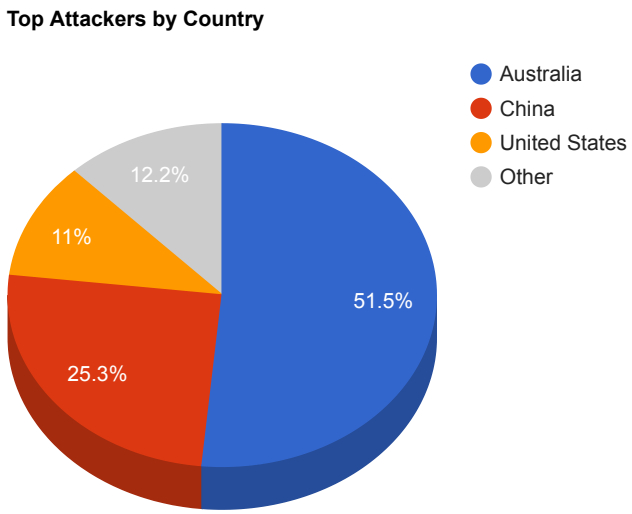
Trends

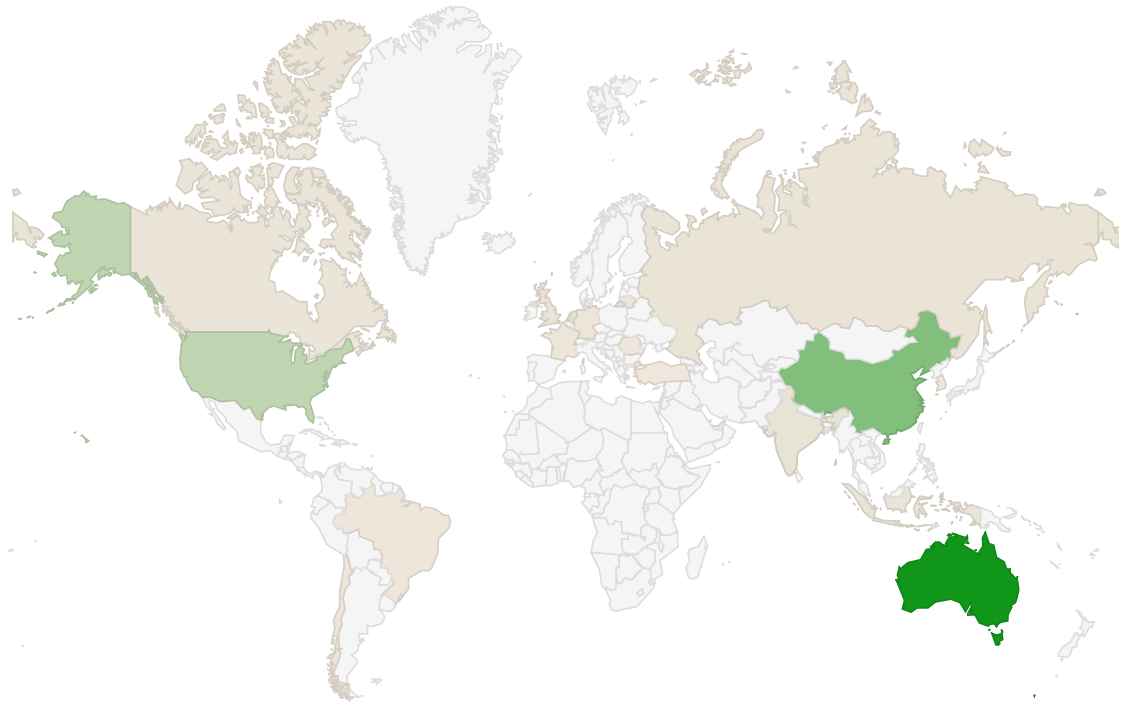
- The top attacker country was Australia with 407900 unique attackers (50.00%).
- The top Trojan C&C server detected was Heodo with 65 instances detected.
- The top phishing campaign detected was against Facebook accounts with 72 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
Australia	407900	50.00%
China	200569	24.00%
United States	87274	10.00%
India	15334	1.00%
Indonesia	11359	1.00%
Netherlands	11262	1.00%
United Kingdom	10602	1.00%
Russia	10056	1.00%
Canada	8751	1.00%
France	5590	0%
Lithuania	5242	0%
South Korea	4450	0%
Germany	4141	0%
Chile	2852	0%
Brazil	2137	0%
Romania	1873	0%
Turkey	1161	0%
United Arab Emirates	774	0%
Seychelles	697	0%



