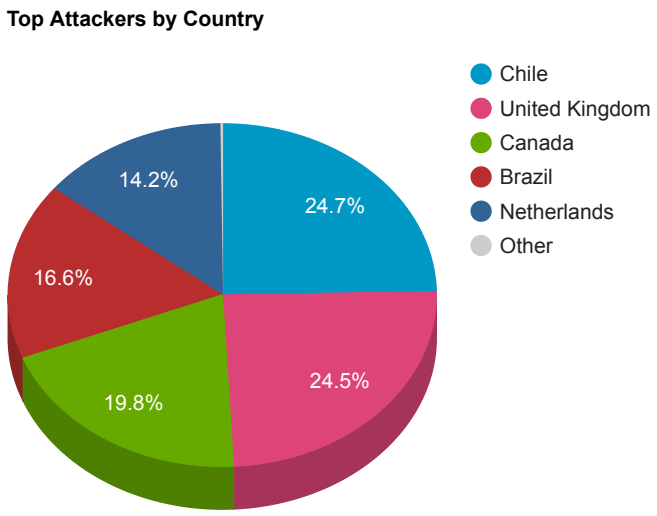
Trends

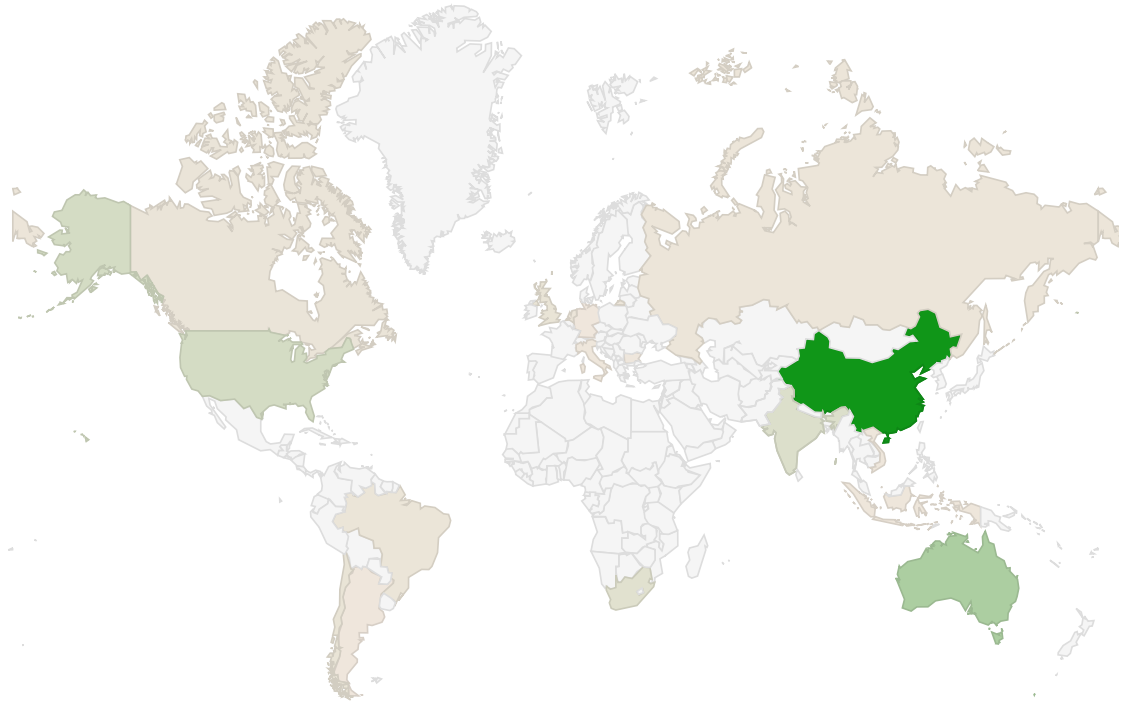
- The top attacker country was China with 228733 unique attackers (53%).
- The top Trojan C&C server detected was Heodo with 45 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	228733	53.00%
Australia	69389	16.00%
United States	28149	6.00%
India	20175	4.00%
South Africa	15457	3.00%
Chile	7438	1.00%
United Kingdom	7384	1.00%
Canada	5970	1.00%
Brazil	5011	1.00%
Netherlands	4274	0%
Russia	3885	0%
Italy	1882	0%
Vietnam	1807	0%
Indonesia	1797	0%
Singapore	1525	0%
Bulgaria	1340	0%
Germany	916	0%
Argentina	853	0%
Gambia	801	0%



