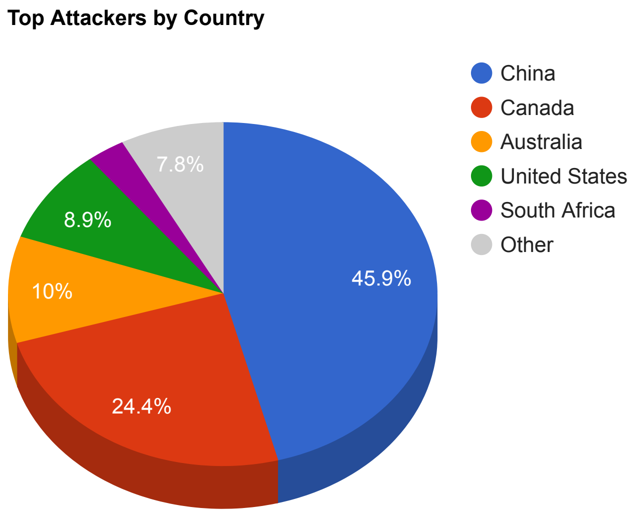
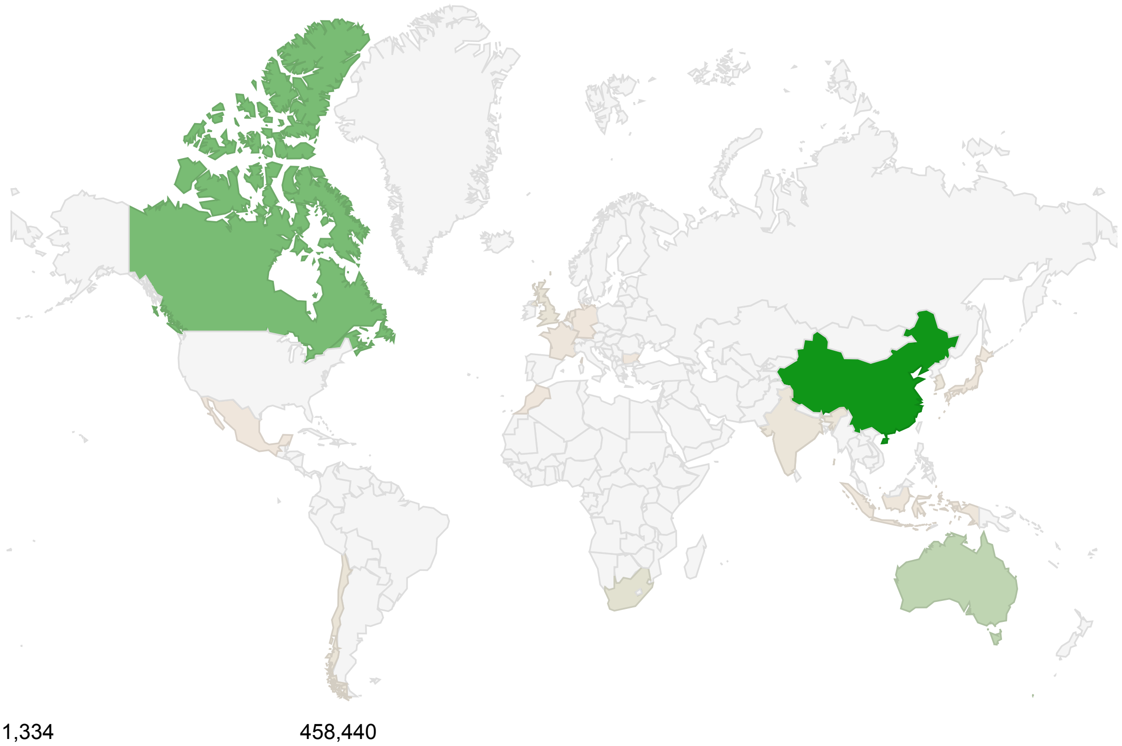
Trends

- The top attacker country was China with 458440 unique attackers (44.00%).
- The top Trojan C&C server detected was Oski with 7 instances detected.

Top Attackers By Country

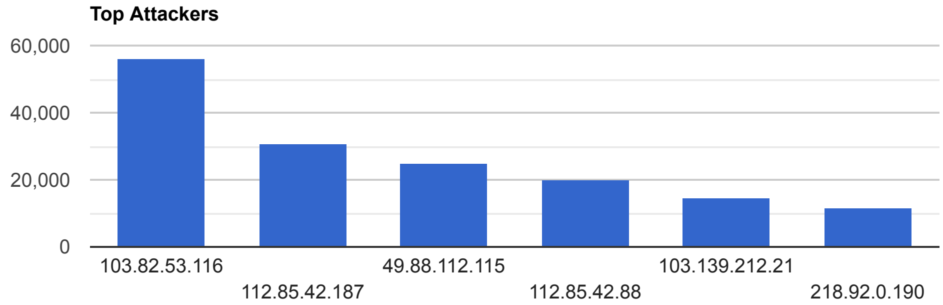
Country	Occurences	Percentage
China	458440	44.00%
Canada	244023	23.00%
Australia	100190	9.00%
United States	89301	8.00%
South Africa	28643	2.00%
United Kingdom	16407	1.00%
Chile	12182	1.00%
South Korea	9495	0%
India	9465	0%
Hong Kong	5560	0%
Netherlands	5291	0%
France	4810	0%
Japan	4090	0%
Indonesia	3828	0%
Germany	2188	0%
Morocco	1874	0%
Bulgaria	1571	0%
Mexico	1334	0%





