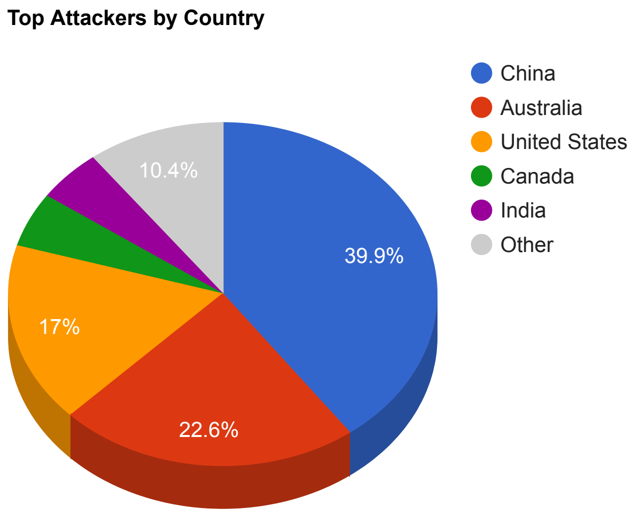
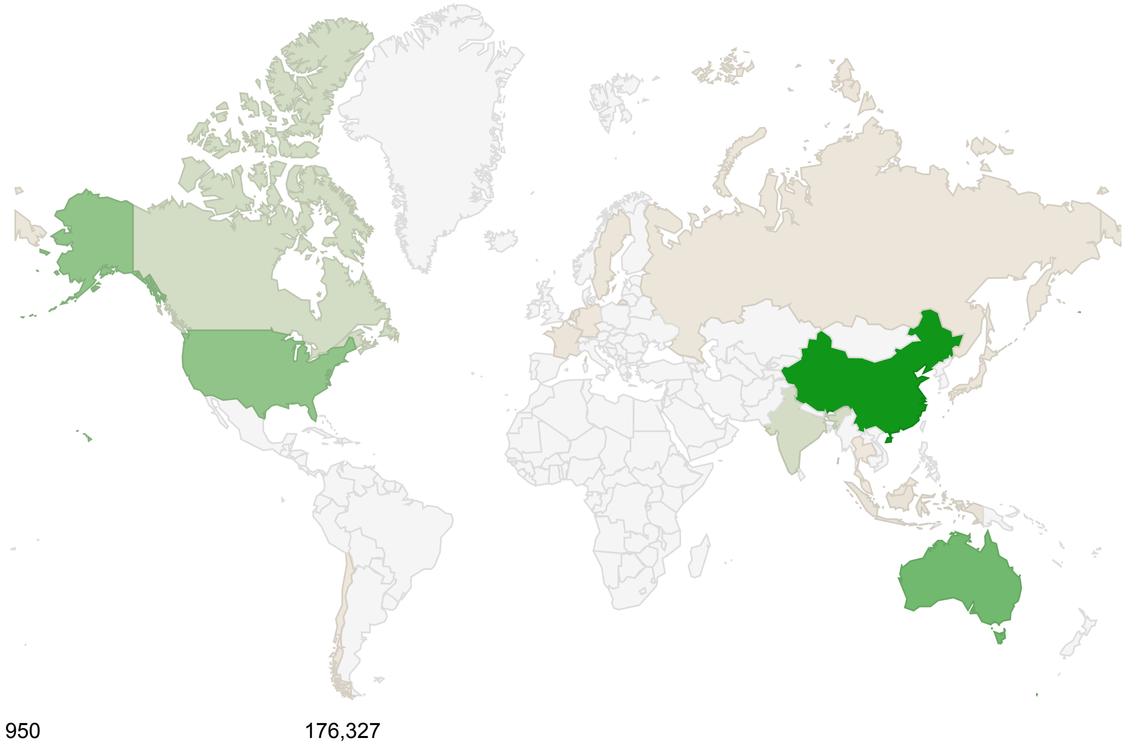
Trends

