PayPal	9
Halifax	3
Amazon.com	11
Netflix	1
AOL	2
Google	10
Microsoft	7
Visa	1

Adobe	1
LinkedIn	1
Virustotal	2

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-2020-1472 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	09/28/2020
CVE-2020-14386 Linux kernel "af_packet.c" Memory Corruption Vulnerability Multi-Vendor	A Memory corruption vulnerability exists in the Linux kernel that can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.	CVSSv3BaseScore:6.7(AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	09/16/2020	09/28/2020
CVE-2020-4486 IBM QRadar Arbitrary File Overwrite Vulnerability IBM	IBM QRadar allows an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation.	CVSSv3BaseScore:8.1(AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H)	08/11/2020	08/11/2020

CVE-2020-8437 BitTorrent uTorrent Denial of Service Vulnerability bittorrent	The bencoding parser in BitTorrent uTorrent misparses nested bencoded dictionaries, which allows a remote attacker to cause a denial of service.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	03/02/2020	03/05/2020
CVE-2020-1350 Microsoft Windows DNS Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	07/14/2020	07/23/2020
CVE-2020-9496 Apache OFBiz XML-RPC Cross-Site Scripting Vulnerability Apache	Apache OFBiz XML-RPC request are vulnerable to unsafe deserialization and Cross-Site Scripting vulnerability.	CVSSv3BaseScore:6.1(AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	07/15/2020	08/17/2020
CVE-2020-16875 Microsoft Exchange Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft Exchange server due to improper validation of cmdlet arguments. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the System user. Exploitation of the vulnerability requires an authenticated user in a certain Exchange role to be compromised.	CVSSv3BaseScore:8.4(AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H)	09/11/2020	09/17/2020

CVE-2020-2037 PAN-OS Management Interface Command Injection Vulnerability PAN-OS	An OS Command Injection vulnerability exists in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue affects some unknown processing of the component Management Interface. The manipulation with an unknown input leads to a privilege escalation vulnerability.	CVSSv3BaseScore:7.2(V:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	09/09/2020	09/15/2020
CVE-2020-1380 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. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.	CVSSv3BaseScore:7.5(AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H)	08/17/2020	08/21/2020