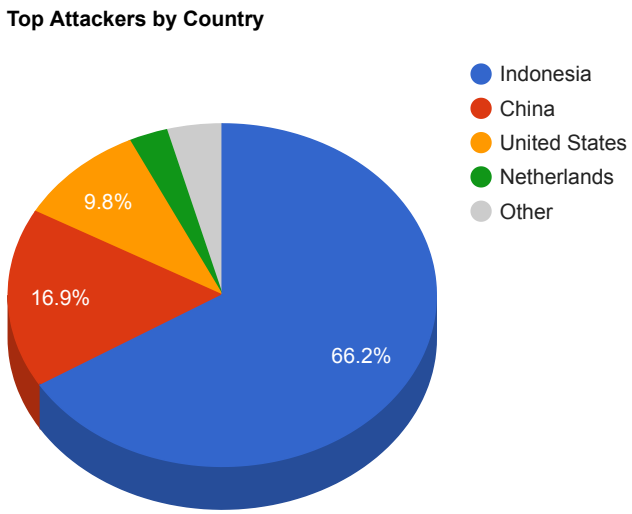
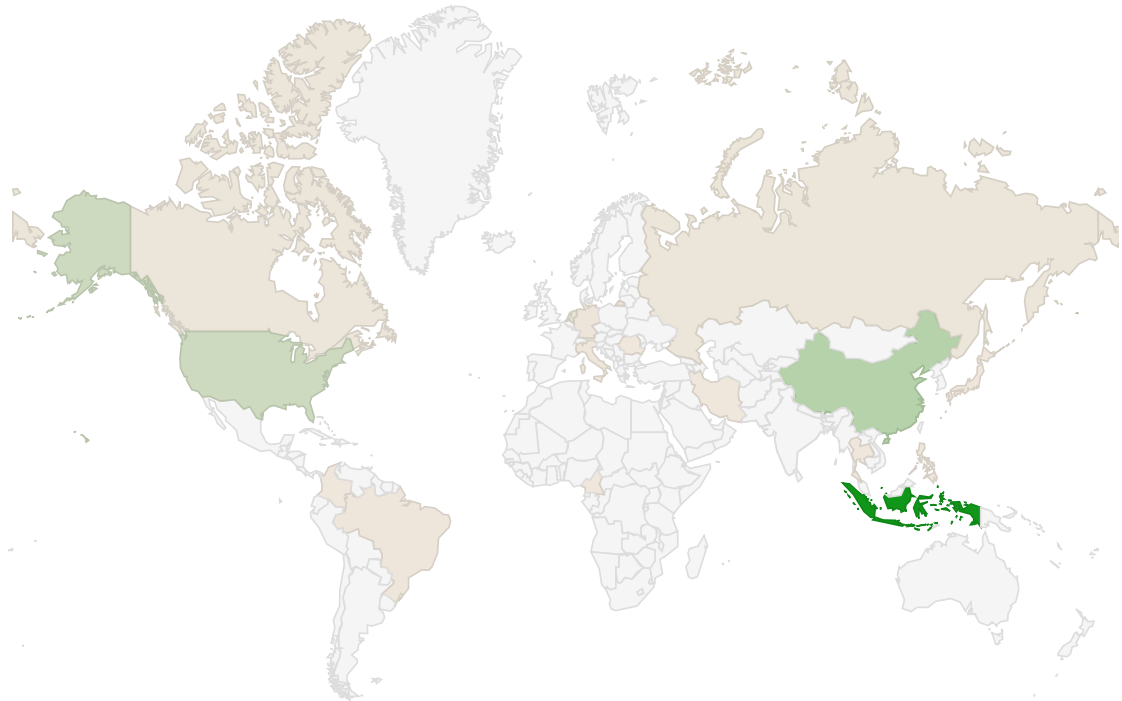
Trends

- The top attacker country was Indonesia with 562538 unique attackers (66.08%).
- The top Trojan C&C server detected was Heodo with 56 instances detected.
- The top phishing campaign detected was against Halifax accounts with 87 instances detected.