- The top attacker country was China with 176327 unique attackers (37.00%).
- The top Trojan C&C server detected was Heodo with 49 instances detected.
- The top phishing campaign detected was against Facebook accounts with 236 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	176327	37.00%
Australia	99681	21.00%
United States	75072	16.00%
Canada	22671	4.00%
India	21806	4.00%
Netherlands	6588	1.00%
Indonesia	6439	1.00%
Hong Kong	5695	1.00%
United Kingdom	4846	1.00%
France	4055	0%
Russia	3409	0%
Sweden	3242	0%
Japan	3239	0%
Singapore	2113	0%
Germany	1923	0%
Malaysia	1772	0%
Chile	1623	0%
Thailand	950	0%

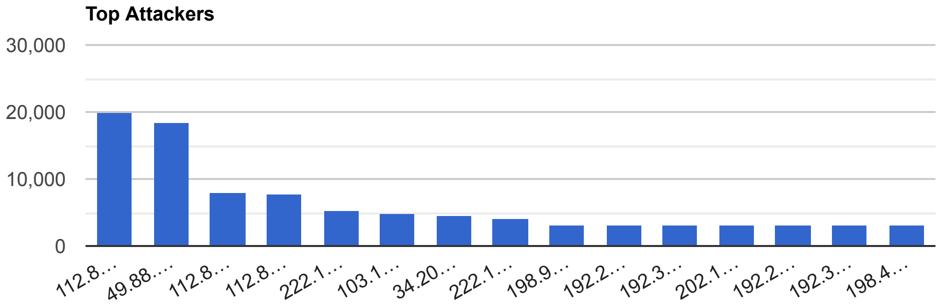




Top Attacking Hosts

Host	Occurrences
112.85.42.187	20076
49.88.112.115	18523
112.85.42.189	8170
112.85.42.88	7767
222.186.30.59	5482

103.138.149.6	4859
34.200.247.158	4735
222.186.52.131	4189
198.97.190.53	3282
192.203.230.10	3251
192.36.148.17	3242
202.12.27.33	3239
192.228.79.201	3234
192.33.4.12	3231
198.41.0.4	3227



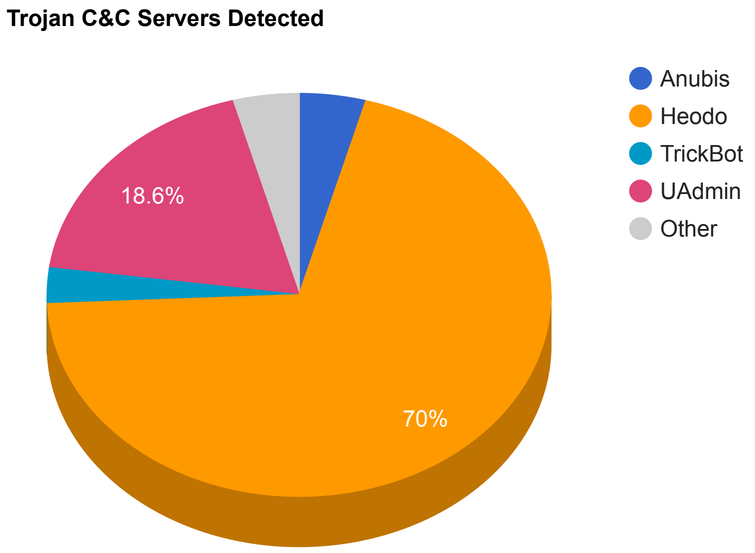
Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN
133441	South Korea	CLOUDITIDC-KR CloudITIDC Global, HK
14618	United States	AMAZON-AES, US
9105	United Kingdom	TISCALI-UK TalkTalk Communications Limited, GB
1508	United States	DNIC-AS-01508, US
21556	United States	NARC-EROOT, US
29216	Sweden	I-ROOT DNS root name server i.root-servers.net., SE
7500	Japan	M-ROOT-DNS WIDE Project, JP
394353	United States	BROOT-AS, US
2149	France	COGENT-2149, US
32651 396549 396566 396570 396571 396574 397197 397203	United States	VGRS-AC24, US VRSN-AC50-340, US VRSN-AC50-340, US VRSN-AC50-340, US VRSN-AC50-340, US VRSN-AC50-340, US VRSN-AC28, US VRSN-AC28, US

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	3	185.209.1.115 , 45.141.84.85 , 8.208.84.18
FlexNet	1	8.209.97.194

