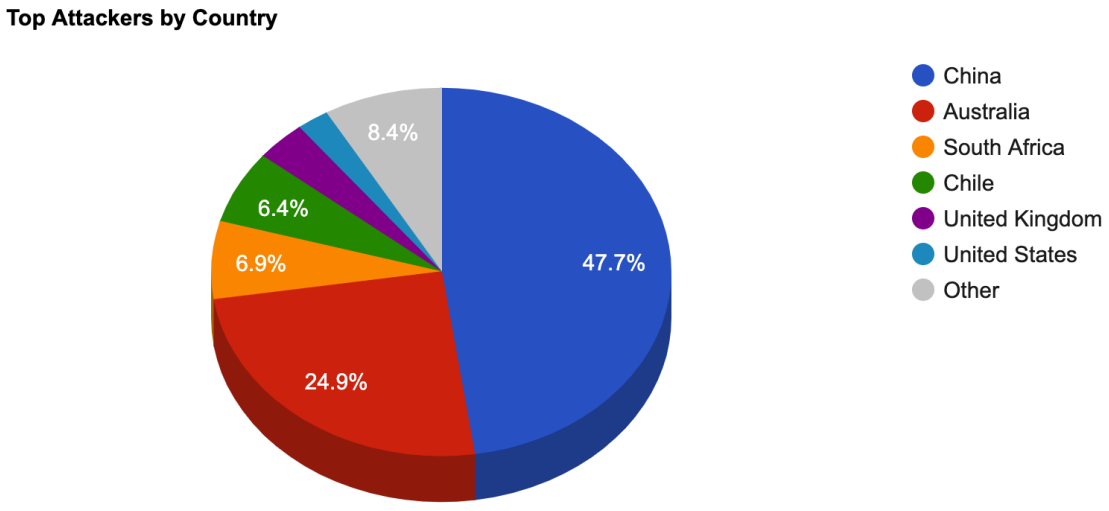
Trends

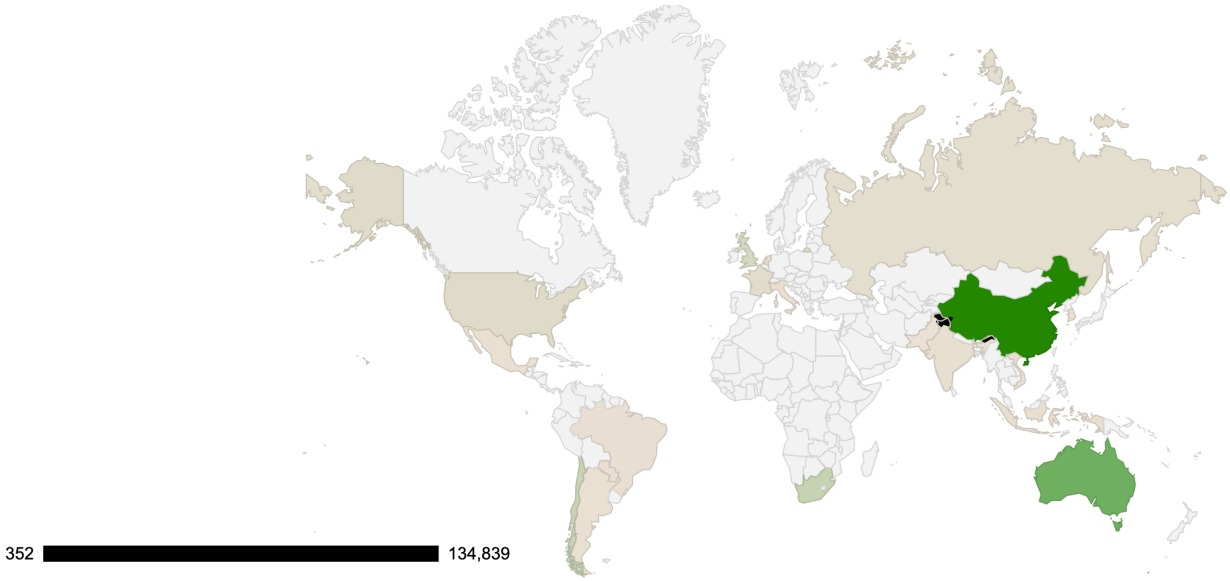
- The top attacker country was China with 134839 unique attackers (46.00%).
- The top Trojan C&C server detected was Heodo with 26 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	134839	46.00%
Australia	70288	24.00%
South Africa	19376	6.00%
Chile	18140	6.00%
United Kingdom	9991	3.00%
United States	6378	2.00%
France	5018	1.00%
Russia	3824	1.00%
India	2160	0%
South Korea	1954	0%
Italy	1667	0%
Netherlands	1643	0%
Indonesia	1509	0%
Paraguay	1332	0%
Brazil	1292	0%
Vietnam	1067	0%
Mexico	1010	0%
Argentina	833	0%
Pakistan	352	0%