Top Attackers By Country

Country	Occurences	Percentage
Indonesia	562538	66.08%
China	144078	16.92%
United States	83037	9.75%
Netherlands	24836	2.91%
Russia	7880	0.92%
Canada	7103	0.83%
Germany	6077	0.83%
Singapore	4239	0.49%
Italy	2808	0.32%
Brazil	2674	0.31%
Colombia	1133	0.13%
Romania	733	0.08%
Thailand	701	0.08%
Europe	671	0.07%
Japan	591	0.06%
Philippines	436	0.05%
Iran	340	0.03%
Cameroon	334	0.03%



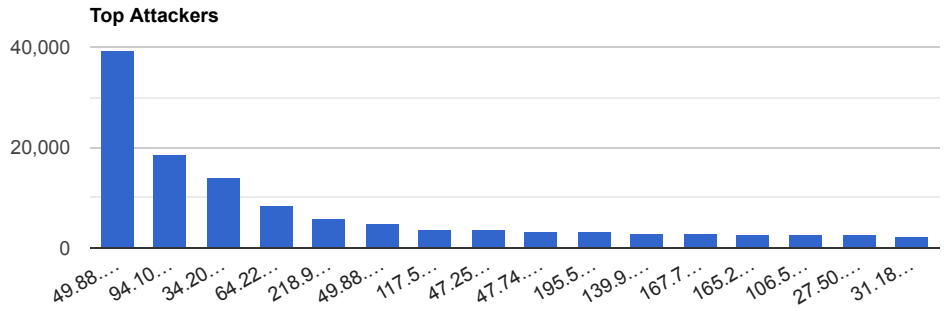


334 562,538

Top Attacking Hosts

Host	Occurrences
49.88.112.68	39498
94.102.51.29	18653
34.200.247.158	13866
64.225.79.21	8410
218.92.0.205	5824
49.88.112.65	4926
117.50.82.156	3566

47.252.8.80	3434
47.74.153.98	3353
195.54.161.122	3248
139.9.5.224	2952
167.71.7.180	2781
165.227.140.36	2746
106.55.150.3	2617
27.50.48.188	2583
31.184.199.114	2439



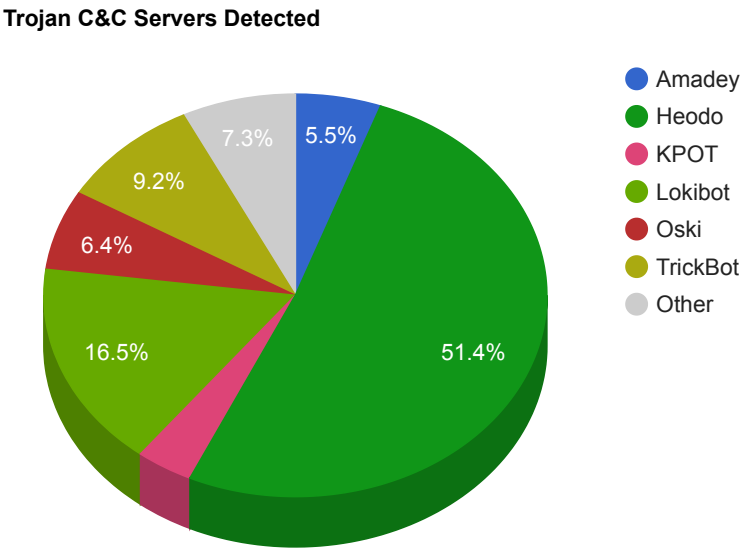
Top Network Attackers

ASN	Country	Name
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
202425	Netherlands	INT-NETWORK, SC
14618	United States	AMAZON-AES, US
14061	United States	DIGITALOCEAN-ASN, US
4808 23724	China	CHINA169-BJ China Unicom Beijing Province Network, CN CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation, CN
45102	United States	CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd., CN
55990	Russia	SELECTEL, RU
55990	China	HWCSNET Huawei Cloud Service data center, CN
45090	China	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
135026	United States	THINKDREAM-AS-AP ThinkDream Technology Limited, HK
34665	Russia	PINDC-AS, RU

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Amadey	6	104.27.174.136 , 176.123.8.254 , 217.8.117.62 , 217.8.117.98 , 95.142.47.69 , gunbot.bid
Azorult	1	198.54.126.17
DT-Stealer	1	185.50.25.23

