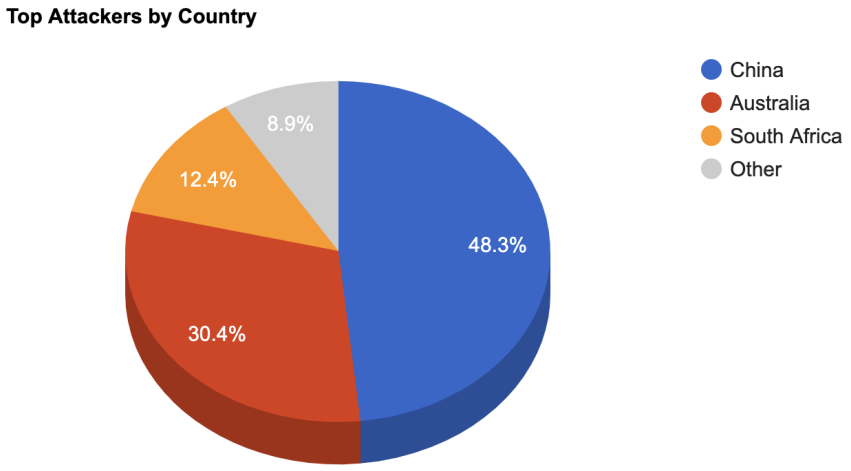
Trends

- The top attacker country was China with 92412 unique attackers (47.00%).
- The top Trojan C&C server detected was Heodo with 55 instances detected.

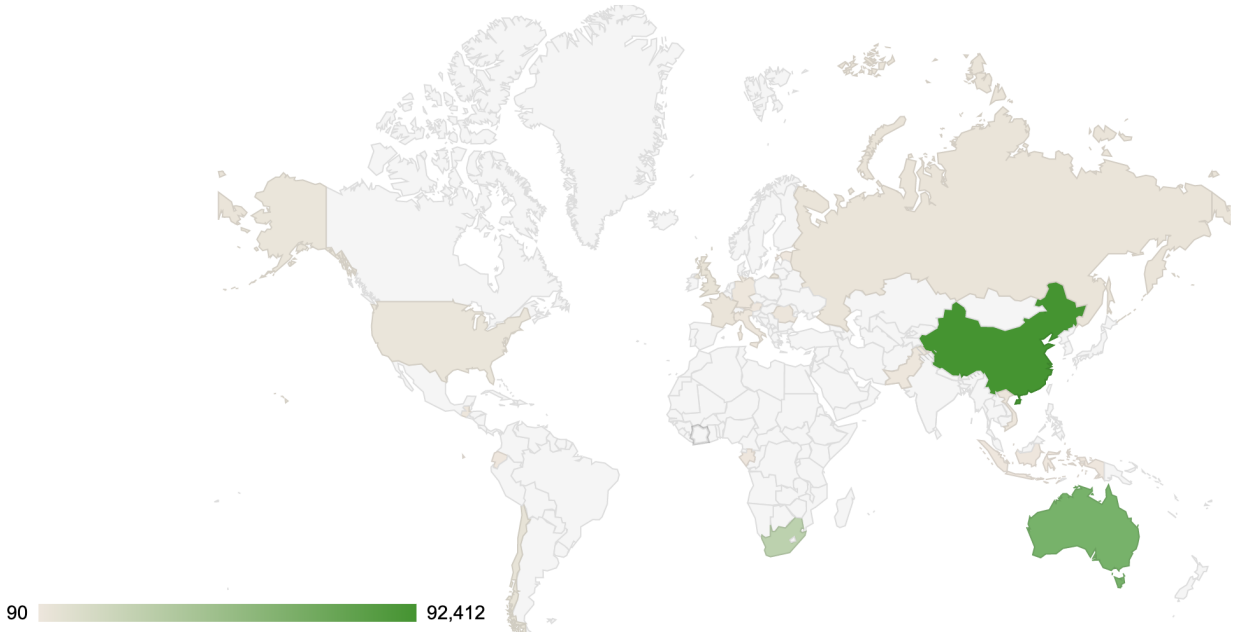
Top Attackers By Country

Country	Occurences	Percentage
China	92412	47.00%
Australia	58064	29.00%
South_Africa	23634	12.00%
Chile	3594	1.00%
United_Kingdom	3194	1.00%
Russia	1914	0%
France	1890	0%
United_States	1727	0%
Vietnam	1053	0%
Romania	812	0%
Guatemala	580	0%
Italy	489	0%
Pakistan	416	0%
Germany	375	0%
Gabon	258	0%
Indonesia	247	0%
Estonia	198	0%

Ecuador	185	0%
Austria	90	0%



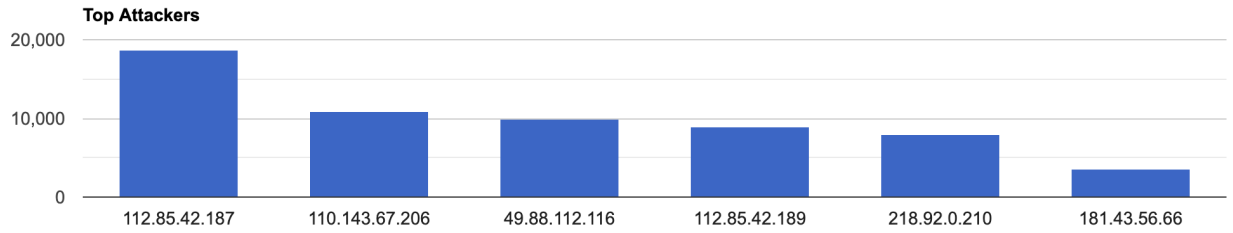
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
112.85.42.187	18714
110.143.67.206	10848
49.88.112.116	9852
112.85.42.189	8943