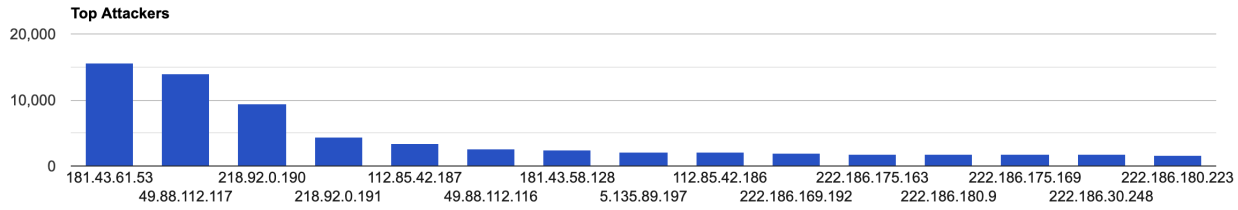
Threat Geo-location



Top Attacking Hosts

Host	Occurrences
181.43.61.53	15651
49.88.112.117	14050
218.92.0.190	9414
218.92.0.191	4363
112.85.42.187	3395
49.88.112.116	2654
181.43.58.128	2406
5.135.89.197	2072
112.85.42.186	2065
222.186.169.192	1967

222.186.175.163	1852
222.186.180.9	1845
222.186.175.169	1819
222.186.30.248	1717
222.186.180.223	1686



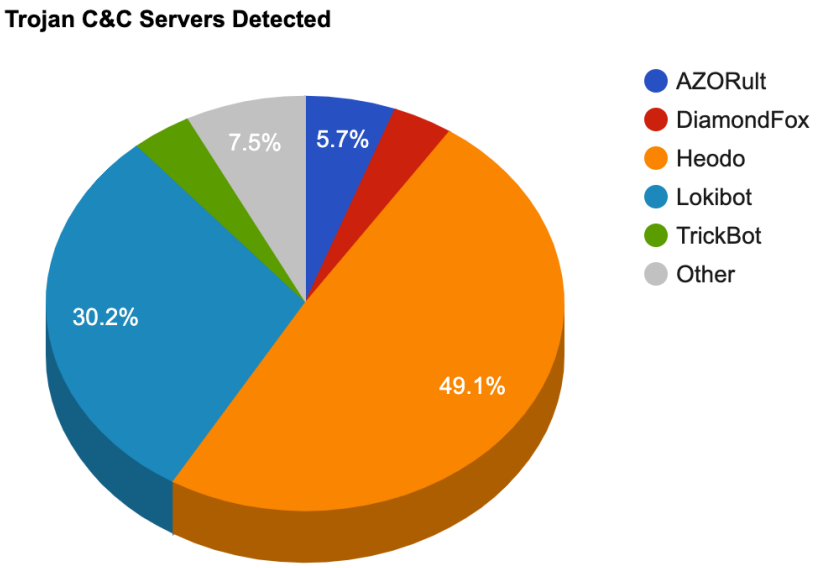
Top Network Attackers

ASN	Country	Name
6471	Chile	ENTEL CHILE S.A., CL
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
16276	Italy	OVH, FR
23650	China	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	3	176.107.160.202 , 188.227.85.53 , 209.127.19.34
DiamondFox	2	195.123.226.145 , 86.106.93.103

