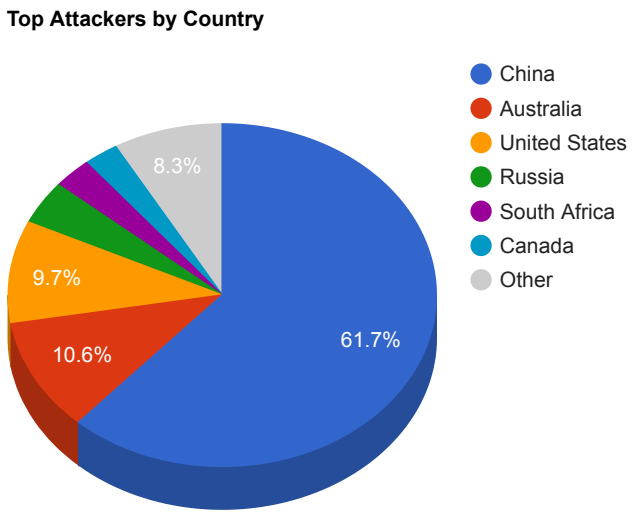
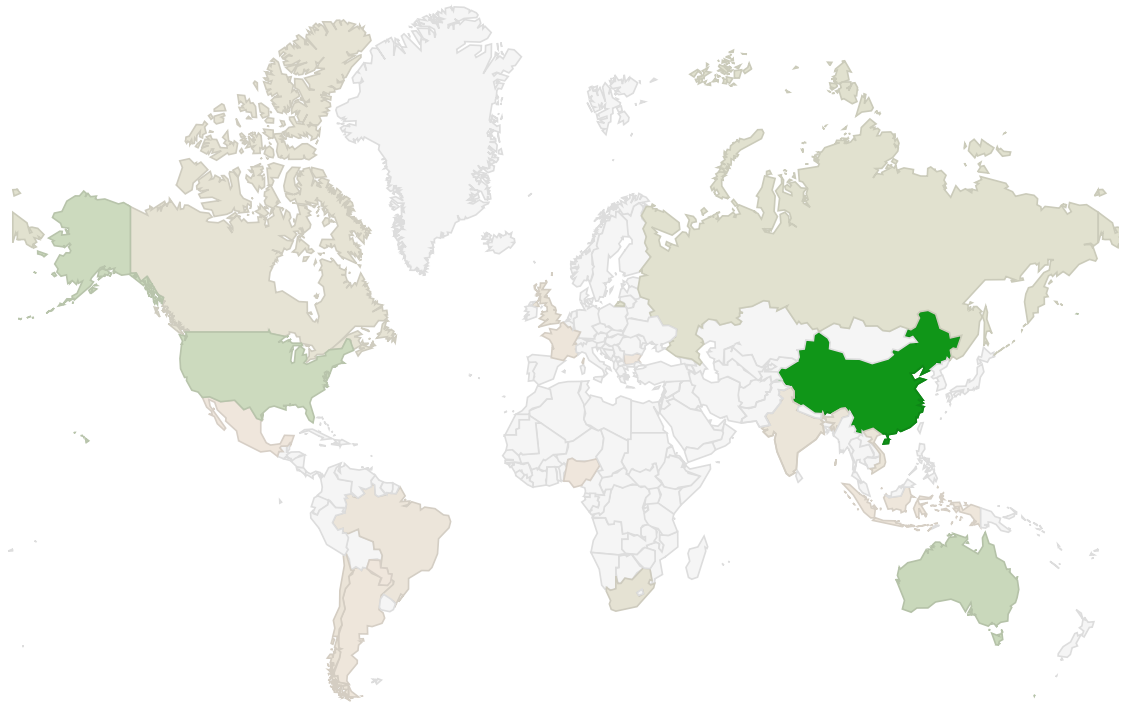
Trends

- The top attacker country was China with 567852 unique attackers (58.00%).
- The top Trojan C&C server detected was Trickbot with 23 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	567852	58.00%
Australia	97729	10.00%
United States	89184	9.00%
Russia	38043	3.00%
South Africa	26896	2.00%
Canada	24375	2.00%
United Kingdom	13403	1.00%
Chile	12598	1.00%
India	10876	1.00%
Vietnam	10390	1.00%
Brazil	7946	0%
France	6770	0%
Indonesia	3939	0%
Argentina	3699	0%
Mexico	2429	0%
Bulgaria	1552	0%
Nigeria	1496	0%
Paraguay	1276	0%

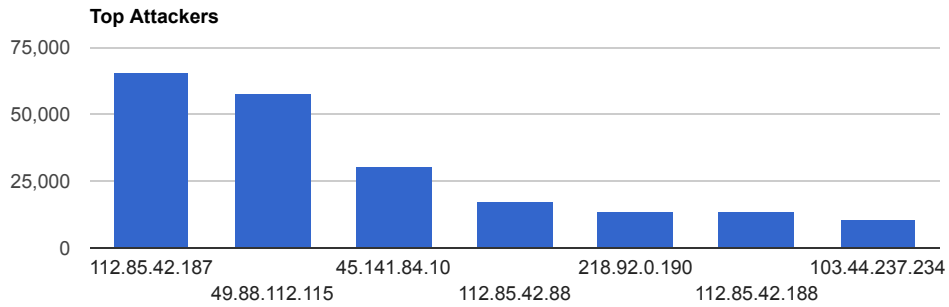




1,276 567,852

Top Attacking Hosts

Host	Occurrences
112.85.42.187	65730
49.88.112.115	57845
45.141.84.10	30584
112.85.42.88	17615
218.92.0.190	14081
112.85.42.188	13939
103.44.237.234	10941