218.92.0.210	7976
181.43.56.66	3580



Top Network Attackers

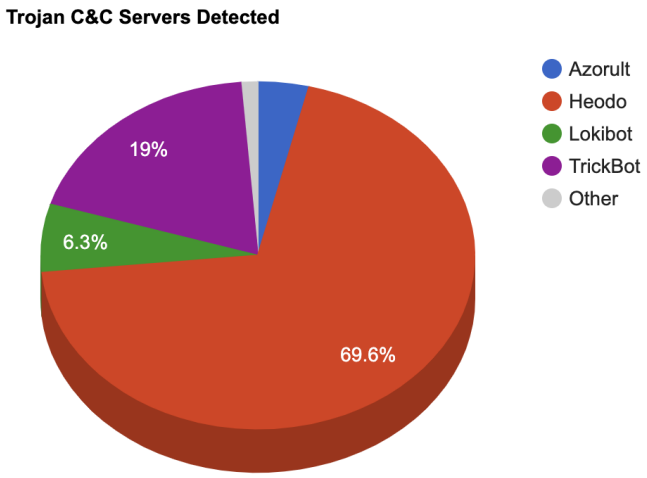
ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
1221	Australia	ASN-TELSTRA Telstra Corporation Ltd, AU
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
6471	Chile	ENTEL CHILE S.A., CL

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AzorUlt	3	142.44.149.175 , 156.96.58.101 , 45.143.138.64
Heodo	55	108.6.140.26 , 115.65.111.148 , 118.200.47.120 , 144.139.228.113 , 150.246.246.238 , 151.231.7.154 , 152.168.248.128 , 153.137.36.142 , 153.183.25.24 , 175.181.7.188 , 176.9.43.37 , 177.103.157.126 , 178.152.92.246 , 178.20.74.212 , 180.33.71.88 , 181.196.27.123 , 185.207.57.205 , 186.138.186.74 , 186.200.205.170 , 186.223.86.136 ,

		188.218.104.226 , 189.78.156.8 , 190.63.7.166 , 195.250.143.182 , 202.175.121.202 , 202.229.211.95 , 203.45.161.179 , 211.192.153.224 , 220.247.70.174 , 222.144.13.169 , 23.92.16.164 , 42.200.226.58 , 45.55.65.123 , 5.199.130.105 , 68.114.229.171 , 68.62.245.148 , 70.180.35.211 , 70.184.9.39 , 72.176.87.136 , 73.125.15.41 , 74.101.225.121 , 74.108.124.180 , 74.130.83.133 , 75.114.235.105 , 75.86.6.174 , 76.104.80.47 , 78.101.70.199 , 81.213.78.151 , 81.214.142.115 , 81.214.253.80 , 87.81.51.125 , 88.225.230.33 , 90.69.145.210 , 91.242.136.103 , 99.229.254.209
KPOT	1	104.31.89.151
Lokibot	5	103.234.209.212 , 107.175.150.73 , 108.167.146.149 , 195.123.222.144 , 91.215.170.245

TrickBot	15	146.185.219.165 , 146.185.253.18 , 164.68.120.56 , 185.178.46.184 , 185.99.2.160 , 194.5.250.155 , 194.87.238.87 , 195.123.216.223 , 5.182.210.230 , 51.89.115.116 , 5.2.75.167 , 5.2.75.93 , 85.143.219.58 , 85.204.116.237 , 93.189.42.146



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos

c2406fc0fce67ae79e625013325e2a68	https://www.virustotal.com/gui/file/1c3ed460a7f78a43bab0ae575056d00c629f35cf7e72443b4e874ede0f305871/details	SegurazoIC.exe	DigitalCommunicationsInc.	PUA.Win.Adware.Ursu::95.sbx.tg
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
7c38a43d2ed9af80932749f6e80fea6f	https://www.virustotal.com/gui/file/c0cdd2a671195915d9ffb5c9533337db935e0cc2f4d7563864ea75c21ead3f94/details	xme64-520.exe	N/A	PUA.Win.File.Coinminer::1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	W32.Generic:Gen.22fz.1201

CVEs with Recently Discovered Exploits

This is a list of recent vulnerabilities for which exploits are available.

CVE, Title, Vendor	Description	CVSS v2 Base Score	Date Created	Date Updated
CVE-2019-19781 Citrix ADC And Citrix Gateway Arbitrary Code Execution Vulnerability Citrix	A vulnerability has been identified 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. Successfully exploiting this issue will allow attackers to execute arbitrary code within the context of the application.	7.5(AV:N/AC:L/Au:N/C:P/I:P/A:P)	12/27/2019	01/08/2020
CVE-2019-9730 Synaptics Audio Driver Vulnerability Synaptics	Incorrect access control in the CxUtilSvc.exe component of the Synaptics (previously Conexant) Audio driver could allow a standard user to increase access privileges to the Windows Registry via an unpublished API.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	06/05/2019	06/07/2019

CVE-2020-3941 VMWare Privilege Escalation Vulnerability VMWare	A vulnerability exists in VMware Tools for windows, which may allow for privilege escalation in the Virtual Machine where Tools is installed. A malicious actor on the guest VM might exploit the race condition and escalate their privileges on a Windows VM.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	01/15/2020	01/24/2020
CVE-2019-1547 OpenSSL vulnerability Multi-Vendor	In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. A local attacker can recover a full key during an ECDSA signature operation.	1.9(AV:L/AC:M/Au:N/C:P/I:N/A:N)	09/10/2019	09/12/2019