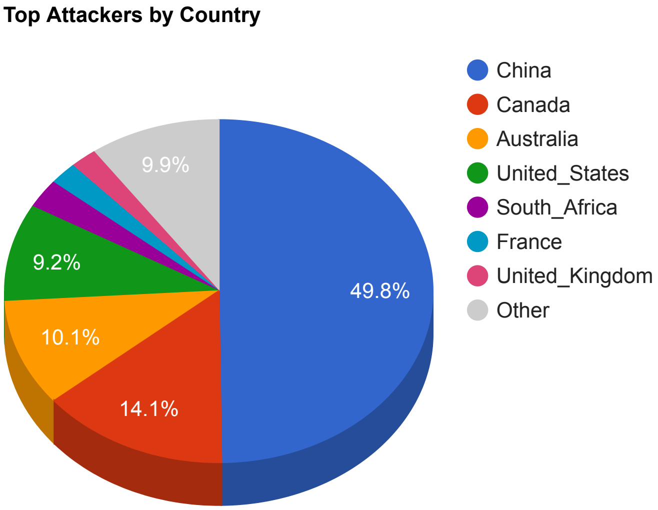
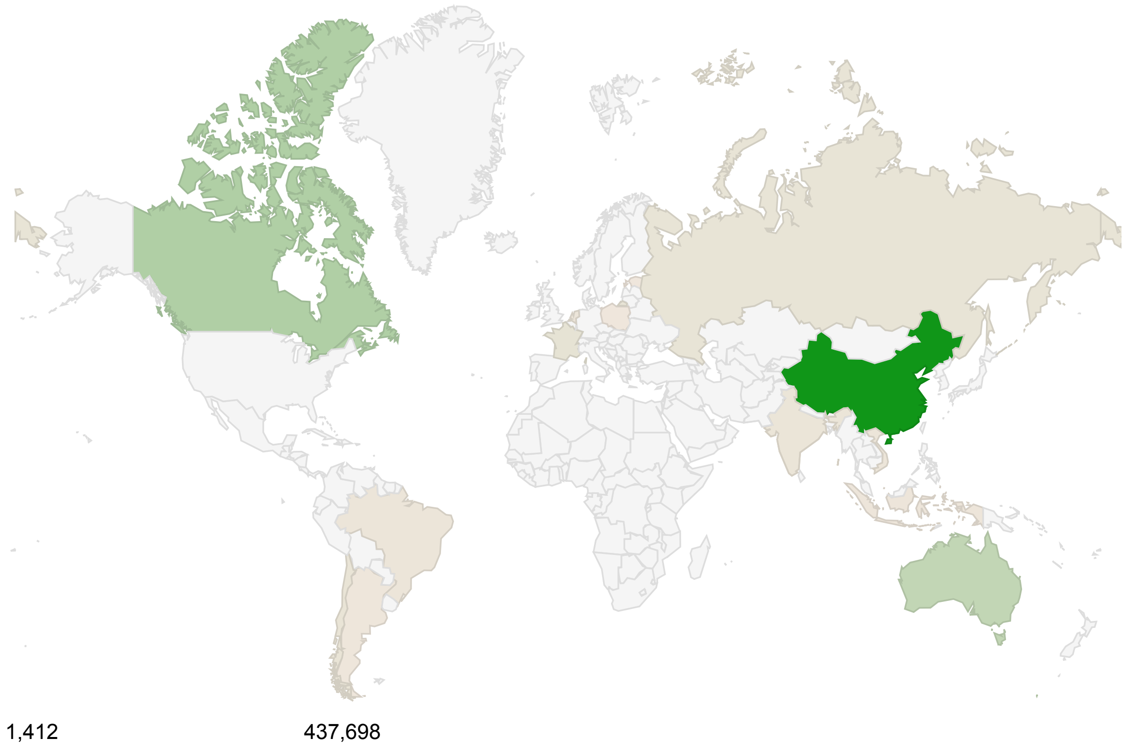
Trends

