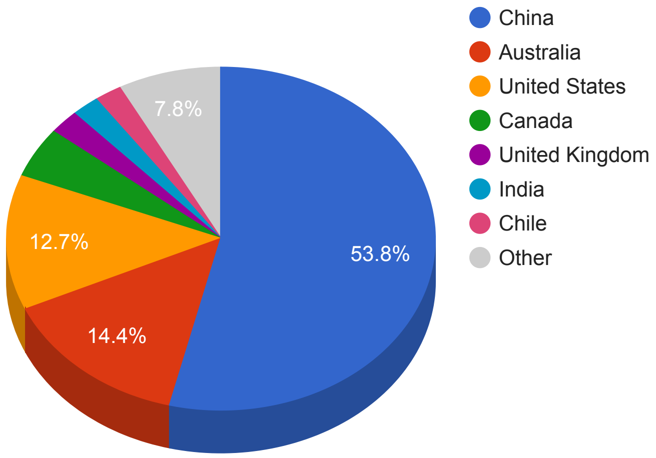
Trends

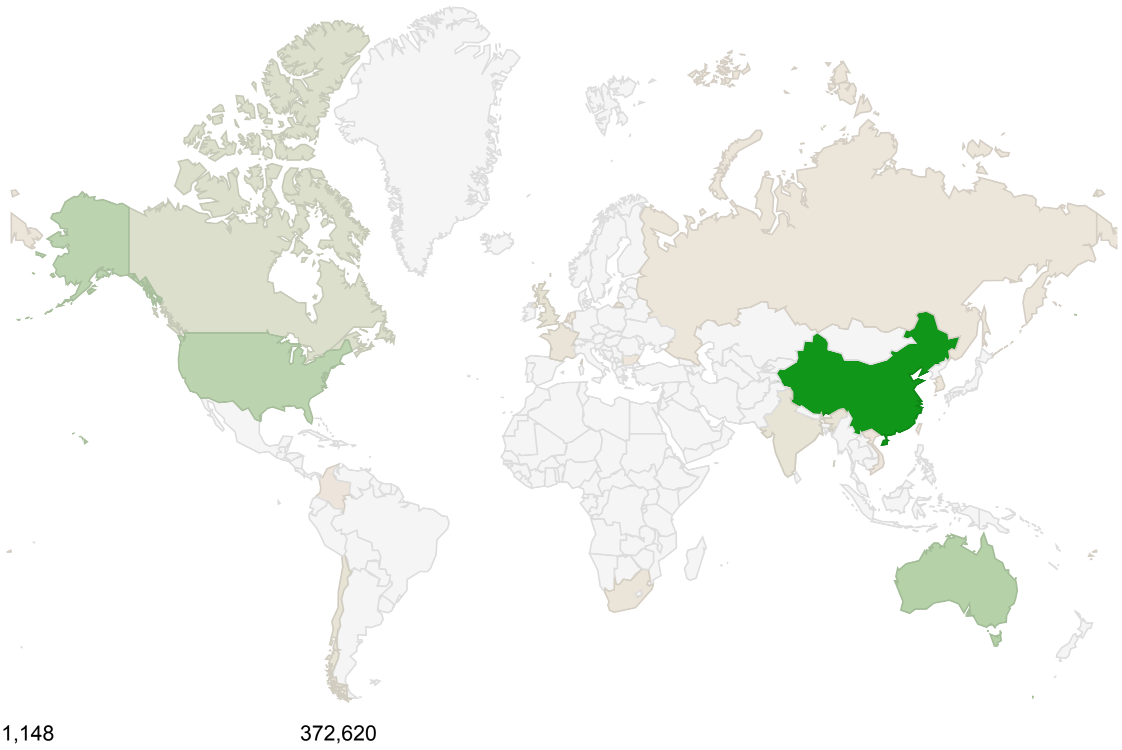
- The top attacker country was China with 372620 unique attackers (51.00%).
- The top Trojan C&C server detected was TrickBot with 10 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	372620	51.00%
Australia	99708	13.00%
United States	87998	12.00%
Canada	33097	4.00%
United Kingdom	15766	2.00%
India	14497	2.00%
Chile	14245	1.00%
France	10317	1.00%
South Africa	7185	1.00%
Netherlands	6276	0%
Russia	5657	0%
Fiji	4847	0%
South Korea	4053	0%
Vietnam	3979	0%
Colombia	3737	0%
Hong Kong	2545	0%
Singapore	2268	0%
Bulgaria	2190	0%
Taiwan	1148	0%

