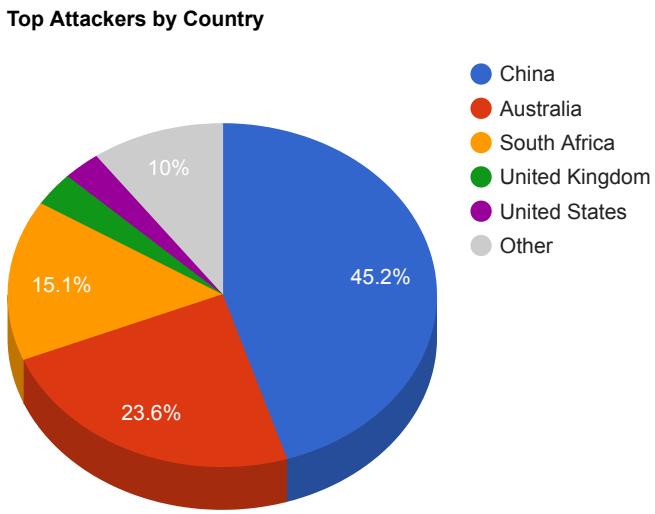
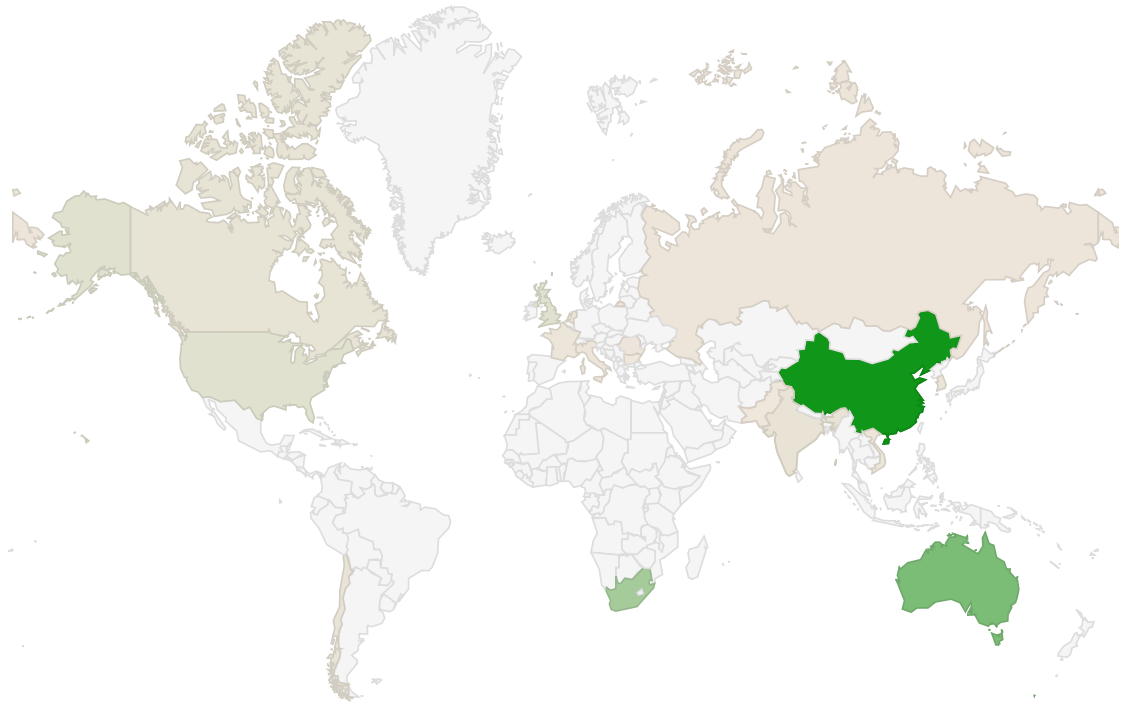
Trends

- The top attacker country was China with 327247 unique attackers (44.00%).
- The top Trojan C&C server detected was TrickBot with 28 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	327247	44.00%
Australia	170979	23.00%
South Africa	109659	14.00%
United Kingdom	23214	3.00%
United States	20621	2.00%
Canada	12308	1.00%
India	11673	1.00%
Chile	9791	1.00%
Netherlands	6908	0%
South Korea	6422	0%
France	5528	0%
Vietnam	5513	0%
Russia	4425	0%
Italy	3530	0%
Romania	3057	0%
Hong Kong	1442	0%
Pakistan	1300	0%
Bulgaria	805	0%



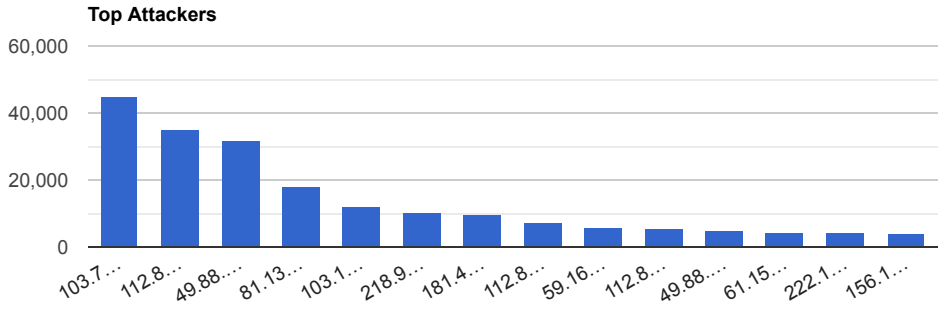


805 327,247

Top Attacking Hosts

Host	Occurrences
103.70.234.5	45119
112.85.42.187	35044
49.88.112.117	31504
81.132.145.37	18054
103.100.29.81	12304
218.92.0.190	10380
181.43.58.47	9573
112.85.42.88	7095

