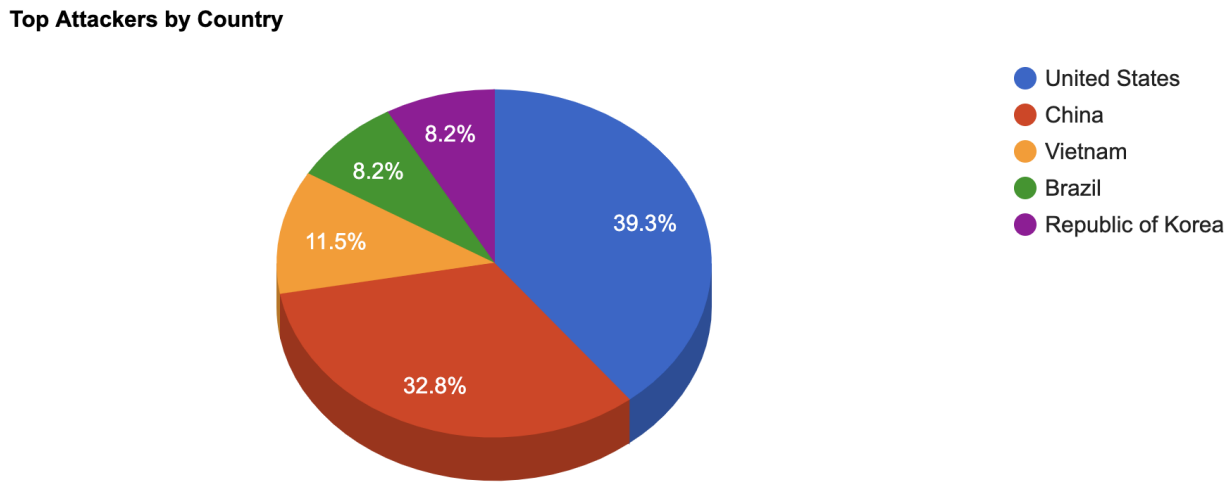
Trends

- The top attacker country was Australia with 75997 unique attackers (37%).
- The top Trojan C&C server detected was Heodo with 75 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
Australia	75997	37.00%
China	72638	35.00%
United States	16619	8.00%
South Africa	6136	3.00%
Italy	3508	1.00%
France	3207	1.00%
Russia	2644	1.00%
South Korea	2304	1.00%
Vietnam	1717	0%
Indonesia	1671	0%
Canada	1646	0%
India	1599	0%
United Kingdom	1551	0%
Brazil	1494	0%
Argentina	1435	0%
Netherlands	1347	0%
Singapore	763	0%
Chile	737	0%

Kyrgyzstan	480	0%



Top Attacking Hosts

Host	Occurrences
112.85.42.187	11435
68.183.236.148	8280
112.85.42.188	6672
49.88.112.116	2803
218.92.0.191	2677
121.201.38.248	2189
192.34.62.227	1150

Top Network Attackers

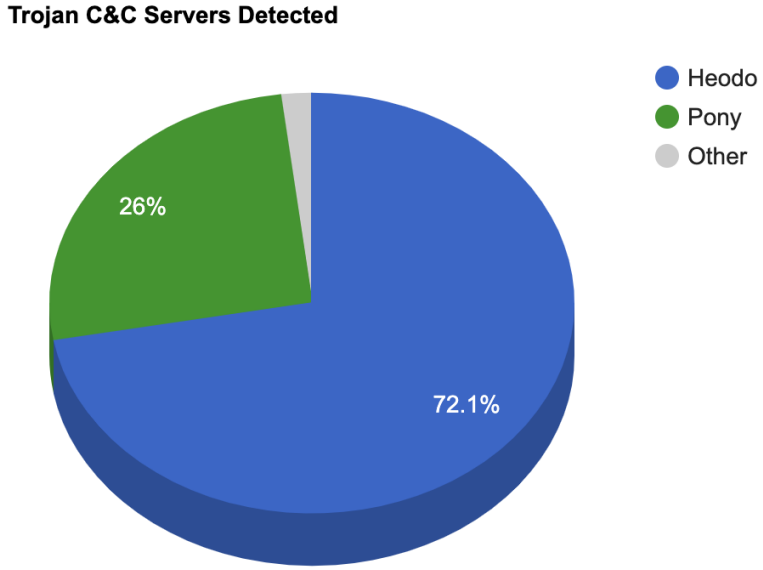
ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
14061	Singapore	DIGITALOCEAN-ASN, US
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
58543	China	CHINATELECOM-GUANGDONG-IDC Guangdong, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	75	100.6.23.40 , 101.187.197.33 , 120.150.247.164 , 120.151.135.224 , 122.176.116.57 , 122.19.63.27 ,

		125.209.114.180, 139.47.135.215, 152.231.89.226, 154.73.137.131, 160.226.171.255, 165.255.142.118, 177.103.159.44, 177.103.240.93, 177.239.160.121, 179.208.84.218, 181.129.96.162, 181.13.24.82, 181.54.246.80, 183.82.123.60, 186.147.245.204, 186.15.52.123, 186.177.165.196, 187.72.47.161, 188.85.143.170, 190.114.244.182, 190.143.39.231, 192.241.143.52, 195.223.215.190, 197.89.27.26, 200.71.200.4, 200.82.88.254, 201.213.100.141, 201.229.45.222, 201.236.135.104, 211.20.154.102, 24.141.12.228, 24.196.49.98, 2.47.112.72, 58.171.38.26, 58.92.179.55, 59.120.5.154, 59.135.126.129, 60.130.173.117, 60.152.212.149, 60.250.78.22, 61.204.119.188, 61.221.152.140, 64.40.250.5, 66.7.242.50, 68.172.243.146, 70.123.95.180, 70.184.69.146, 72.186.137.156, 72.189.57.105, 73.239.11.159,

		76.11.76.47 , 76.185.136.132 , 76.69.26.71 , 78.101.95.172 , 78.142.114.69 , 78.189.180.107 , 78.189.60.109 , 81.16.1.45 , 81.17.92.70 , 82.152.149.79 , 83.35.213.87 , 85.105.241.192 , 86.123.138.76 , 89.211.186.227 , 91.250.96.22 , 95.130.37.244 , 98.192.74.164 , 98.199.196.197 , 98.30.113.161
KPOT	1	45.139.236.16
Pony	1	162.210.96.127
TrickBot	27	104.168.96.113 , 146.185.253.122 , 146.185.253.177 , 162.247.155.133 , 185.105.1.141 , 185.142.99.8 , 185.62.188.34 , 185.99.2.117 , 188.165.62.36 , 195.123.221.53 , 198.23.252.132 , 212.109.220.111 , 5.182.210.226 , 5.182.210.246 , 5.2.78.43 , 5.2.78.98 , 5.2.79.72 , 5.34.176.218 , 5.34.176.242 , 62.109.15.126 , 64.44.133.131 , 82.146.62.52 , 85.143.217.237 , 85.143.220.228 , 85.204.116.233 , 93.189.41.107 , 93.189.46.122



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	01/15/2020

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