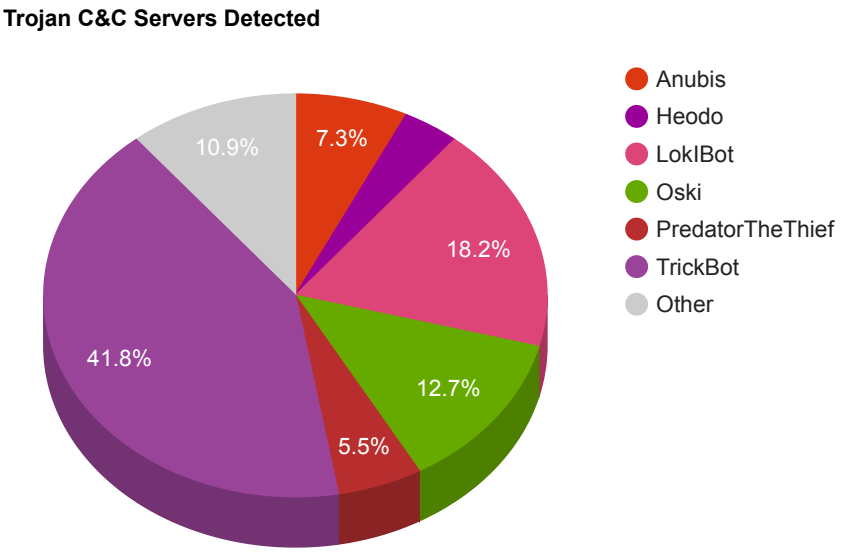


Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
206728	Russia	MEDIALAND-AS, RU
4816	China	CHINANET-IDC-GD China Telecom (Group), CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Amadey	1	188.120.233.19
Anubis	4	176.121.14.173 , 8.208.102.203 , 84.38.180.68 , 84.38.182.177
Azorult	1	185.212.148.78
Gozi2RM3	1	195.123.245.212
Heodo	2	24.1.189.87 , 41.215.92.157
KPOT	1	8.208.102.118
LokIBot	10	101.50.1.17 , 103.17.8.47 , 104.27.162.37 , 172.67.192.52 , 176.223.209.5 , 194.180.224.87 , 45.143.138.143 , 79.124.8.8 , 84.38.182.128 , 94.199.200.248
Oski	7	109.94.208.119 , 195.133.197.142 , 199.192.24.69 , 217.8.117.45 , 45.143.93.28 , 45.147.198.62 , 5.101.50.55
PredatorTheThief	3	141.8.192.151 , 81.16.141.225 , 81.177.141.11
Taurus	1	45.153.241.9
TrickBot	23	107.172.141.128 , 148.251.185.180 , 164.68.120.59 , 164.68.120.62 , 172.245.185.184 , 185.164.33.125 , 185.234.72.230 , 185.234.72.231 , 185.65.202.58 , 192.3.247.18 , 194.5.250.183 , 194.5.250.184 , 195.133.197.46 , 45.155.173.166 , 45.155.173.224 , 51.77.112.240 , 62.108.35.175 , 62.108.35.221 , 62.108.35.225 , 85.143.219.23 , 85.204.116.149 , 85.204.116.155 , 92.38.163.8
UAdmin	1	46.29.161.2



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
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg
a10a6d9dfc0328a391a3fdb1a9fb18db	https://www.virustotal.com/gui/file/094d4da0ae3ded8b936428bb7393c77aaedd5efb5957116afd4263bd7edc2188/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::100.sbx.vioc
73d1de319c7d61e0333471c82f2fc104	https://www.virustotal.com/gui/file/32155b070c7e1b9d6bdc021778c5129edfb9cf7e330b8f07bb140dedb5c9aae7/details	SAntivirusService.exe	AntivirusService	Win.Dropper.Zudochka::in03.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/detection	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201

Top Phishing Campaigns

Phishing Target	Count
Other	717
Twitter	1
Facebook	25
Microsoft	4
Netflix	1
Three	10
PayPal	5
Amazon.com	3
Virustotal	3
Blockchain	1
ZML	1
Dropbox	1
Bradesco	1
Steam	1
RuneScape	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-2020-1300 Microsoft Windows Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when Microsoft Windows fails to properly handle cabinet files. To exploit the vulnerability, an attacker would have to convince a user to either open a specially crafted cabinet file or spoof a network printer and trick a user into installing a malicious cabinet file disguised as a printer driver.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/16/2020

CVE-2020-1206 Microsoft Windows SMBv3 Client/Server Remote Code Execution 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 target.	CVSSv3BaseScore:8.6(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)	06/09/2020	06/12/2020
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
CVE-2020-5410 Spring Cloud Config Directory Traversal Vulnerability VMWare	Spring Cloud Config allows applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	06/02/2020	06/04/2020

CVE-2020-1301 Microsoft Windows SMB Authenticated 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. To exploit the vulnerability an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server.	CVSSv3BaseScore: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. 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-2020-0796 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.	CVSSv3BaseScore: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-2020-13160 AnyDesk UDP Discovery Remote Code Execution Vulnerability AnyDesk	A format string vulnerability exists in AnyDesk that can be exploited for remote code execution. By sending a single UDP packet to the target machine, an attacker can successfully exploit the discovered format string vulnerability to gain Remote Code Execution.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	06/09/2020	06/11/2020
CVE-2018-13379 Fortinet FortiOS Directory Traversal Vulnerability Fortinet	Fortinet FortiOS is exposed to a directory traversal vulnerability because it fails to properly sanitize user supplied input. A path traversal vulnerability in the FortiOS SSL VPN web portal may allow an unauthenticated attacker to download FortiOS system files through specially crafted HTTP resource requests.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	06/04/2019	01/22/2020