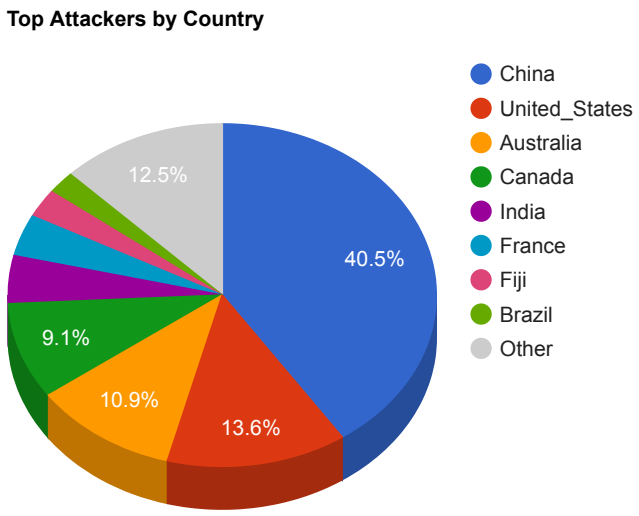
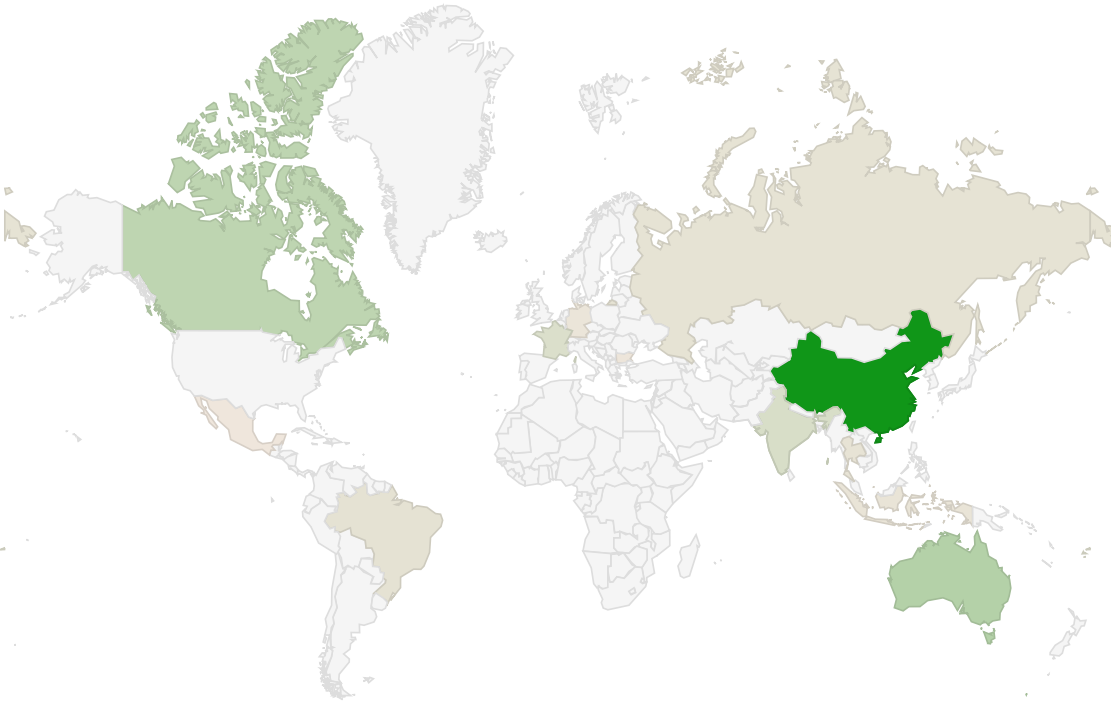
Trends

- The top attacker country was China with 71942 unique attackers (37.00%).
- The top Trojan C&C server detected was TrickBot with 16 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	71942	37.00%
United States	24091	12.00%
Australia	19431	10.00%
Canada	16193	8.00%
India	8003	4.00%
France	6974	3.00%
Fiji	4759	2.00%
Brazil	3798	1.00%
Russia	3432	1.00%
Thailand	3190	1.00%
South Korea	2767	1.00%
South Africa	2645	1.00%
Indonesia	2427	1.00%
Germany	1802	0%
United Kingdom	1767	0%
Hong Kong	1454	0%
Bulgaria	1411	0%
Mexico	748	0%
Macao	619	0%



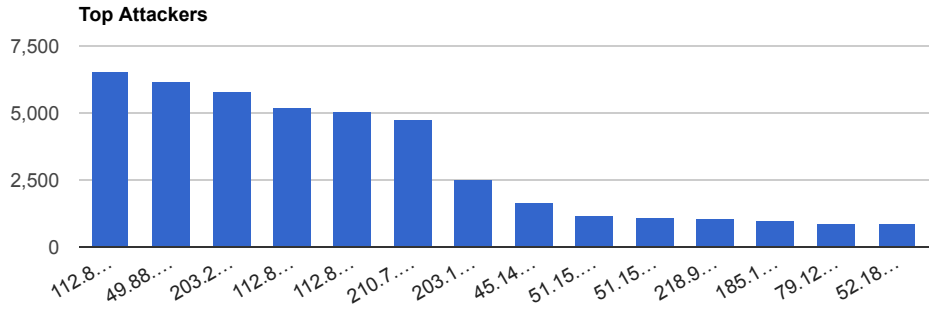


619 71,942

Top Attacking Hosts

Host	Occurrences
112.85.42.187	6531
49.88.112.115	6135
112.85.42.189	5211
112.85.42.88	5061
210.7.22.74	4759
203.151.47.26	2495
45.145.66.250	1661

