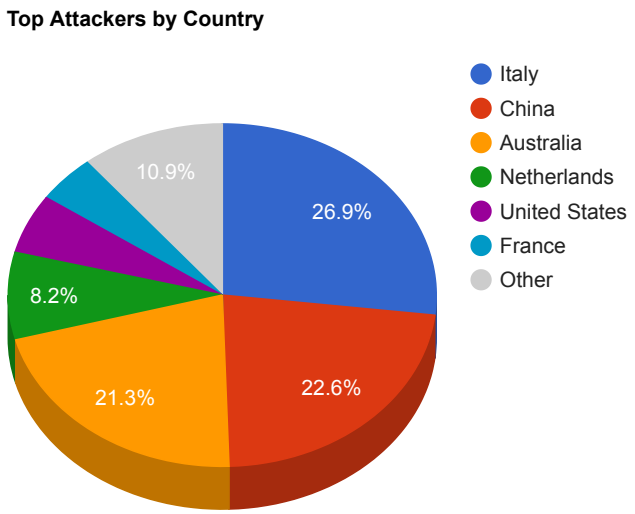
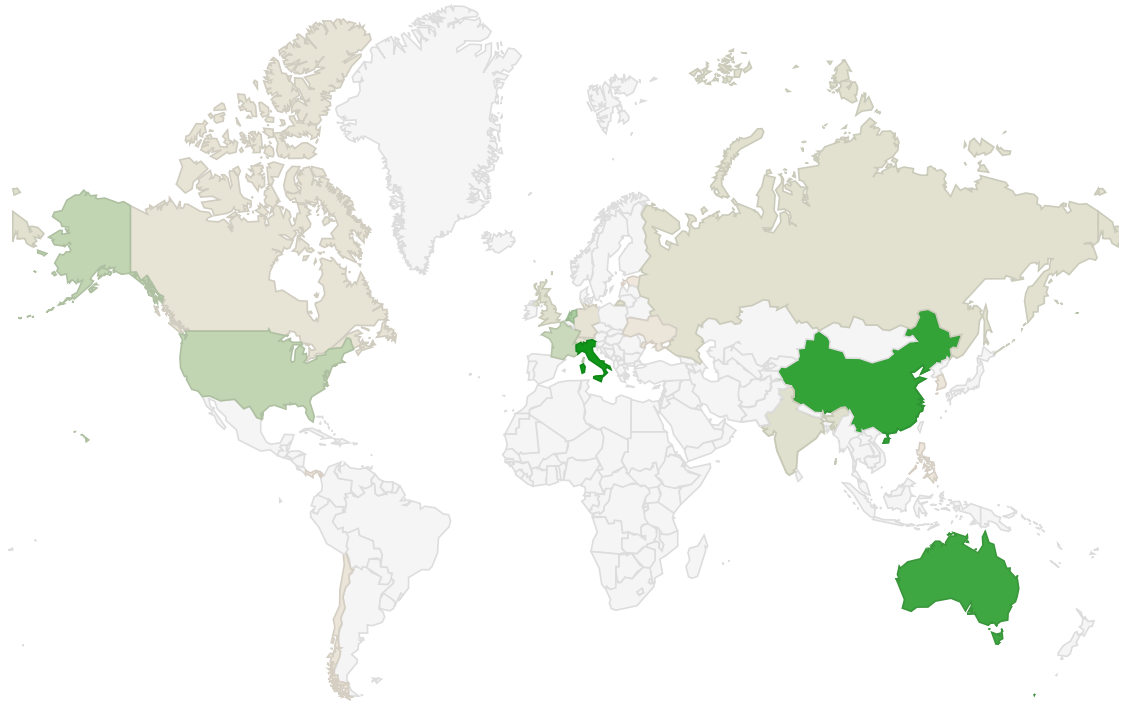

# Trends

- The top attacker country was Italy with 243846 unique attackers (26.00%).
- The top Trojan C&C server detected was Trickbot with 28 instances detected.
- The top phishing campaign detected was against Facebook accounts with 35 instances detected.

## Top Attackers By Country

| Country | Occurences | Percentage |
|---|---|---|
| Italy | 243846 | 26.00% |
| China | 205286 | 22.00% |
| Australia | 193103 | 20.00% |
| Netherlands | 74778 | 8.00% |
| United States | 50902 | 5.00% |
| France | 40737 | 4.00% |
| India | 17346 | 1.00% |
| United Kingdom | 17294 | 1.00% |
| Russia | 15237 | 1.00% |
| Germany | 10656 | 1.00% |
| Switzerland | 9633 | 1.00% |
| Canada | 9399 | 1.00% |
| Chile | 4657 | 0% |
| South Korea | 4209 | 0% |
| Ukraine | 3564 | 0% |
| Hong Kong | 3427 | 0% |
| Philippines | 1987 | 0% |
| Estonia | 753 | 0% |
| Panama | 524 | 0% |



