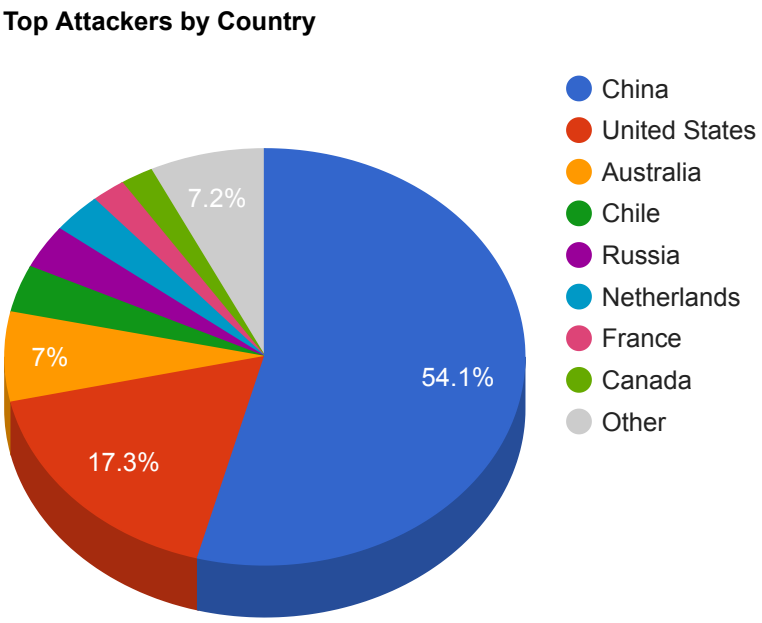
Trends

- The top attacker country was China with 311117 unique attackers (52.00%).
- The top Malware detected was W32.Auto.