51.15.152.61	1156
51.158.24.255	1126
218.92.0.192	1007
185.135.74.60	951
79.124.62.74	863

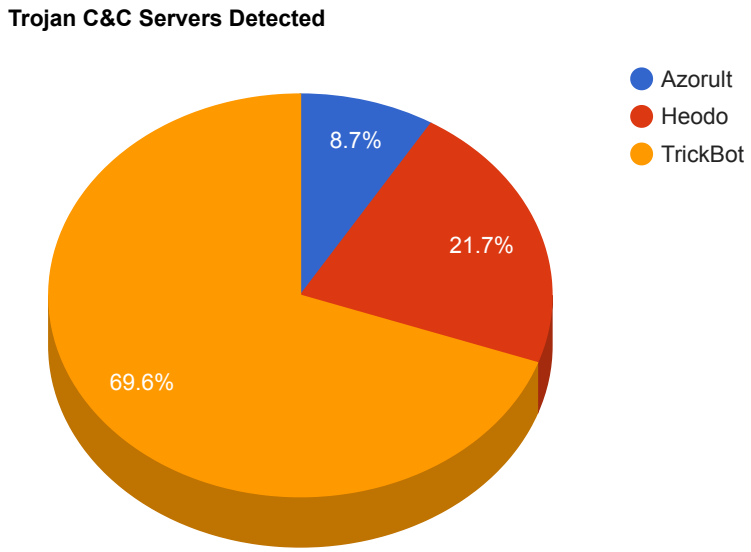


Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4638	Fiji	IS-FJ-AS Telecom Fiji Limited, FJ
4618	Thailand	INET-TH-AS Internet Thailand Company Limited, TH
50340	Russia	SELECTEL-MSK, RU
12876	France	Online SAS, FR
55720	Iran	GIGABIT-MY Gigabit Hosting Sdn Bhd, MY
207812	Bulgaria	DM_AUTO, BG

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	2	mmakaronagre.xyz , wildberriesqa.xyz
Heodo	5	109.117.53.230 , 181.134.9.162 , 186.70.127.199 , 198.27.69.201 , 58.153.68.176
TrickBot	16	162.216.0.186 , 185.14.31.44 , 185.164.32.148 , 185.99.2.183 , 185.99.2.191 , 194.5.249.157 , 194.87.145.86 , 195.123.221.37 , 195.123.221.77 , 204.155.30.121 , 45.155.173.211 , 5.182.211.223 , 5.188.133.193 , 85.204.116.144 , 85.204.116.198 , 86.104.194.82



34560233e751b7e95f155b6f61e7419a	https://www.virustotal.com/gui/file/8b4216a7c50599b11241876ada8ae6f07b48f1abe6590c2440004ea4db5becc9/details	SAService.exe	SAService	PUA.Win.Dropper.Seguraz o::tpd
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/094d4da0ae3ded8b936428bbb7393c77aaedd5efb5957116afd4263bd7edc2188/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::100.sbx.vioc
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Seguraz o::95.sbx.tg

Top Phishing Campaigns

Phishing Target	Count
Other	530
Facebook	20
RuneScape	8
Google	7
Americanas.com	2
Yahoo	2
Twitter	1

Steam	1
Microsoft	1
Mastercard	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-2020-6287 SAP NetWeaver Application Server JAVA Multiple Vulnerabilities SAP	SAP NetWeaver AS JAVA (LM Configuration Wizard) does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	07/14/2020	07/16/2020
CVE-2020-1350 Microsoft Windows DNS Server Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	07/14/2020	07/20/2020

CVE-2020-14664 Oracle Java SE Critical Vulnerability Oracle	A vulnerability exists in the Java SE product of Oracle Java SE. In order to exploit the vulnerability, it allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE.	CVSSv3BaseScore:8.3(AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)	07/15/2020	07/20/2020
CVE-2020-5902 F5 BIG-IP Remote Code Execution Vulnerability F5	F5 BIG-IP is exposed to remote code execution vulnerability. The vulnerability that has been actively exploited in the wild allows attackers to read files, execute code or take complete control over vulnerable systems having network access.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/01/2020	07/21/2020
CVE-2019-19781 Citrix Application Delivery Controller and Gateway Directory Traversal Vulnerability Citrix	A vulnerability exists in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway that, if exploited, could allow an unauthenticated attacker to perform arbitrary code execution. This vulnerability exploits a directory traversal to execute an arbitrary command payload.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	12/27/2019	01/08/2020

CVE-2020-2021 Palo Alto Networks PAN-OS Authentication Bypass in SAML Authentication Vulnerability Palo Alto Networks	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	06/29/2020	07/06/2020
CVE-2020-1421 Microsoft LNK Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. The attacker could present to the user a removable drive, or remote share, that contains a malicious .LNK file and an associated malicious binary. When the user opens this drive(or remote share) in Windows Explorer, or any other application that parses the .LNK file, the malicious binary will execute code of the attacker's choice, on the target system.	CVSSv3BaseScore:7.5(AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)	07/14/2020	07/15/2020