Heodo	49	112.185.64.233 , 112.78.142.170 , 113.203.250.121 , 116.202.234.183 , 118.70.15.19 , 137.119.36.33 , 152.169.22.67 , 153.163.83.106 , 153.232.188.106 , 162.249.220.190 , 168.0.97.6 , 173.94.215.84 , 174.137.65.18 , 175.29.183.2 , 177.94.227.143 , 178.128.14.92 , 178.238.232.46 , 181.126.54.234 , 181.137.229.1 , 185.33.0.233 , 186.109.104.67 , 186.109.152.201 , 187.161.206.24 , 190.128.173.10 , 197.221.158.162 , 197.249.6.179 , 200.114.213.233 , 202.4.57.96 , 219.92.8.17 , 220.254.198.228 , 24.135.1.177 , 41.84.237.198 , 41.84.248.134 , 45.173.88.33 , 60.125.114.64 , 64.183.73.122 , 65.36.62.20 , 68.188.112.97 , 70.121.172.89 , 73.213.208.163 , 81.129.198.57 , 82.163.245.38 , 85.109.159.61 , 85.25.207.108 , 86.57.216.23 , 86.98.143.163 , 89.186.91.200 , 93.147.212.206 , 98.109.204.230
Nexus	1	62.113.118.92
PurpleWave	1	188.120.235.130
TrickBot	2	2.57.184.70 , 37.220.0.28
UAdmin	13	107.173.24.170 , 170.81.40.234 , 185.212.148.253 , 185.94.191.6 , 193.23.126.213 , 194.62.29.25 , 199.192.19.30 , 23.254.228.25 , 37.221.113.19 , 45.141.84.163 , 63.250.37.44 , 63.250.47.109 , 92.42.46.104



5f155b6f61e7419a	da8ae6f07b48f1abe6590c2440004ea4db5becc9/details	SAService.exe	SAService	urazo::tpd
26b2996b69542d039c303e2fee6dac81	https://www.virustotal.com/gui/file/9836cf123caa799eaf57a449ba6da0cdecf0445f58a8238fa0d98b19e93cdb22/details	226a60f6-4340-45e9-9b01-d95106369b83	N/A	W32.9836CF123C-100.SBX.TG

Top Phishing Campaigns

Phishing Target	Count
PayPal	21
Other	1425
Amazon.com	10
Microsoft	8
RuneScape	8
Facebook	236
Netflix	1
Halifax	6
Virustotal	14
Yahoo	1
LinkedIn	2
Adobe	6
Google	4
EE	1
Apple	3
Steam	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-2020-1147 Microsoft Sharepoint Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the process responsible for deserialization of the XML content.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	07/14/2020	08/20/2020
CVE-2020-1464 Microsoft Windows Spoofing Vulnerability Microsoft	A spoofing vulnerability exists when Windows incorrectly validates file signatures. An attacker who successfully exploited this vulnerability could bypass security features and load improperly signed files. In an attack scenario, an attacker could bypass security features intended to prevent improperly signed files from being loaded	CVSSv3BaseScore:5.3(AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)	08/17/2020	08/21/2020
CVE-2020-9715 Adobe Acrobat Reader User After Free Vulnerability Adobe	A use-after-free vulnerability could allow remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. The specific flaw exists within the handling of ESObject data objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	08/19/2020	08/19/2020

CVE-2020-3411 Cisco DNA Center Information Disclosure Vulnerability Cisco	A vulnerability in Cisco DNA Center software could allow an unauthenticated remote attacker access to sensitive information on an affected system. The vulnerability is due to improper handling of authentication tokens by the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	08/17/2020	08/21/2020
CVE-2020-3698 Qualcomm Out-Of-Bounds Memory Corruption Vulnerability Qualcomm	An Out of bound write happens in the component QoS DSCP when mapping due to improper input validation for data received from association response frame in Qualcomm Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music and Snapdragon Wearables (ChipSoftware).	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/30/2020	07/30/2020

CVE-2019-16759 vBulletin Remote Code Execution Vulnerability vBulletin	vBulletin allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request. The vulnerability was disclosed through an 18-line exploit that was published on Monday by an unidentified person. The exploit allows unauthenticated attackers to remotely execute malicious code on just about any vBulletin server.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	09/24/2019	08/19/2020
CVE-2020-3433 Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability Cisco	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	08/17/2020	08/20/2020