Top Attacking Hosts

Host	Occurrences
103.82.53.116	55856
112.85.42.187	30663
49.88.112.115	25011
112.85.42.88	20243
103.139.212.21	14668
218.92.0.190	11758

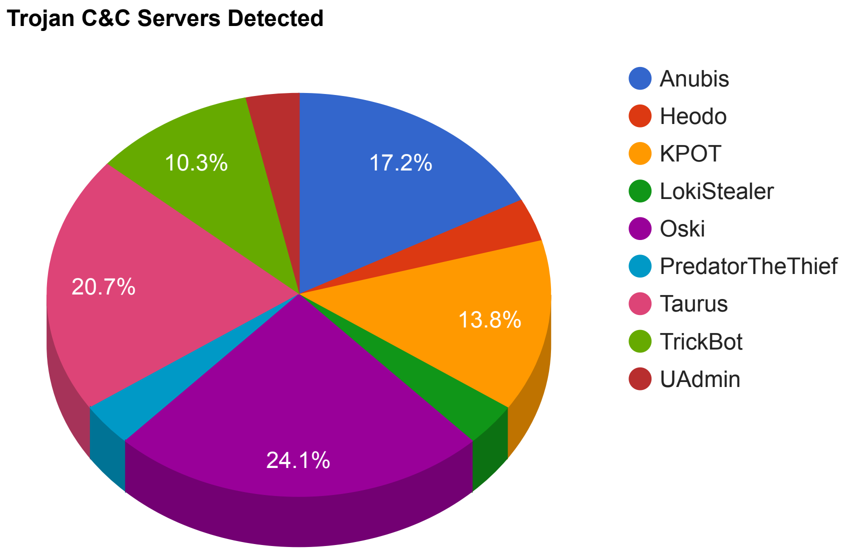


Top Network Attackers

ASN	Country	Name
136160	China	BSYNTCL-AS-AP Beijing Shijihulian Yuntong Network Technology Co., Ltd., CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4847	China	CNIX-AP China Networks Inter-Exchange, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	5	176.121.14.173 , 8.208.102.203 , 8.208.83.128 , 8.211.9.122 , 84.38.183.65
Heodo	1	173.91.22.41
KPOT	4	104.24.110.184 , 92.119.112.32 , karnaval.bar , karnaval.casa
LokiStealer	1	45.147.197.180
Oski	7	194.87.111.188 , 217.8.117.45 , 45.141.84.184 , 47.241.11.25 , 80.85.157.41 , 80.89.228.202 , thekurva.xyz
PredatorTheThief	1	141.8.192.151
Taurus	6	104.18.47.219 , 104.18.51.158 , 47.241.131.180 , 64.225.22.106 , 85.217.171.72 , blogstat28.xyz
TrickBot	3	185.180.198.69 , 45.148.120.164 , 45.155.173.223
UAdmin	1	37.46.130.159



1a31db1a91b18db	b7393c77aaedd5efb 5957116afd4263bd7 edc2188/details	xe		nserv::100.sbx.vioc
e2ea315d9a83e7577 053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/detection	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201
8193b63313019b614 d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg
60ba2a4b8ea5982a 3a671a9e84f9268c	https://www.virustotal.com/gui/file/8e03f05ecd08cb78f37ccd92c48cd9d357c438112b85bd154e8261c19e38a56e/details	Diagnostics.txt	N/A	Win.Dropper.Shadowbrokers::222044.in02

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-2020-0022 Google Android Bluetooth Remote Denial Of Service Vulnerability Google	A remote denial of service vulnerability exists in Google Android. In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed.	CVSSv3BaseScore:8.8(AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	02/13/2020	05/13/2020
CVE-2020-10189 WPA and WPA2 Disassociation Vulnerability ("Kr00k") Multi-Vendor	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic.	CVSSv3BaseScore:9.8(AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)	03/06/2020	03/09/2020
CVE-2020-1170 Microsoft Windows Defender Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system. To exploit the vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/12/2020

CVE-2020-1181 Microsoft SharePoint Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls. An authenticated attacker who successfully exploited the vulnerability could use a specially crafted page to perform actions in the security context of the SharePoint application pool process. To exploit the vulnerability, an authenticated user must create and invoke a specially crafted page on an affected version of Microsoft SharePoint Server.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/12/2020
CVE-2020-12388 Firefox Default Content Process DACL Sandbox Escape Vulnerability Mozilla	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla Firefox ESR. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on user.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	05/26/2020	05/28/2020

CVE-2020-3347 Cisco Webex Meetings Desktop App for Windows Shared Memory Information Disclosure Vulnerability Cisco	A vulnerability in Cisco Webex Meetings Desktop App for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. The vulnerability is due to unsafe usage of shared memory that is used by the affected software. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens that could aid the attacker in future attacks.	CVSSv3BaseScore:5.5AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	06/17/2020	06/24/2020
CVE-2020-1054 Microsoft Win32k Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.	CVSSv3BaseScore:7.0(AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/21/2020	05/27/2020