- The top attacker country was China with 437698 unique attackers (48.00%).
- The top Trojan C&C server detected was Heodo with 6 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	437698	48.00%
Canada	124310	13.00%
Australia	88508	9.00%
United_States	80712	8.00%
South_Africa	24011	2.00%
France	18645	2.00%
United_Kingdom	17823	1.00%
Russia	14141	1.00%
Chile	13778	1.00%
India	9418	1.00%
Vietnam	8254	0%
South_Korea	8197	0%
Brazil	7768	0%
Singapore	7178	0%
Netherlands	7127	0%
Indonesia	5489	0%
Argentina	2947	0%
Poland	1454	0%
Estonia	1412	0%

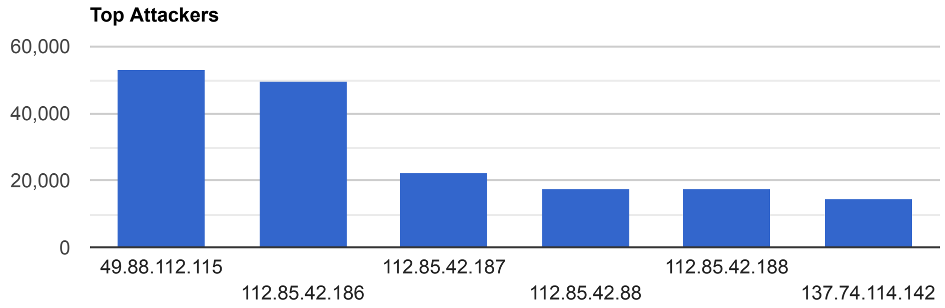




Top Attacking Hosts

Host	Occurrences
49.88.112.115	53174
112.85.42.186	49845
112.85.42.187	22622
112.85.42.88	17632
112.85.42.188	17597

137.74.114.142	14878

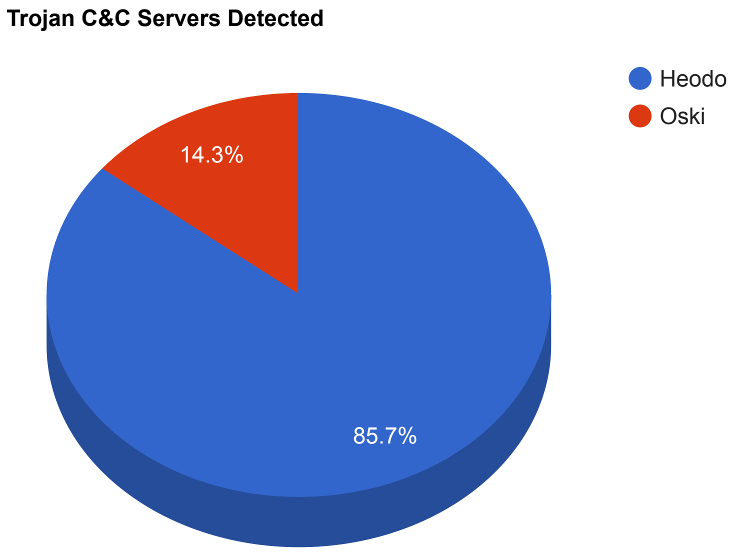


Top Network Attackers

ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
16276	France	OVH, FR

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	6	108.48.41.69 , 14.99.112.138 , 190.55.233.156 , 200.55.243.138 , 212.51.142.238 , 219.92.13.25
Oski	1	194.87.146.229



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	FlashHelperServices.exe	FlashHelperServices	Win.Exploit.Shadowbrokers::5A5226262.auto.talos
a10a6d9dfc0328a391a3fdb1a9fb18db	https://www.virustotal.com/gui/file/094d4da0ae3ded8b936428bb7393c77aaedd5efb5957116afd4263bd7edc2188/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::100.sbx.vioc
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/detection	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg
60ba2a4b8ea5982a3a671a9e84f9268c	https://www.virustotal.com/gui/file/8e03f05ecd08cb78f37ccd92c48cd9d357c438112b85bd154e8261c19e38a56e/details	Diagnostics.txt	N/A	Win.Dropper.Shadowbrokers::222044.in02

Top Phishing Campaigns

Phishing Target	Count
Other	1593
Facebook	86
Google	13
Amazon.com	7
PayPal	6
RuneScape	6
Microsoft	4
Three	4
Visa	3
Dropbox	3
Adobe	2
Virustotal	2
LinkedIn	2
Caixa	2
Steam	2
DHL	2
Itau	1
Yahoo	1
WalMart	1
Alibaba.com	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-2020-0022 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