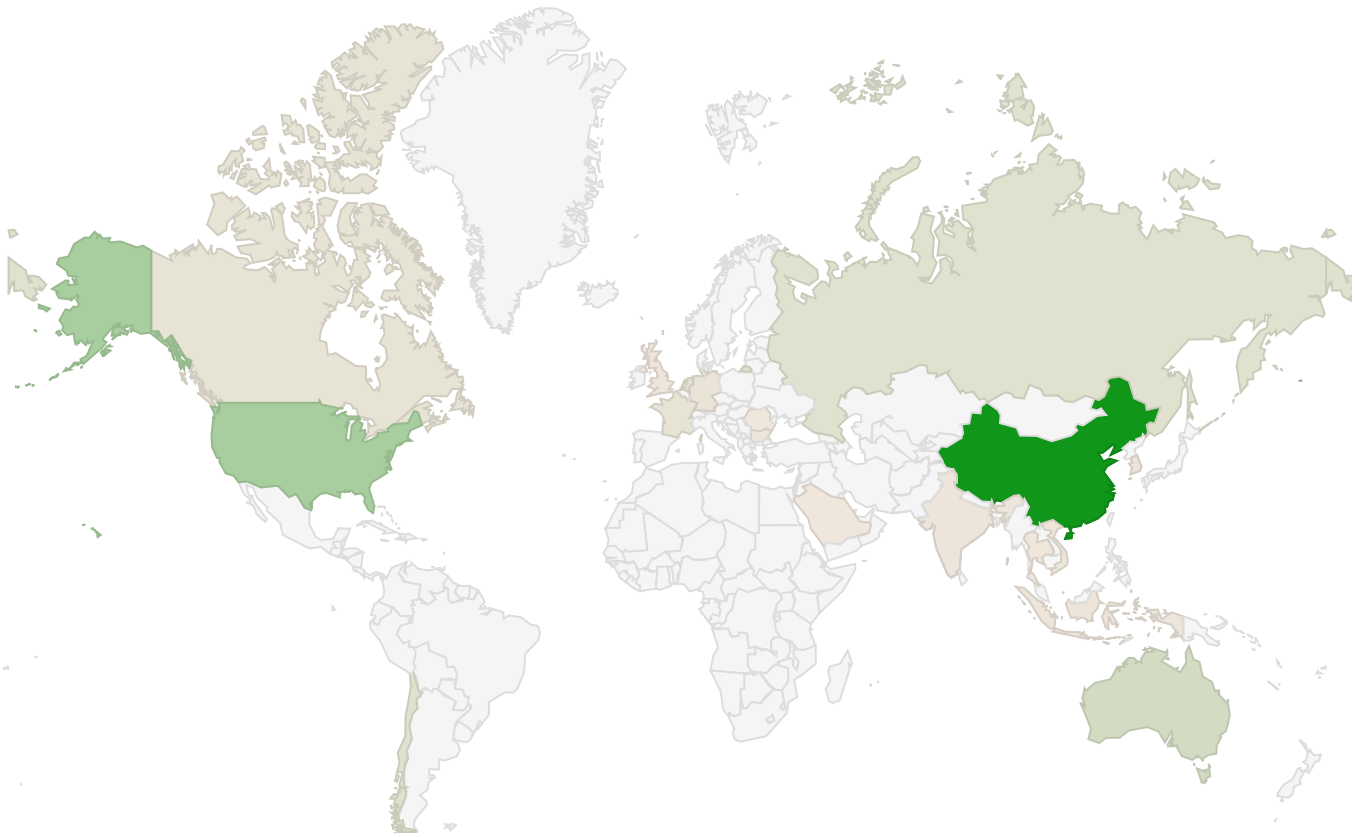
Top Attackers By Country

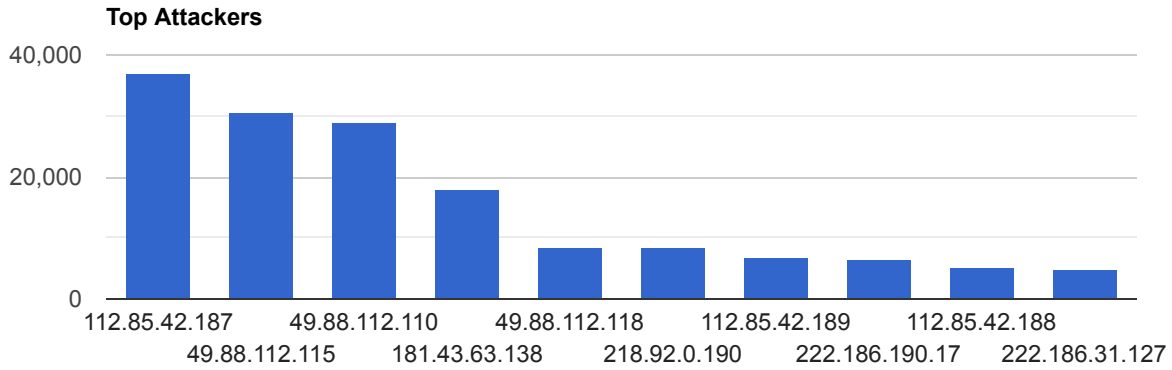
Country	Occurences	Percentage
China	311117	52.00%
United States	99621	16.00%
Australia	39981	6.00%
Chile	21091	3.00%
Russia	19591	3.00%
Netherlands	17854	3.00%
France	12182	2.00%
Canada	11691	1.00%
Germany	8804	1.00%
South Korea	8569	1.00%
Hong Kong	4998	0%
Indonesia	3271	0%
Bulgaria	3132	0%
India	3003	0%
United Kingdom	2674	0%
Singapore	2374	0%
Vietnam	2296	0%
Romania	955	0%

Thailand	723	0%
Saudi Arabia	679	0%



Threat Geo-location





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
6471	Chile	ENTEL CHILE S.A., CL
23650	China	CHINANET-JIANGSU-PROVINCE-IDC AS Number for CHINANET jiangsu province backbone, CN

Common Malware

MD5	VirusTotal	FileName	Claimed Product	Detection Name
f0fdc17674950a4eaa4bbaafce5007f6	https://www.virustotal.com/gui/file/e66d6d13096ec9a62f5c5489d73c0d1dd113ea4668502021075303495fd9ff82/details	FlashHelperServices.exe	FlashHelperService	W32.Auto:e66d6d1309.in03.Talos
34560233e751b7e95f155b6f61e7419a	https://www.virustotal.com/gui/file/8b4216a7c50599b11241876ada8ae6f07b48f1abe6590c2440004ea4db5becc9/details	SAService.exe	SAService	PUA.Win.Dropper.Segurazo::tpd
81936b63313019b614d5be721c538486b	https://www.virustotal.com/gui/file/e3eeaee0af4b549eae4447fa20cfe205e8d56beecf43cf14a11bf3e86ae6e8bd/details	SAntivirusService.exe	SAService	PUA.Win.Dropper.Segurazo::95.sbx.tg
47b97de62ae8b2b927542aa5d7f3c858	https://www.virustotal.com/gui/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
e2ea315d9a83e7577053f52c974f6a5a	https://www.virustotal.com/gui/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	Win.Dropper.Agentwdcr::1201

Top Phishing Campaigns

Phishing Target	Count

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-2020-3187 Cisco ASA Software and FTD Software Web Services Path Traversal Vulnerability Cisco	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences.	CVSSv3BaseScore:9.1(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)	05/06/2020	07/29/2020

CVE-2020-3452 Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability Cisco	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device.	CVSSv3BaseScore:7.5(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	07/22/2020	07/29/2020

CVE-2020-8163 Ruby On Rails Remote Code Execution Vulnerability Ruby On Rails	The is a code injection vulnerability that would allow an attacker who controlled the "locals" argument of a "render" call to perform a remote code execution vulnerability.	CVSSv3BaseScore:8.8(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	07/02/2020	07/27/2020
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	07/27/2020

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-2020-3140 Cisco Prime License Manager Privilege Escalation Vulnerability Cisco	A vulnerability in the web management interface of Cisco Prime License Manager (PLM) Software could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. The vulnerability is due to insufficient validation of user input on the web management interface. An attacker could exploit this vulnerability by submitting a malicious request to an affected system. An exploit could allow the attacker to gain administrative-level privileges on the system.	CVSSv3BaseScore:9.8(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	07/16/2020	07/23/2020

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