Heodo	26	108.6.170.195 , 110.145.101.66 , 110.145.124.178 , 110.37.226.196 , 113.160.88.86 , 118.69.71.14 , 147.83.10.212 , 147.83.10.59 , 177.6.166.4 , 177.72.13.80 , 179.127.59.210 , 182.191.75.93 , 186.250.113.201 , 189.1.185.248 , 190.164.206.121 , 190.188.51.185 , 191.92.120.49 , 200.127.51.94 , 201.82.155.121 , 24.179.13.67 , 47.47.196.171 , 50.91.82.212 , 78.186.174.210 , 86.247.108.13 , 87.127.197.7 , 89.249.222.142
ISRStealer	1	192.185.92.172
KeyBase	1	111.90.142.42
Lokibot	16	103.253.115.205 , 103.74.123.4 , 104.18.38.156 , 104.27.169.180 , 104.28.0.190 , 131.153.22.142 , 131.153.22.219 , 192.185.75.187 , 192.185.75.206 , 194.180.224.126 , 198.23.200.241 , 198.27.81.31 , 209.127.19.34 , 209.127.19.34 , 5.152.210.188 , 89.208.196.16
RansomBuyDecrypt	1	46.29.160.26
TrickBot	2	185.99.2.193 , 5.182.210.4
Zloader	1	217.29.57.164



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
88cbadec77cf90357f46a3629b6737e6	https://www.virustotal.com/gui/file/1460fd00cb6addf9806a341fee9c5ab0a793762d1d97dca05fa17467c8705af7/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.File.2144flashplayer::tpd
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
be52a2a3074a014b163096055df127a0	https://www.virustotal.com/gui/file/97d8ea6cee63296eaf0fa5d97a14898d7cec6fa49fee1bf77c015ca7117a2ba7/details	xme64-553.exe	N/A	Win.Trojan.Coinminer::tpd

799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details	mf2016341595.exe	N/A	W32.Generic:Gen.22fz.1201
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc00555583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f		N/A

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-2020-0665 Microsoft Active Directory Privilege Escalation Vulnerability Microsoft	The vulnerability exists in Active Directory Forest trust due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest. The vulnerability allows a remote user to escalate privileges on the system. A remote user can gain elevated privileges on the target system.	9.0(AV:N/AC:L/Au:S/C:C/I:C/A:C)	02/11/2020	02/13/2020

CVE-2020-0674 Microsoft Scripting Engine Memory Corruption Vulnerability Microsoft	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. An attacker could then install programs view, change, or delete data or create new accounts with full user rights.	7.6(AV:N/AC:H/Au:N/C:C/I:C/A:C)	02/11/2020	02/12/2020

CVE-2020-0759 Microsoft Excel Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. A	6.8(AV:N/AC:M/Au:N/C:P/I:P/A:P)	02/11/2020	02/14/2020
CVE-2020-8808 CORSAIR iCUE Driver Local Privilege Escalation Vulnerability CORSAIR	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE allows local non privileged users to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITYSYSTEM privileges, via a function call such as MmMapIoSpace.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	02/07/2020	02/12/2020

CVE-2019-8449 Atlassian Jira Information Disclosure Vulnerability Atlassian	The /rest/api/latest/groupuserpicker resource in Jira allows remote attackers to enumerate usernames through an information disclosure vulnerability.	5.0(AV:N/AC:L/Au:N/C:P/I:N/A:N)	09/11/2019	02/03/2020
CVE-2019-18634 Sudo pwfeedback Buffer Overflow Vulnerability Multi-Vendor	A potential security issue exists in sudo when the pwfeedback option is enabled in sudoers that can lead to a buffer overflow. If pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.	4.6(AV:L/AC:L/Au:N/C:P/I:P/A:P)	01/29/2020	02/07/2020

CVE-2019-19470 Tinywall Controller Privilege Escalation Vulnerability Tinywall	In Tinywall, unsafe usage of .NET deserialization in Named Pipe message processing allows privilege escalation to NT AUTHORITYSYSTEM for a local attacker. An attacker who has already compromised the local system could use TinyWall Controller to gain additional privileges by attaching a debugger to the running process and modifying the code in memory.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	12/30/2019	01/13/2020