Threat Geo-location

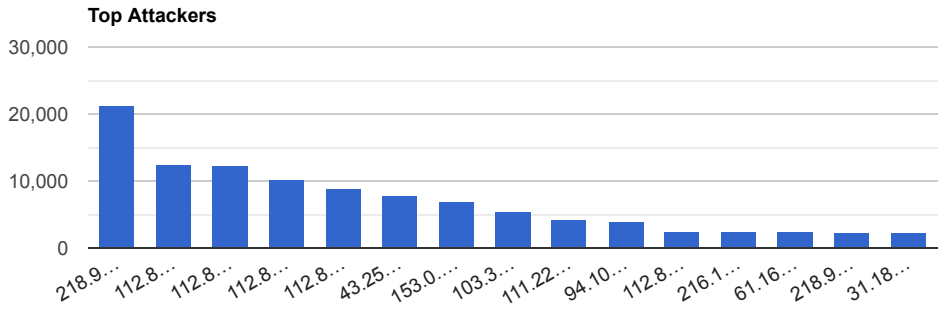


697 407,900

Top Attacking Hosts

Host	Occurrences
218.92.0.210	21167
112.85.42.88	12434

112.85.42.186	12239
112.85.42.187	10157
112.85.42.188	8717
43.252.145.42	7825
153.0.227.36	6733
103.36.84.148	5350
111.229.163.217	4238
94.102.51.17	3788
112.85.42.69	2503
216.10.245.13	2446
61.164.39.66	2348
218.92.0.192	2316
31.184.199.114	2238



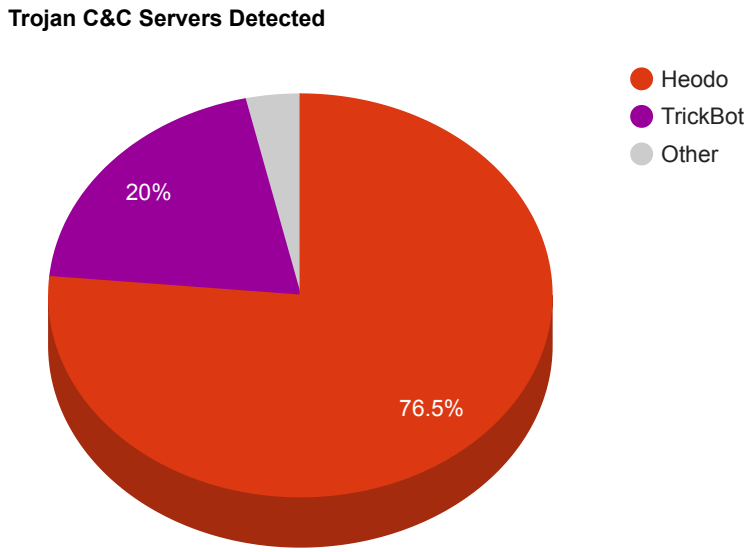
Top Network Attackers

ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
56233	Indonesia	ATSINDO-AS-ID PT Asia Teknologi Solusi, ID
133273	India	TISS-AS Tata Institute of Social Sciences, IN
45090	China	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
202425	Netherlands	INT-NETWORK, SC
394695	India	PUBLIC-DOMAIN-REGISTRY, US
34665	Russia	PINDC-AS, RU

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
DiamondFox	1	37.140.192.205

