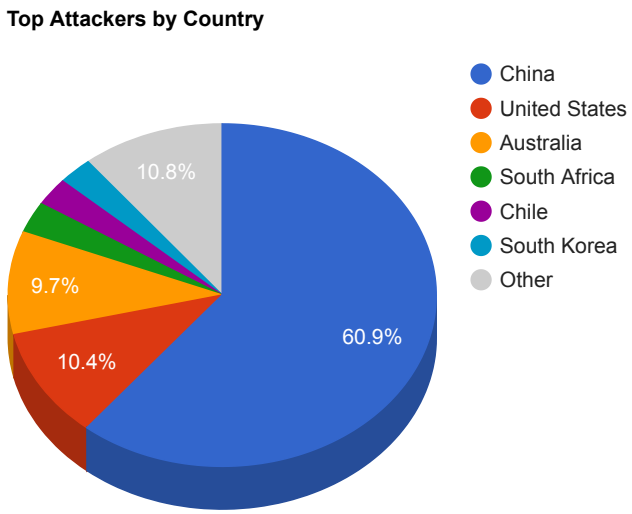
Trends

- The top attacker country was China with 398353 unique attackers (58.00%).
- The top Trojan C&C servers detected were TrickBot and Heodo with 18 instances detected each.

Top Attackers By Country

Country	Occurences	Percentage
China	398353	58.00%
United States	67944	9.00%
Australia	63586	9.00%
South Africa	19271	2.00%
Chile	17312	2.00%
South Korea	17094	2.00%
India	12718	1.00%
France	10223	1.00%
United Kingdom	8669	1.00%
Canada	8156	1.00%
Brazil	7892	1.00%
Indonesia	7221	1.00%
Russia	5219	0%
Netherlands	3903	0%
Iran	2159	0%
Venezuela	1397	0%
Ukraine	1369	0%
Hong Kong	892	0%
Nepal	788	0%

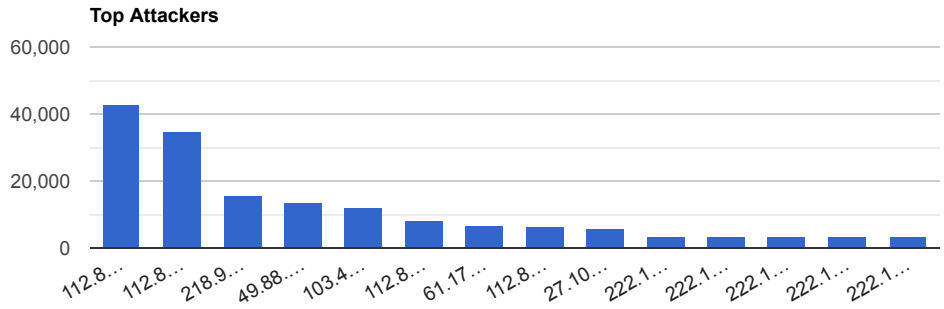


788 398,353

Top Attacking Hosts

Host	Occurrences
112.85.42.187	42799
112.85.42.88	34612
218.92.0.190	15755
49.88.112.115	13619
103.44.253.24	12103

112.85.42.189	8478
61.177.172.13	7021
112.85.42.238	6170
27.106.60.179	5842
222.186.175.148	3637
222.186.169.192	3470
222.186.173.226	3430
222.186.173.238	3400
222.186.173.154	3310

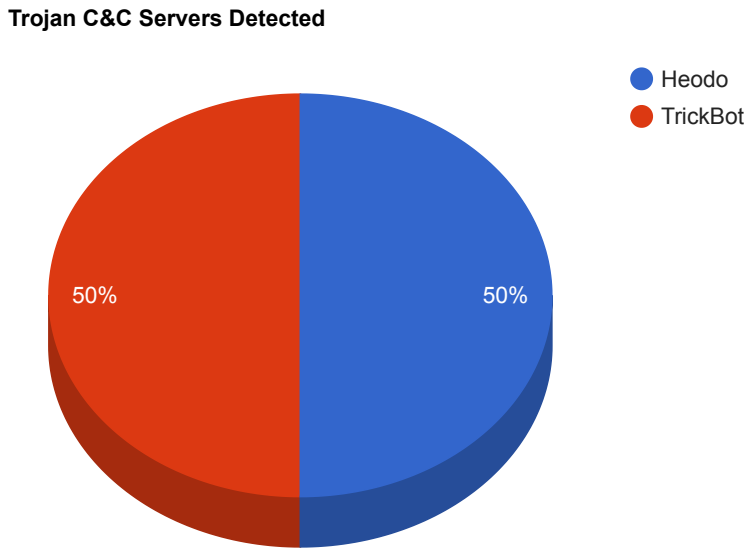


Top Network Attackers

ASN	Country	Name
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
4816	China	CHINANET-IDC-GD China Telecom (Group), CN
45194	India	SIPL-AS Syscon Infoway Pvt. Ltd., IN
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN

Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	18	108.26.231.214 , 124.45.106.173 , 153.204.32.49 , 157.7.199.53 , 187.106.41.99 , 187.207.207.16 , 190.163.31.26 , 190.164.75.175 , 190.96.118.251 , 201.170.77.7 , 212.156.133.218 , 212.231.60.98 , 70.167.215.250 , 71.208.216.10 , 71.50.31.38 , 74.207.230.187 , 78.189.111.208 , 95.9.185.228
TrickBot	18	107.174.26.187 , 162.216.0.187 , 162.216.0.190 , 185.14.31.135 , 185.164.32.204 , 185.172.165.211 , 188.40.203.209 , 188.40.203.215 , 194.5.249.15 , 195.123.221.121 , 195.123.239.53 , 217.12.209.44 , 46.17.107.116 , 78.108.216.13 , 80.82.68.132 , 80.82.68.32 , 93.189.41.213 , 93.189.42.114



MD5	VirusTotal	FileName	Claimed Product	Detection Name
34560233e751b7e95f155b6f61e7419a	https://www.virustotal.com/gui/file/8b4216a7c50599b11241876ada8ae6f07b48f1abe6590c2440004ea4db5becc9/details	SAService.exe	SAService	PUA.Win.Dropper.Seguraz o::tpd
179c09b866c9063254083216b55693e6	https://www.virustotal.com/gui/file/449f4a4524c06e798193c1d3ba21c2d9338936375227277898c583780392d4d8/details	SAService.exe	SAService	PUA.Win.File.Seguraz o::95.sbx.tg
a10a6d9dfc0328a391a3fdb1a9fb18db	https://www.virustotal.com/gui/file/094d4da0ae3ded8b936428bb7393c77aaedd5efb5957116afd4263bd7edc2188/details	FlashHelperServices.exe	FlashHelperService	PUA.Win.Adware.Flashserv::100.sbx.vioc
8193b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Seguraz o::95.sbx.tg
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201

Top Phishing Campaigns

Phishing Target	Count

Other	1502
Facebook	177
Three	17
Blockchain	1
RuneScape	50
Apple	2
Microsoft	14
PayPal	4
DHL	3
TSB	1
Westpac	1
Twitter	1
Amazon.com	4
Caixa	2
Virustotal	1
Dropbox	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-2020-8605 Trend Micro Web Security Virtual Appliance Remote Code Execution Vulnerability Trend Micro	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance may allow remote attackers to execute arbitrary code on affected installations. An attacker can leverage this vulnerability to disclose information in the context of the IWSS user. An authenticated remote attacker could exploit a command injection vulnerability in the product, leading to remote code execution vulnerability.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	05/27/2020	07/14/2020

CVE-2020-1350 Microsoft Windows DNS Server Remote Code Execution Vulnerability 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-2020-5902 F5 BIG-IP Remote Code Execution Vulnerability F5	F5 BIG-IP is exposed to remote code execution vulnerability. The vulnerability that has been actively exploited in the wild allows attackers to read files, execute code or take complete control over vulnerable systems having network access.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/01/2020	07/21/2020
CVE-2020-6287 SAP NetWeaver Application Server JAVA Multiple Vulnerabilities SAP	SAP NetWeaver AS JAVA (LM Configuration Wizard) does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	07/14/2020	07/16/2020

CVE-2020-15363 WordPress Theme NexosReal Estate 'search_order' SQL Injection Vulnerability Nexos	NexosReal Estate Theme is exposed to remote SQL injection vulnerability that allows side-map/?search_order= SQL Injection.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	06/28/2020	07/22/2020
CVE-2020-13866 WinGate Privilege Escalation Vulnerability qbik	WinGate has insecure permissions for the installation directory, which allows local users to gain privileges by replacing an executable file with a Trojan horse. The WinGate directory hands full control to authenticated users, who can then run arbitrary code as SYSTEM after a WinGate restart or system reboot.	CVSSv3BaseScore:7.8(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	06/08/2020	06/11/2020
CVE-2020-2021 Palo Alto Networks PAN-OS Authentication Bypass in SAML Authentication Vulnerability Palo Alto Networks	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability.	CVSSv3BaseScore:10.0(AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)	06/29/2020	07/06/2020

CVE-2020-3952 VMware vCenter vmdir Information Disclosure Vulnerability VMware	Under certain conditions vmdir does not correctly implement access controls. A malicious actor with network access to an affected vmdir deployment may be able to extract highly sensitive information which could be used to compromise vCenter Server or other services which are dependent upon vmdir for authentication.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	04/10/2020	06/02/2020