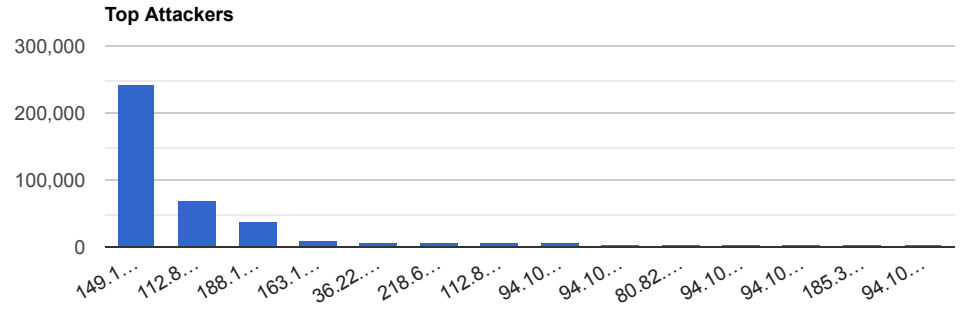



524 243,846

## Top Attacking Hosts

| Host | Occurrences |
|---|---|
| 149.132.54.49 | 243104 |
| 112.85.42.188 | 71809 |
| 188.165.203.93 | 38693 |
| 163.172.101.48 | 10940 |
| 36.22.187.234 | 7953 |
| 218.65.30.24 | 7164 |

| | |
|---|---|
| 112.85.42.102 | 6549 |
| 94.102.51.95 | 6281 |
| 94.102.57.135 | 3608 |
| 80.82.64.98 | 3600 |
| 94.102.57.179 | 3563 |
| 94.102.57.153 | 3561 |
| 185.39.10.89 | 3547 |
| 94.102.57.172 | 3540 |



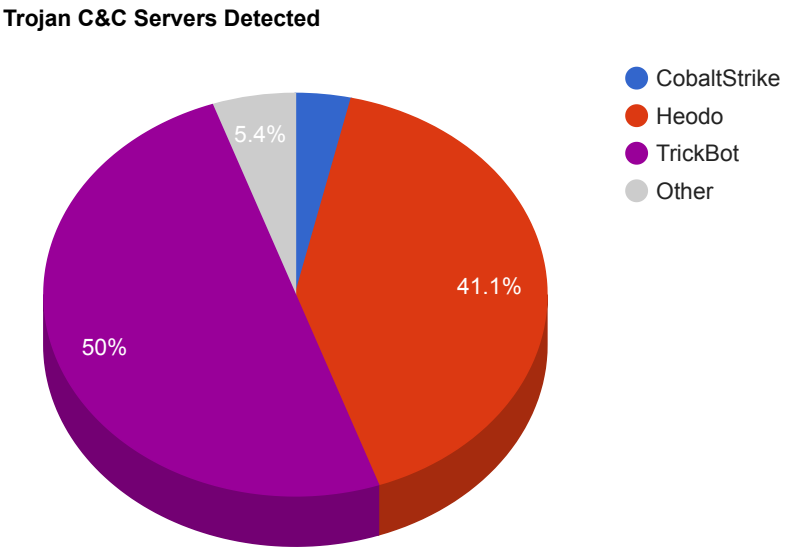

## Top Network Attackers

| ASN | Country | Name |
|---|---|---|
| 137 | Italy | ASGARR Consortium GARR, EU |
| 4837 | China | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN |
| 16276 | France | OVH, FR |
| 12876 | France | Online SAS, FR |
| 4134 | China | CHINANET-BACKBONE No.31,Jin-rong Street, CN |
| 202425 | Netherlands | INT-NETWORK, SC |
| 62355 | Switzerland | NETWORKDEDICATED, CH |

## Remote Access Trojan C&C Servers Found

| Name | Number Discovered | Location |
|---|---|---|
| CobaltStrike | 2 | 45.141.84.218 , 45.141.84.234 |
| Heodo | 23 | 104.131.123.136 , 104.193.103.61 , 105.186.233.33 , 109.169.12.78 , 128.92.203.42 , 130.0.132.242 , 181.74.0.251 , 187.49.206.134 , 189.35.44.221 , 190.188.245.242 , 202.22.141.45 , 202.29.239.162 , 203.205.28.68 , 37.187.161.206 , 38.18.235.242 , 5.196.108.189 , 70.169.17.134 , 71.15.245.148 , 76.175.162.101 , 78.188.106.53 , 80.241.255.202 , 80.87.201.221 , 91.146.156.228 |
| Oski | 1 | 45.141.84.143 |
| SmokeLoader | 1 | 45.141.84.247 |