Threat Geo-location



801 228,733

Top Attacking Hosts

Host	Occurrences
112.85.42.187	42879

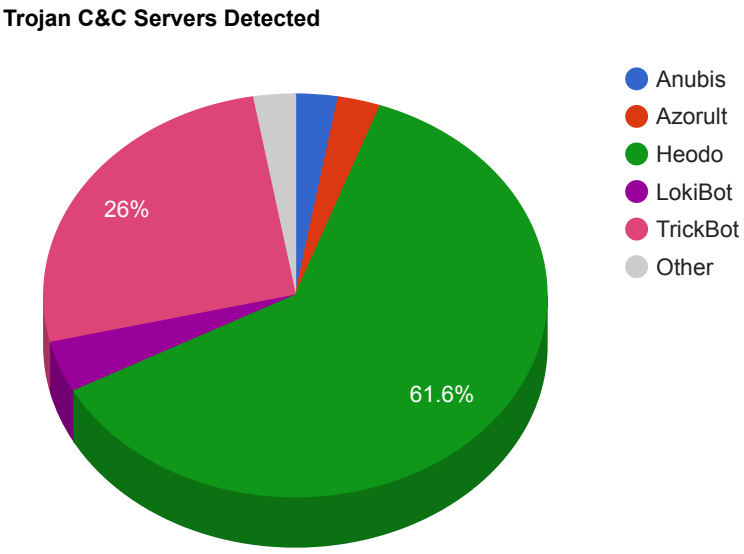
116.118.253.189	34524
49.88.112.116	19311
218.92.0.189	18271
14.200.151.138	16052
202.161.116.141	16036
122.176.116.48	16011
196.250.39.188	14677

Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
23943	Australia	HYPERSPIKE-AS-AU-AP Hyperspike Pty Ltd, AU
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
7545	Australia	TPG-INTERNET-AP TPG Telecom Limited, AU
24560	India	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services, IN
37515	South Africa	iCONNECT, ZA

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	2	91.195.240.117 , 92.63.197.136
Azorult	2	45.143.138.19 , bishu.ac.ug
BetaBot	1	161.117.87.57
Heodo	45	106.248.79.174 , 112.68.254.127 , 113.190.254.245 , 114.109.179.60 , 1.217.126.11 , 1.221.254.82 , 139.130.242.43 , 173.66.96.135 , 178.153.176.124 , 180.33.6.136 , 181.126.70.117 , 181.30.61.163 , 183.87.40.21 , 183.91.3.63 , 186.86.247.171 , 188.0.135.237 , 189.179.108.157 , 189.203.177.41 , 190.151.5.130 , 190.191.82.216 , 190.201.144.85 , 190.55.181.54 , 196.6.119.137 , 198.199.112.197 , 201.137.247.222 , 209.146.22.34 , 221.165.123.72 , 24.164.79.147 , 27.109.153.201 , 37.187.72.193 , 41.215.79.182 , 41.60.200.34 , 45.73.157.243 , 47.180.91.213 , 5.32.55.214 , 58.162.218.151 , 60.231.217.199 , 73.217.39.73 , 78.210.132.35 , 86.108.77.73 , 88.249.120.205 , 88.249.181.198 , 91.205.173.150 , 91.73.169.210 , 98.174.166.205
LokiBot	3	107.175.150.73 , 5.182.211.76 , 91.134.234.202
Raccoon	1	34.65.233.80
TrickBot	19	103.94.122.254 , 146.185.253.107 , 176.31.87.209 , 185.186.77.247 , 185.99.2.149 , 195.123.218.13 , 195.123.218.14 , 195.133.146.185 , 198.8.91.10 , 212.109.223.162 , 23.95.231.187 , 5.2.76.122 , 5.2.77.116 , 78.24.221.145 , 79.174.12.245 , 85.143.219.230 , 92.63.105.138 , 92.63.98.59 , 95.181.198.151



