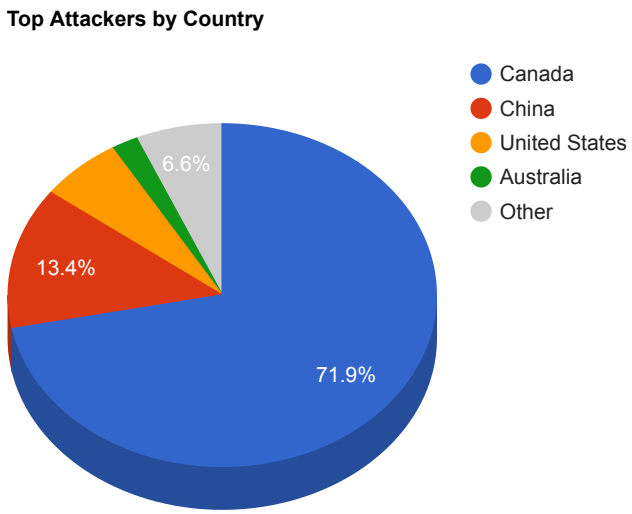
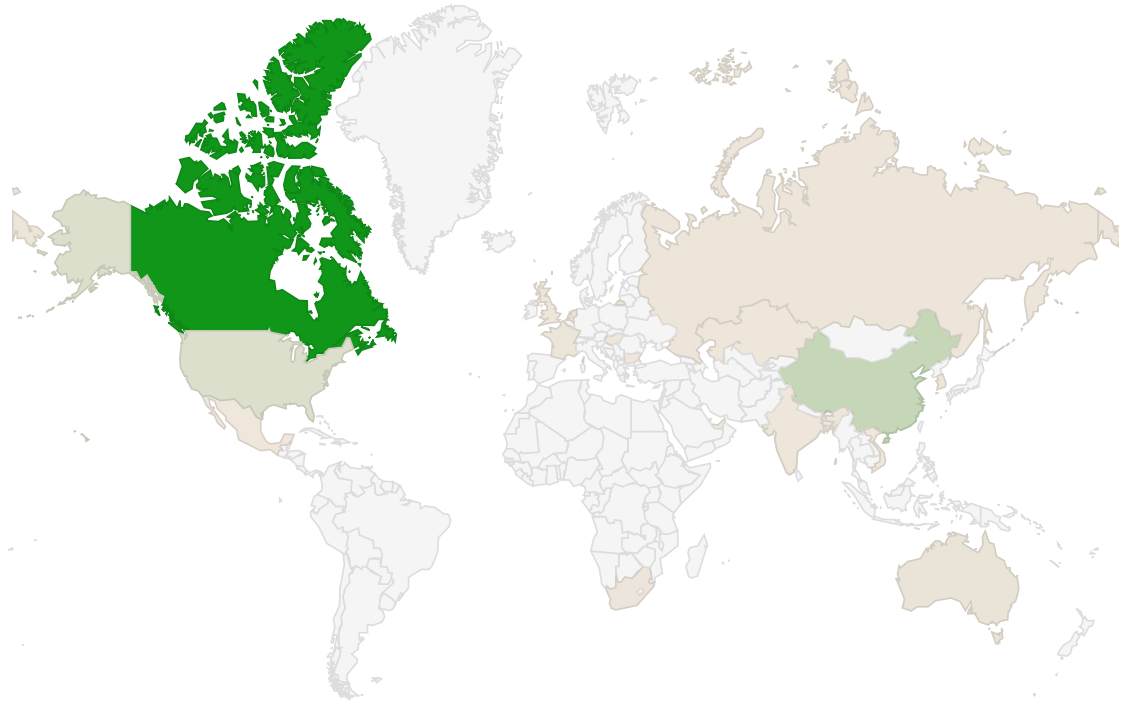
Trends