| | | |
|---|---|---|
| TrickBot | 28 | 104.161.32.10 , 185.105.1.149 , 185.164.32.108 , 185.234.72.147 , 185.99.2.180 , 194.156.98.172 , 194.5.249.107 , 194.5.249.156 , 194.5.249.31 , 195.123.239.59 , 195.123.241.157 , 195.123.241.182 , 195.2.93.227 , 212.80.219.98 , 45.141.103.194 , 45.155.173.196 , 45.8.230.108 , 45.89.127.27 , 51.89.177.18 , 62.108.35.179 , 62.108.35.204 , 85.143.219.36 , 88.150.197.186 , 91.200.101.192 , 91.210.171.82 , 93.189.40.214 , 94.250.254.84 , 94.250.255.217 |
| UAdmin | 1 | 45.141.84.163 |




## Common Malware

| MD5 | VirusTotal | FileName | Claimed Product | Detection Name |
|---|---|---|---|---|
| 8c80dd97c37525927c1e549cb59bcbf3 | https://www.virustotal.com/gui/file/85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5/details | Eter.exe | N/A | Win.Exploit.Shadowbrokers::5A5226262.auto.talos |
| 29f47c2f15d6421bdd813be27a2e3b25 | https://www.virustotal.com/gui/file/be29d4902d72abbc293376b42005d954807b3e6794b13fe628faff9bc94f6063/details | FlashHelperServices.exe | N/A | FlashHelperService |

| | | | | |
|---|---|---|---|---|
| 01a607b4d69c549629e6f0dfd3983956 | https://www.virustotal.com/gui/file/1eef72aa566ba6c76b33f9d430d7233e358392382bfb3db81ca4f28d74f415a5/details | wupxarch.exe | N/A | W32.Auto:1eef72aa56.in03.Talos |
| e2ea315d9a83e7577053f52c974f6a5a | https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details | Tempmf582901854.exe | N/A | Win.Dropper.Agentwdcr::1201 |
| 799b30f47060ca05d80ece53866e01cc | https://www.virustotal.com/gui/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details | mf2016341595.exe | N/A | Win.Downloader.Generic::1201 |

## Top Phishing Campaigns

| **Phishing Target** | **Count** |
|---|---|
| Other | 1391 |
| Citibank | 1 |
| Vodafone | 3 |
| Facebook | 35 |
| Microsoft | 8 |
| Halifax | 23 |
| PayPal | 8 |
| Amazon.com | 28 |
| Special | 3 |
| Caixa | 4 |
| Instagram | 1 |
| VKontakte | 1 |
| RuneScape | 2 |
| AOL | 1 |
| Netflix | 1 |
| DHL | 2 |
| Orange | 2 |
| Virustotal | 17 |

## 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-2020-1472<br>Microsoft Netlogon Elevation of Privilege Vulnerability<br>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 | 10/03/2020 |
| CVE-2020-1895<br>Instagram App Heap Buffer Overflow Vulnerability<br>Facebook | A large heap overflow could occur in Instagram for Android when attempting to upload an image with specially crafted dimensions. | CVSSv3BaseScore:7.8(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) | 04/09/2020 | 04/10/2020 |
| CVE-2020-0688<br>Microsoft Exchange Validation Key Remote Code Execution Vulnerability<br>Microsoft | A remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time. Knowledge of a the validation key allows an authenticated user with a mailbox to pass arbitrary objects to be deserialized by the web application, which runs as SYSTEM. | CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | 02/11/2020 | 02/20/2020 |

| | | | | |
|---|---|---|---|---|
| CVE-2020-1350<br>Microsoft Windows DNS Server Remote Code Execution Vulnerability<br>Microsoft | A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the Local System Account. Windows servers that are configured as DNS servers are at risk from this vulnerability. | CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H) | 07/14/2020 | 07/23/2020 |
| CVE-2020-4486<br>IBM QRadar Arbitrary File Overwrite Vulnerability<br>IBM | IBM QRadar allows an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation. | CVSSv3BaseScore:8.1(AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H) | 08/11/2020 | 08/11/2020 |
| CVE-2020-8437<br>BitTorrent uTorrent Denial of Service Vulnerability<br>bittorrent | The bencoding parser in BitTorrent uTorrent misparses nested bencoded dictionaries, which allows a remote attacker to cause a denial of service. | CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) | 03/02/2020 | 09/30/2020 |
| CVE-2020-6506<br>Google Chrome on Android Insufficient Bounds Check Vulnerability<br>Google | Insufficient policy enforcement in WebView in Google Chrome on Android allows a remote attacker to bypass site isolation via a crafted HTML page. An Android WebView instance with default configuration and JavaScript enabled allows an iframe on a different origin to bypass same-origin policies and execute arbitrary JavaScript in the top document. | CVSSv3BaseScore:6.5(AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N) | 07/22/2020 | 10/01/2020 |