Heodo	56	102.182.93.220 , 104.131.144.215 , 110.37.224.243 , 115.94.207.99 , 123.142.37.166 , 129.232.220.11 , 172.193.79.237 , 173.212.197.71 , 173.63.222.65 , 176.113.52.6 , 177.107.79.214 , 177.130.51.198 , 180.23.53.200 , 181.123.6.86 , 181.126.74.180 , 181.56.32.36 , 181.59.59.54 , 181.61.182.143 , 182.208.30.18 , 186.189.249.2 , 186.70.56.94 , 188.226.165.170 , 190.101.156.139 , 190.29.166.0 , 194.166.147.143 , 197.245.25.228 , 200.243.153.66 , 201.49.239.200 , 201.71.228.86 , 212.71.250.88 , 24.178.90.49 , 24.230.141.169 , 27.83.209.210 , 2.85.9.41 , 37.179.204.33 , 37.183.81.217 , 49.3.224.99 , 50.245.107.73 , 5.196.108.185 , 5.2.246.108 , 59.125.219.109 , 59.148.253.194 , 60.108.128.186 , 61.76.222.210 , 66.76.12.94 , 76.121.199.225 , 82.76.52.155 , 85.105.111.166 , 85.246.78.192 , 86.123.55.0 , 89.121.205.18 , 91.121.87.90 , 94.230.70.6 , 95.76.142.243 , 95.9.5.93 , 96.126.101.6
Keitaro	1	217.12.201.93
KeyBase	1	185.196.8.138
KPOT	4	172.67.191.2 , 45.141.86.76 , 47.254.28.133 , kpotuvorot10.bit
Lokibot	18	104.223.170.13 , 104.237.252.41 , 104.24.102.29 , 162.244.32.175 , 172.67.204.202 , 178.250.157.171 , 192.185.136.237 , 195.69.140.147 , 204.11.58.39 , 45.252.248.12 , 79.124.8.8 , 91.203.192.84 , 95.213.224.107 , jlk-comercial.com , tvtoc.xyz , vtoct.xyz , www.fitydent.com , xgmb.ga
Oski	7	104.27.188.199 , 198.23.213.114 , 217.8.117.77 , 45.137.152.118 , 45.137.152.201 , 45.8.228.100 , malarcvgs.ac.ug
SmokeLoader	1	217.12.208.12
StormKitty	1	172.67.140.38
Stuffer	1	217.12.209.41
TrickBot	10	103.109.78.174 , 103.127.165.250 , 103.206.128.121 , 199.38.120.89 , 199.38.120.91 , 199.38.121.150 , 199.38.123.58 , 208.86.161.113 , 208.86.162.215 , 208.86.162.241
Zloader	1	47.241.25.81



Scotiabank	1
Vodafone	2
Amazon.com	33
Rakuten	1
VKontakte	2
Apple	1
Instagram	1
PayPal	13
Rabobank	2
Dropbox	1
MyCrypto	1
Halifax	87
Three	2
Blockchain	1
RuneScape	3
Blizzard	1
Revolut	2
DHL	1
Microsoft	3
Google	3
Yahoo	1
Twitter	1
Binance	1
Orange	3
AT&T	1
Netflix	1

CVEs with Recently Discovered Exploits

This is a list of recent vulnerabilities for which exploits are available.

CVE, Title, Vendor	Description	CVSS v3.1 Base Score	Date Created	Date Updated

CVE-2020-16898 Microsoft Windows TCP/IP Stack Remote Code Execution Vulnerability Microsoft	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client. To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	10/16/2020	10/23/2020
CVE-2020-1472 Microsoft Netlogon Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	08/17/2020	10/05/2020

CVE-2020-1034 Microsoft Windows Kernel Elevation of Privilege Vulnerability Microsoft	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	09/11/2020	09/15/2020
CVE-2020-13957 Apache Solr ConfigSet Remote Code Execution Vulnerability Apache	Apache Solr allows some features to be configured in ConfigSet that's uploaded via API without authentication/authorization, which could be used for remote code execution. The checks in place to prevent such features can be circumvented by using a combination of UPLOAD/CREATE actions.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	10/13/2020	10/23/2020
CVE-2019-1151 Microsoft Font Subsetting DLL ReadAllocFormat12CharGlyphMapList Heap Corruption Microsoft	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	08/14/2019	08/24/2020
CVE-2020-14144 Gitea Authenticated Remote Code Execution Vulnerability Gitea	A vulnerability exists in Gitea, that allows an attacker with access to an administrative account or an account with special privileges to execute arbitrary code on the server.	CVSSv3BaseScore:7.2(AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	10/16/2020	10/21/2020

CVE-2020-4280 IBM QRadar RemoteJavaScript Deserialization Vulnerability IBM	A Java deserialization vulnerability exists in the IBM QRadar RemoteJavaScript Servlet. An authenticated user can call one of the vulnerable methods and cause the Servlet to deserialize arbitrary objects. An attacker can exploit this vulnerability by creating a specially crafted (serialized) object, which amongst other things can result in a denial of service, change of system settings, or execution of arbitrary code.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	10/08/2020	10/19/2020