- The top attacker country was Canada with 130713 unique attackers (70.00%).
- The top Trojan C&C server detected was TrickBot with 29 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
Canada	130713	70.00%
China	24298	13.00%
United States	11289	6.00%
Australia	3683	1.00%
France	1909	1.00%
Netherlands	1838	0%
Russia	1418	0%
South Africa	1172	0%
South Korea	790	0%
Kazakhstan	789	0%
United Kingdom	718	0%
Bulgaria	603	0%
India	595	0%
Singapore	515	0%
Vietnam	392	0%
Mexico	389	0%
Hungary	283	0%
Bangladesh	262	0%
United Arab Emirates	261	0%



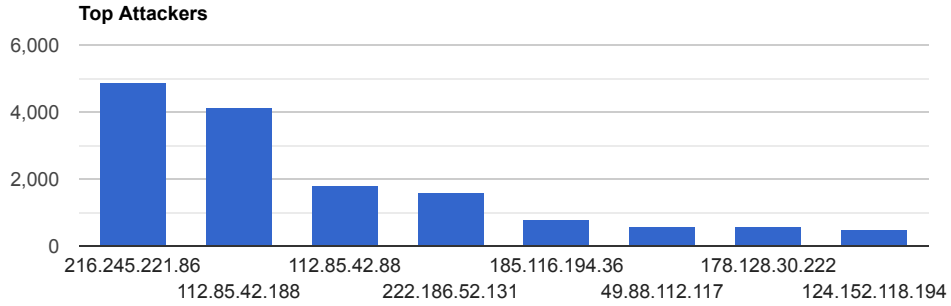


261 130,713

Top Attacking Hosts

Host	Occurrences
216.245.221.86	4902
112.85.42.188	4144
112.85.42.88	1784
222.186.52.131	1632
185.116.194.36	757

49.88.112.117	593
178.128.30.222	565
124.152.118.194	504



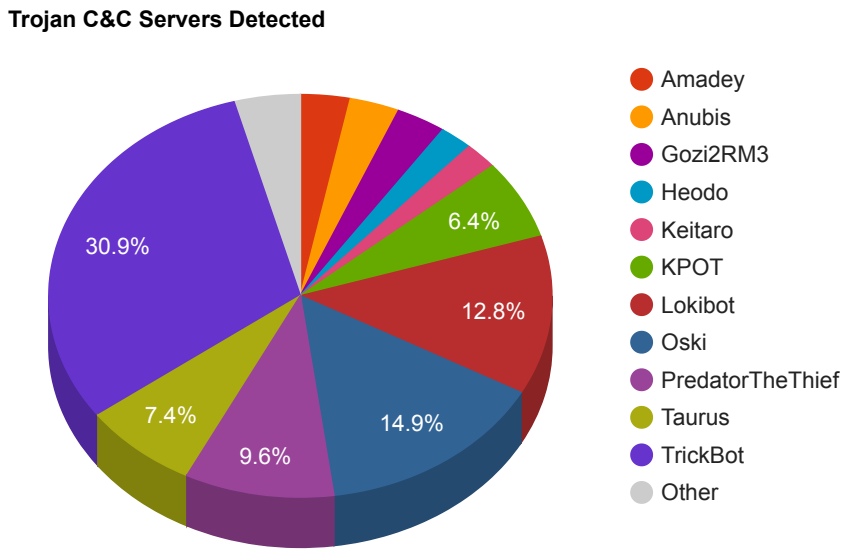
Top Network Attackers

ASN	Country	Name
46475	United States	LIMESTONENETWORKS, US
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
23650	China	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN
202958	Kazakhstan	HOSTER-, KZ
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
14061	Singapore	DIGITALOCEAN-ASN, US