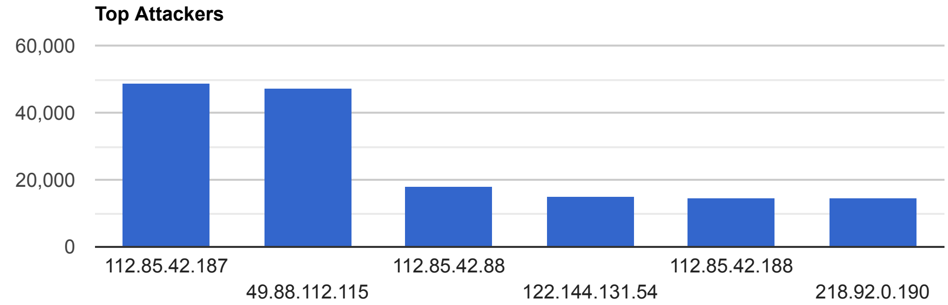
Top Attackers by Country





Top Attacking Hosts

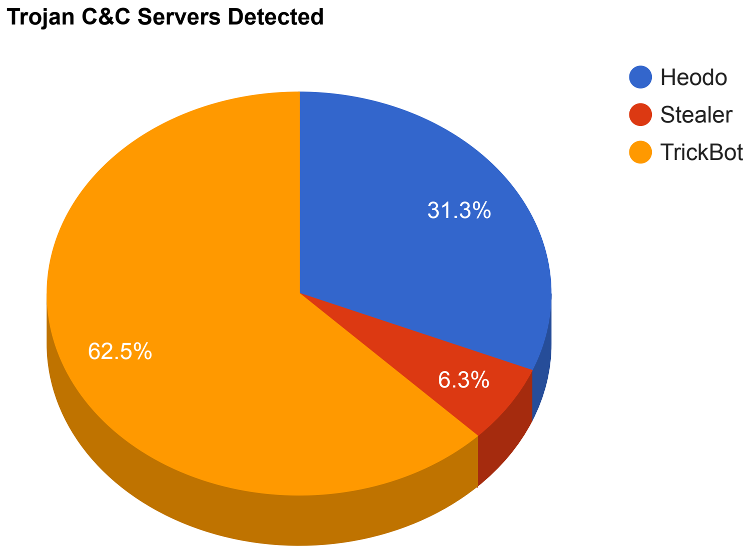
Host	Occurrences
112.85.42.187	48566
49.88.112.115	47105
112.85.42.88	17939
122.144.131.54	15144
112.85.42.188	14679
218.92.0.190	14533



		E CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
17775	China	STN-CN shanghai science and technology network communication limited company, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	5	181.120.79.227 , 186.250.52.226 , 189.218.165.63 , 190.194.242.254 , 93.156.165.186
Stealer	1	172.67.139.160
TrickBot	10	104.161.32.109 , 162.216.0.181 , 185.142.99.149 , 188.120.255.141 , 188.120.255.249 , 194.156.99.124 , 194.5.249.109 , 217.12.209.151 , 66.70.218.37 , 92.63.105.67



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name

a10a6d9dfc0328a391a3fdb1a9fb18db	https://www.virustotal.com/gui/file/094d4da0ae3ded8b936428bb7393c77aaedd5efb5957116afd4263bd7edc2188/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::100.sbx.vioc
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	FlashHelperServices.exe	FlashHelperServices	Win.Exploit.Shadowbrokers::5A5226262.auto.talos
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
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::95.sbx.tg

Top Phishing Campaigns

Phishing Target	**Count**
Other	1614
Facebook	60
PayPal	46
Virustotal	2
RuneScape	25
Google	9
Three	8
Blockchain	4
Microsoft	13
Amazon.com	11
Coinbase	2
Americanas.com	1
DHL	1
Steam	3
EE	3
Netflix	1
Yahoo	2
Caixa	2
Apple	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-2020-5902 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	07/08/2020
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-2020-12828 AnchorFree OpenVPN SDK Privilege Escalation Vulnerability Pango	An issue was discovered in AnchorFree VPN SDK. The VPN SDK service takes certain executable locations over a socket bound to localhost. Binding to the socket and providing a path where a malicious executable file resides leads to executing the malicious executable file with SYSTEM privileges.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	05/21/2020	06/02/2020
CVE-2020-2012 Palo Alto Networks PAN-OS XML External Entity Reference Vulnerability Palo Alto Networks	Improper restriction of XML external entity reference ('XXE') vulnerability in Palo Alto Networks Panorama management service allows remote unauthenticated attackers with network access to the Panorama management interface to read arbitrary files on the system.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	05/13/2020	05/14/2020
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-2020-9497 Apache Guacamole Information Disclosure Vulnerability Apache	Apache Guacamole do not properly validate data received from RDP servers via static virtual channels. If a user connects to a malicious or compromised RDP server, specially-crafted PDUs could result in disclosure of information within the memory of the guacd process handling the connection.	CVSSv3BaseScore:6.5(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)	07/02/2020	07/07/2020