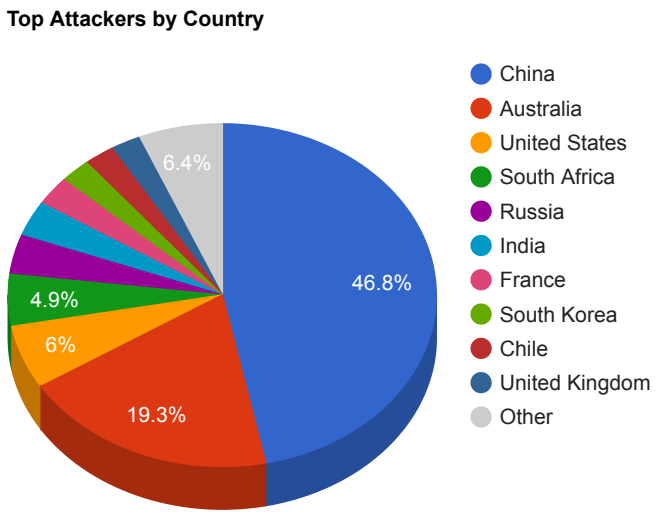
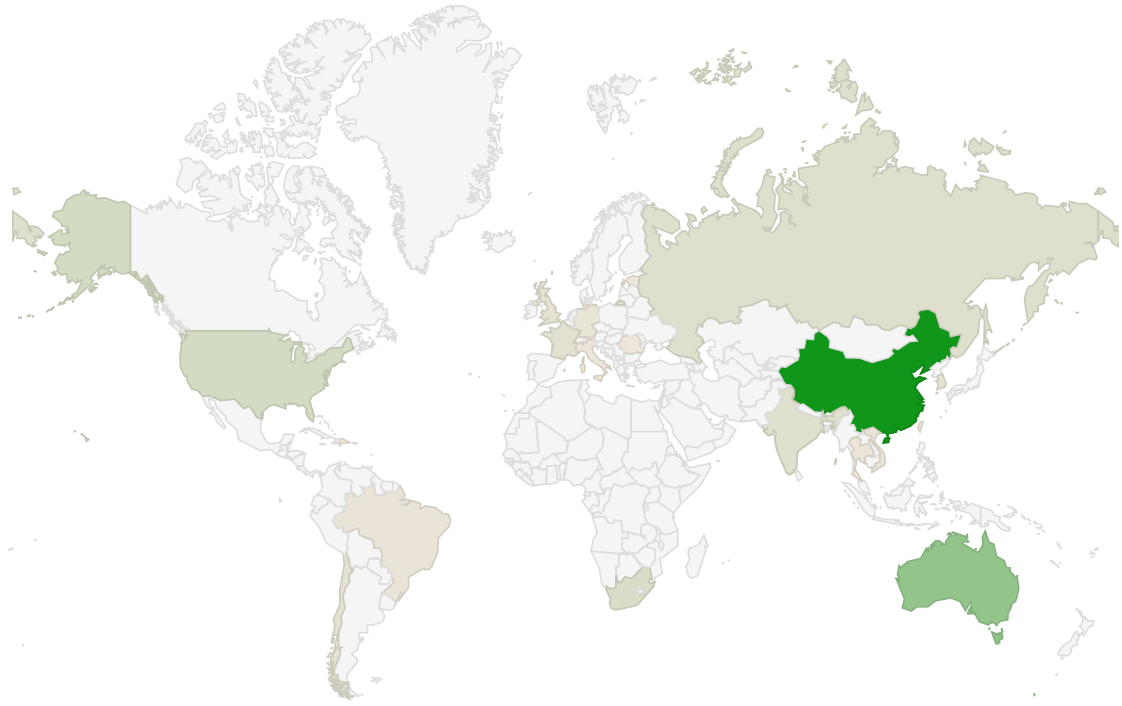
Trends

- The top attacker country was China with 1973468 unique attackers (46.00%).
- The top Trojan C&C server detected was Lokibot with 10 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
China	1973468	46.00%
Australia	814269	19.00%
United States	253479	5.00%
South Africa	205922	4.00%
Russia	157269	3.00%
India	140988	3.00%
France	115213	2.00%
South Korea	98487	2.00%
Chile	96654	2.00%
United Kingdom	94702	2.00%
Germany	64241	1.00%
Brazil	57869	1.00%
Vietnam	42996	1.00%
Thailand	41507	0%
Italy	29084	0%
Romania	13052	0%
Estonia	10131	0%
Taiwan	7876	0%
Dominican Republic	3302	0%



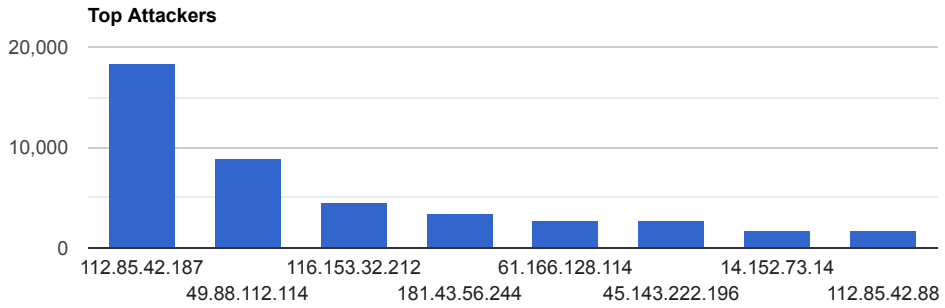


3,302 1,973,468

Top Attacking Hosts

Host	Occurrences
112.85.42.187	18341
49.88.112.114	8885
116.153.32.212	4583
181.43.56.244	3336
61.166.128.114	2829