59.167.111.46	5749
112.85.42.188	5598
49.88.112.116	4662
61.157.207.92	4576
222.186.175.154	4364
156.155.162.226	3877



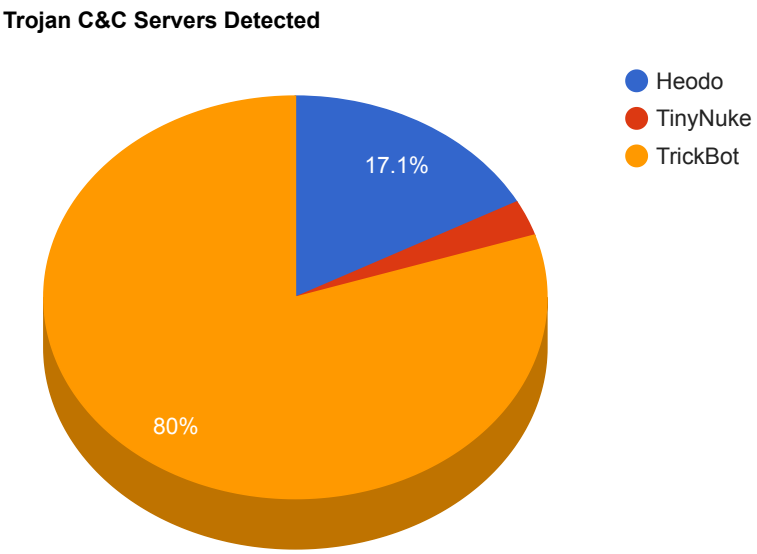
Top Network Attackers

ASN	Country	Name

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	6	152.170.222.65 , 189.154.128.205 , 190.161.45.112 , 190.196.143.58 , 220.213.79.166 , 91.73.197.186
TinyNuke	1	45.141.86.213

TrickBot	28	103.12.161.194 , 107.155.137.19 , 108.170.61.186 , 134.255.221.55 , 148.251.185.164 , 164.132.255.19 , 164.68.120.58 , 172.245.159.116 , 185.14.29.141 , 185.234.72.193 , 185.234.72.50 , 185.99.2.44 , 185.99.2.67 , 188.119.113.60 , 194.5.250.118 , 194.5.250.200 , 194.5.250.201 , 195.123.237.105 , 217.12.209.148 , 217.12.209.159 , 217.12.209.176 , 51.89.115.108 , 85.204.116.193 , 91.200.102.6 , 91.235.129.199 , 92.223.79.48 , 94.250.249.170 , 94.250.250.69



Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name

47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
5d34464531ddbdc7b0a4dba5b4c1cfea	https://www.virustotal.com/gui/file/a545df34334b39522b9cc8cc0c11a1591e016539b209ca1d4ab8626d70a54776/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::in03.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	W32.AgentWDCR:Gen.21gn.1201
799b30f47060ca05d80ece53866e01cc	https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac912661422 66a9910f6f3f85cfd193ec1d6ed8b/details	f2016341595.exe	N/A	W32.Generic:Gen.22fz.1201
8c80dd97c37525927c1e549cb59bcbf3	https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details	Eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos

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-2020-0674 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. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.	CVSSv3BaseScore:7.5(AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)	02/11/2020	02/12/2020

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.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	03/12/2020	03/31/2020
CVE-2020-0041 Google Android Privilege Escalation Vulnerability Android	In binder_transaction of binder.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	03/10/2020	03/11/2020
CVE-2020-10204 Sonatype Nexus Repository Remote Code Execution Vulnerability Sonatype	A Remote Code Execution vulnerability exists in Nexus Repository Manager. The vulnerability allows for an attacker with any type of account on NXRM to execute arbitrary code by crafting a malicious request to NXRM.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	04/01/2020	04/02/2020
CVE-2020-3947 VMWare Workstation vmnetdhcp Denial of Service Vulnerability VMWare	VMware Workstation contain a use-after vulnerability in vmnetdhcp. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial of service condition of the vmnetdhcp service running on the host machine.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	03/16/2020	03/20/2020
CVE-2020-3919 Apple MacOS Privilege Escalation Vulnerability Apple	A memory initialization issue was addressed with improved memory handling. A malicious application may be able to execute arbitrary code with kernel privileges.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	04/01/2020	04/02/2020

CVE-2020-7982 OpenWrt's opkg Man In The Middle Attack Vulnerability OpenWrt	A bug in the fork of the opkg package manager before 2020-01-25 prevents correct parsing of embedded checksums in the signed repository index, allowing a man-in-the-middle attacker to inject arbitrary package payloads (which are installed without verification).	CVSSv3BaseScore:8.1(AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	03/16/2020	03/25/2020
CVE-2020-8515 DrayTek pre-auth Remote Code Execution Vulnerability DrayTek	DrayTek devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	02/01/2020	03/31/2020