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	178.62.14.31
Amadey	3	217.8.117.17 , 217.8.117.76 , 45.147.197.150
Anubis	3	5.101.50.50 , 8.209.104.170 , 84.38.183.209
GodzillaLoader	1	217.8.117.45
Gozi2RM3	3	195.2.71.175 , 94.103.91.32 , 95.174.65.226
Heodo	2	153.133.224.78 , 75.139.38.211
Keitaro	2	88.119.171.152 , 88.119.171.153
KPOT	6	63.250.47.170 , 8.209.79.7 , bumboxik.asia , dikiy.icu , dikiy.website , goodtemp.top
Lokibot	12	104.31.71.68 , 142.11.249.189 , 172.67.219.195 , 185.159.153.117 , 185.185.69.74 , 185.207.38.108 , 185.55.227.103 , 185.98.87.97 , 31.184.254.119 , 46.249.205.36 , 79.124.8.8 , 80.249.147.103
Oski	14	104.24.125.52 , 172.67.216.22 , 185.212.130.9 , 188.165.218.20 , 195.133.147.220 , 195.133.201.172 , 199.192.24.69 , 213.108.4.38 , 213.178.155.74 , 23.91.70.155 , 47.241.11.25 , 5.101.153.82 , 63.250.47.241 , 82.202.227.174

PredatorTheThief	9	141.8.192.151 , 141.8.197.42 , 172.105.52.237 , 185.238.138.146 , 185.50.25.51 , 81.16.141.225 , 81.177.141.241 , 95.211.16.66 , stranskl.site
RaccoonStealer	1	dq7shlx5o67t64ljuzisyp34s3n7vepnhc5ijt5hjh433qzaatyj5bid.onion
Taurus	7	104.18.49.141 , 104.24.105.6 , 172.67.184.127 , 45.138.72.7 , 45.153.241.9 , 49.51.169.175 , cloudstage.xyz
TrickBot	29	107.175.197.154 , 131.255.82.24 , 134.119.191.22 , 134.119.191.55 , 144.91.76.213 , 162.248.225.57 , 185.120.56.37 , 185.164.33.115 , 185.206.212.44 , 185.255.79.108 , 193.37.212.124 , 193.9.60.148 , 195.123.221.93 , 195.123.240.36 , 195.161.114.99 , 212.80.217.89 , 45.155.173.167 , 45.230.176.143 , 45.67.228.186 , 46.173.218.51 , 46.173.219.184 , 82.118.22.57 , 85.10.234.175 , 85.143.222.208 , 85.204.116.121 , 85.204.116.53 , 92.38.163.171 , 93.189.44.203 , 95.181.198.137
UAdmin	1	81.29.134.76



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
4709a871ba0c0a3598eb78dadfe90aec	https://www.virustotal.com/gui/file/8bf5d91950033ef6f40ffbd2340d8b0add0ffdcbbb4cfd309218d6d0810d85be/details	tapout.exe	N/A	Win.Dropper.Zudochka::in03.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/detection	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/detection	mf2016341595.exe	N/A	Win.Downloader.Generic::1201

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-2020-9484 Apache Tomcat Remote Code Execution Vulnerability Apache	When using Apache Tomcat versions if a) an attacker is able to control the contents and name of a file on the server and b)the server is configured to use the Persistence Manager with a FileStore	7.0(AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/20/2020	06/15/2020

CVE-2020-0796 Microsoft Windows SMBv3 Client/Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server.	10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	03/12/2020	06/11/2020
CVE-2020-3956 VMware Cloud Director Code Injection Vulnerability VMware	VMware Cloud Director do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access.	9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	05/20/2020	06/03/2020

CVE-2020-13401 Docker Engine IPv6 Address Spoofing Vulnerability Docker	An issue exists in Docker Engine where an attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service. A user is able to create containers with CAP_NET_RAW privileges on an affected cluster can intercept traffic from other containers on the host or from the host itself.	9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	06/02/2020	06/10/2020
CVE-2020-1301 Microsoft Windows SMB Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.	7.5(AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/15/2020
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.	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-2020-1206 Microsoft Windows SMBv3 Client/Server Information Disclosure Vulnerability Microsoft	An information disclosure vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server. To exploit the vulnerability against a client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it.	8.6(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)	06/09/2020	06/12/2020