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
5142c721e718206 5b299951a5 4d4fe80	https://www.virustotal.com/gui/file/d73ea76f6f07f96b337335213418b58e3fbc7e4b519fec0ef3fbd19c1d335d81/details	Flash Helper Services .exe	Flash Helper Service	PUA.Win.Adware.Flashserv::1201
121e1634bf18768 80242 7f0a1 3f039a9	https://www.virustotal.com/gui/file/5fc600351bade74c2791fc526bca6bb606355cc65e5253f7f791254db58ee7fa/details	AA_v3 .exe	AmmyyAdmin	W32.SPR:Variant.22fn.1201
c2406fc0fce67ae7 9e625 01332 5e2a68	https://www.virustotal.com/gui/file/1c3ed460a7f78a43bab0ae575056d00c629f35cf7e72443b4e874ede0f305871/details	SegurazoIC .exe	Digital Communications Inc.	PUA.Win.Adware.Ursu::95.sbx.tg
56f11ce911 9632b a360e 5b3dd 0a89acd	https://www.virustotal.com/gui/file/d8b594956ed54836817e38b365dafdc69aa7e07776f83dd0f706278def8ad2d1/details	xme64-540 .exe	N/A	PUA.Win.Tool.Coinminer::100.sbx.tg

e2ea3 15d9a 83e75 77053 f52c9 74f6a 5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	W32.AgentWDCR:Gen.21gn.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-2019-16278 Nostromo Web Server Unauthenticated Remote Code Execution Vulnerability Nazgul	A remote code execution vulnerability exists in Nostromo Web Server. This issue is caused by a directory traversal in the function http_verify in nostromo nhttpd allowing an attacker to achieve remote code execution via a crafted HTTP request. After successful exploitation of this vulnerability an attacker can achieve remote code execution via a crafted HTTP request.	7.5(AV:N/AC:L/Au:N/C:P/I:P/A:P)	10/14/2019	10/31/2019
CVE-2019-5596 FreeBSD Privilege Escalation Vulnerability FreeBSD	In FreeBSD, a bug in the reference count implementation for UNIX domain sockets can cause a file structure to be incorrectly released potentially allowing a malicious local user to gain root privileges or escape from a jail. FreeBSD attempts to handle the case where the receiving process does not provide a sufficiently large buffer for an incoming control message containing rights. The code which performs this operation failed to release a reference obtained on the file corresponding to a received right. This bug can be used to cause the reference counter to wrap around and free the file structure.	7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)	02/12/2019	12/30/2019
CVE-2019-1405 Microsoft UPnP Local Privilege Elevation Vulnerability Microsoft	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play service improperly allows COM object creation. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	11/12/2019	12/18/2019
CVE-2019-19726 OpenBSD Dynamic Loader chpass Privilege Escalation Vulnerability Pulse Secure	Qualys discovered a local privilege escalation in OpenBSD's dynamic loader (ld.so). This vulnerability is exploitable in the default installation (via the set-user-ID executable chpass or passwd) and yields full root privileges. OpenBSD allows local users to escalate to root because a check for LD_LIBRARY_PATH in setuid programs can be defeated by setting a very small RLIMIT_DATA resource limit. When executing chpass or passwd (which are setuid root), _dl_setup_env in ld.so tries to strip LD_LIBRARY_PATH from the environment, but fails when it cannot allocate memory. Thus, the attacker is able to execute their own library code as root.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	12/11/2019	12/27/2019
CVE-2019-1184 Windows Shell COM Server Registrar Local Privilege Escalation Vulnerability Microsoft	An elevation of privilege vulnerability exists when Windows Core Shell COM Server Registrar improperly handles COM calls. An attacker who successfully exploited this vulnerability could potentially set certain items to run at a higher level and thereby elevate permissions.	7.2(AV:L/AC:L/Au:N/C:C/I:C/A:C)	08/14/2019	08/19/2019

CVE-2019-19844 Django count Hijack Vulnerability Django	Django allows account takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. Django's password-reset form uses a case-insensitive query to retrieve accounts matching the email address requesting the password reset.	5.0(AV:N/AC:L/Au:N/C:N/I:P/A:N)	12/18/2019	01/07/2020