Heodo	65	103.133.66.57 , 103.48.68.173 , 103.93.220.182 , 104.156.59.7 , 110.5.16.198 , 113.156.82.32 , 113.160.248.110 , 113.193.239.51 , 114.158.45.53 , 115.176.16.221 , 118.243.83.70 , 119.92.77.17 , 120.138.30.150 , 120.51.34.254 , 121.7.127.163 , 124.41.215.226 , 126.126.139.26 , 128.106.187.110 , 134.209.36.254 , 139.59.67.118 , 14.241.182.160 , 145.239.169.32 , 153.177.101.120 , 156.155.166.221 , 162.241.41.111 , 181.169.34.190 , 181.95.133.104 , 182.227.240.189 , 182.253.83.234 , 187.189.66.200 , 189.150.209.206 , 189.160.188.97 , 190.101.48.116 , 190.192.39.136 , 190.85.46.52 , 195.251.213.56 , 200.116.93.61 , 202.166.170.43 , 213.196.135.145 , 220.147.247.145 , 220.245.198.194 , 221.184.46.216 , 223.133.20.171 , 36.91.44.183 , 37.210.220.95 , 41.40.125.237 , 41.84.243.145 , 42.200.107.142 , 45.79.16.230 , 49.243.9.118 , 5.189.168.53 , 59.93.12.150 , 61.92.17.12 , 67.121.104.51 , 74.134.41.124 , 75.80.124.4 , 78.114.175.216 , 78.187.156.31 , 80.200.62.81 , 82.225.49.121 , 82.80.155.43 , 88.247.58.26 , 89.216.122.92 , 94.1.108.190 , 94.23.216.33
MassLogger	1	44.227.238.106
StealthWorker	1	91.240.118.73
TrickBot	17	151.80.121.67 , 162.244.32.217 , 164.68.107.165 , 185.234.72.94 , 185.43.6.59 , 185.90.61.69 , 185.99.2.244 , 194.5.249.229 , 195.123.240.18 , 195.123.241.136 , 45.148.10.161 , 45.148.10.162 , 45.148.10.36 , 5.34.176.59 , 89.191.234.201 , 89.249.65.53 , 95.181.198.100



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eter.exe	N/A	Win.Exploit.Shadowbrokers::5A5226262.auto.talos
73d1de319c7d61e0333471c82f2fc104	https://www.virustotal.com/gui/file/32155b070c7e1b9d6bdc021778c5129edfb9cf7e330b8f07bb140dedb5c9aae7/details	SAntivirusService.exe	AntivirusService	Win.Dropper.Seguraz o::tpd
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	Tempmf582901854.exe	N/A	Win.Dropper.Agentwdcr::1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	Win.Downloader.Generic::1201
6423f6d49466f739d4eaa2a30759c46a	https://www.virustotal.com/gui/file/7bd78114e61ae332e9e9d67b66cdab4a4db4e0c74dc43a0582ab1aecb13d7f0f/details	Xerox_Device_060214.exe	N/A	Win.Dropper.Upatre::1201

Top Phishing Campaigns

Phishing Target	Count
Other	1186
Facebook	72
PayPal	21
Virustotal	17
Amazon.com	16
VKontakte	15
Google	13
RuneScape	9
Microsoft	7
Instagram	5
Vodafone	5
Rabobank	4
EE	2
Yahoo	2
Special	2
Steam	2
Caixa	2
Twitter	1
Apple	1
Paxful	1
Three	1
Bradesco	1
Halifax	1
Sparkasse	1

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	09/17/2020

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	09/16/2020
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-2020-14356 Linux Kernel Denial of Service Vulnerability Multi-Vendor	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system. Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	08/19/2020	09/15/2020
CVE-2020-15505 MobileIron Core and Connector Remote Code Execution Vulnerability MobileIron	A remote code execution vulnerability exists in MobileIron Core and Connector, and Sentry, that allows remote attackers to execute arbitrary code via unspecified vectors. The manipulation with an unknown input leads to a privilege escalation vulnerability.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/06/2020	09/18/2020

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-2020-0751 Microsoft Windows Hyper-V Denial of Service Vulnerability Microsoft	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.	CVSSv3BaseScore:6.0(AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H)	02/11/2020	02/13/2020
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