45.143.222.196	2737
14.152.73.14	1855
112.85.42.88	1847

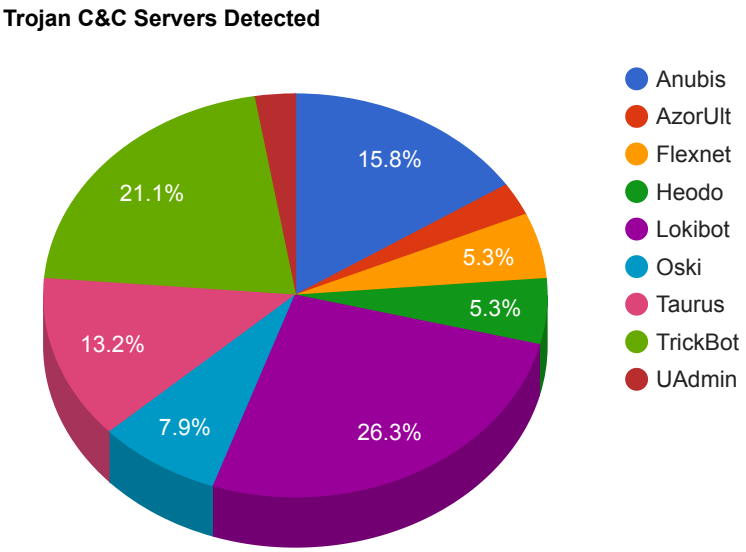


Top Network Attackers

ASN	Country	Name

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	6	34.105.152.77 , 47.241.106.208 , 47.74.186.248 , 8.208.90.79 , 82.148.17.30 , 91.210.104.212
AzorUlt	1	185.90.59.42
Flexnet	2	47.241.116.41 , 8.209.112.8
Heodo	2	181.92.244.156 , 186.226.226.116
LokiBot	10	104.237.252.54 , 104.237.252.91 , 172.67.139.186 , 176.223.209.5 , 185.55.227.103 , 40.87.23.196 , 45.143.138.65 , 5.53.124.78 , 79.124.8.8 , 81.29.134.72
Oski	3	172.67.222.246 , 193.164.150.15 , 194.87.93.125
Taurus	5	104.27.188.245 , 172.67.141.69 , 172.67.158.157 , 202.59.9.104 , toughpalms.top
TrickBot	8	134.119.191.45 , 134.119.191.46 , 162.244.32.199 , 185.14.28.122 , 185.234.52.125 , 192.3.247.122 , 23.92.93.227 , 45.148.120.145
UAdmin	1	80.89.235.67



82749206.pdf	N/A	Pdf.Phishing.Phishing::malicious.tht.talos		
3409ff801cb177f6df26cfec8f4528ae	https://www.virustotal.com/gui/file/dddbfa95401a3f2d9999055b976a0b4ae963e128f7f0d5b043efae29e4306c4a/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.Adware.Flashserv::100.sbx.vioc
b065af93b5fd551526705b5968d0ca10	https://www.virustotal.com/gui/file/28c33a9676f04274b2868c1a2c092503a57d38833f0f8b964d55458623b82b6e/details	vscekgp.exe	NTLMSharedFunctionality	W32.28C33A9676-100.SBX.TG
5d34464531ddbdc7b0a4dba5b4c1cfea	https://www.virustotal.com/gui/file/a545df34334b39522b9cc8cc0c11a1591e016539b2xe09ca1d4ab8626d70a54776/details	FlashHelperServices.exe	FlashHelperServices	PUA.Win.Adware.Flashserv::in03.talos

Top Phishing Campaigns

Phishing TargetCount

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-2020-0096 Google Android Elevation of Privilege Vulnerability Google	Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets. In startActivities of ActivityStartController.java, there is a possible escalation of privilege due to a confused deputy. 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)	05/14/2020	05/18/2020
CVE-2020-9484 Apache Tomcat Remote Code Execution Vulnerability Apache	When using Apache Tomcat versions if a) an attacker is able to control the contents and name of a file on the server and b) the server is configured to use the Persistence Manager with a FileStore	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	05/20/2020	05/28/2020
CVE-2020-1048 Microsoft Windows Print Spooler Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/21/2020	05/26/2020

CVE-2020-3153 Cisco AnyConnect Secure Mobility Client Vulnerability Cisco	A vulnerability in the installer component of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated local attacker to copy user-supplied files to system level directories with system level privileges. The vulnerability is due to the incorrect handling of directory paths. An attacker could exploit this vulnerability by creating a malicious file and copying the file to a system directory. An exploit could allow the attacker to copy malicious files to arbitrary locations with system level privileges.	CVSSv3BaseScore:6.5(AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N)	02/19/2020	04/21/2020
CVE-2020-8617 ISC BIND Denial of Service Vulnerability Multi-Vendor	Using a specially crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly perform other attacks.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	05/19/2020	06/01/2020

CVE-2019-7192 QNAP Pre-Auth Root Remote Code Execution Vulnerability Qnap	QTS (QNAP Turbo NAS System) is a Turbo NAS Operating System, providing file storage, backup, disaster recovery, security management and virtualization applications for businesses multimedia applications. This improper access control vulnerability allows remote attackers to gain unauthorized access to the system.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	12/05/2019	05/28/2020
CVE-2020-12720 vBulletin Remote SQL Injection Vulnerability vBulletin	A remote SQL injection vulnerability exists in vBulletin. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	05/07/2020	06/02/2020
CVE-2020-1048 Microsoft Windows Print Spooler Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/21/2020	05/26/2020