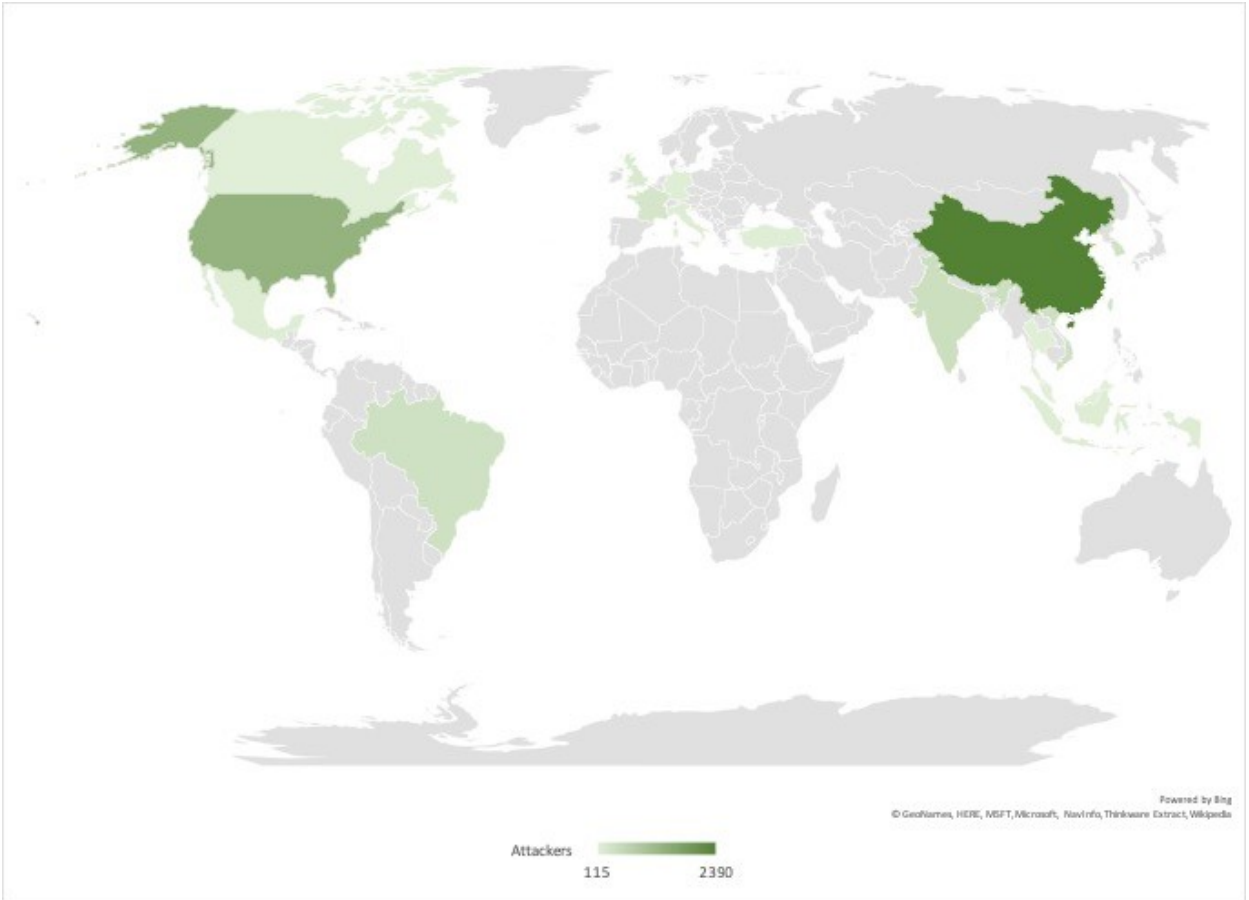
TRENDS

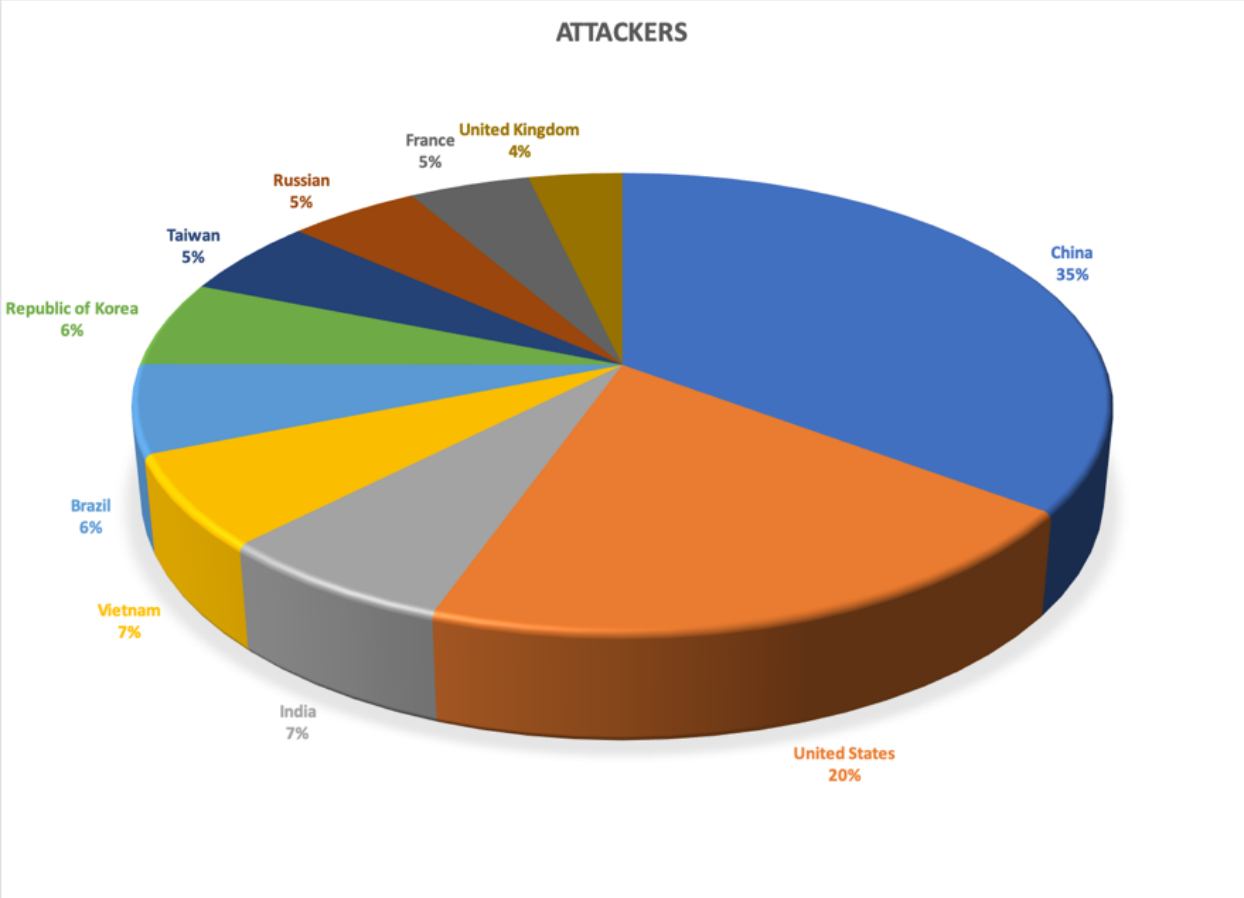
- The top attacker country was China with 2390 unique attackers (27.90%).
- The top Exploit event was Miscellaneous with 63% of occurrences.
- The top Trojan C&C server detected was Formbook with 8428 instances detected.

TOP ATTACKER COUNTRIES

COUNTRY	OCCURRENCES	PERCENTAGE%
China	2390	27.90%
United States	1370	16%
India	470	5.50%
Vietnam	441	5.20%
Brazil	422	4.90%
Republic of Korea	409	4.80%

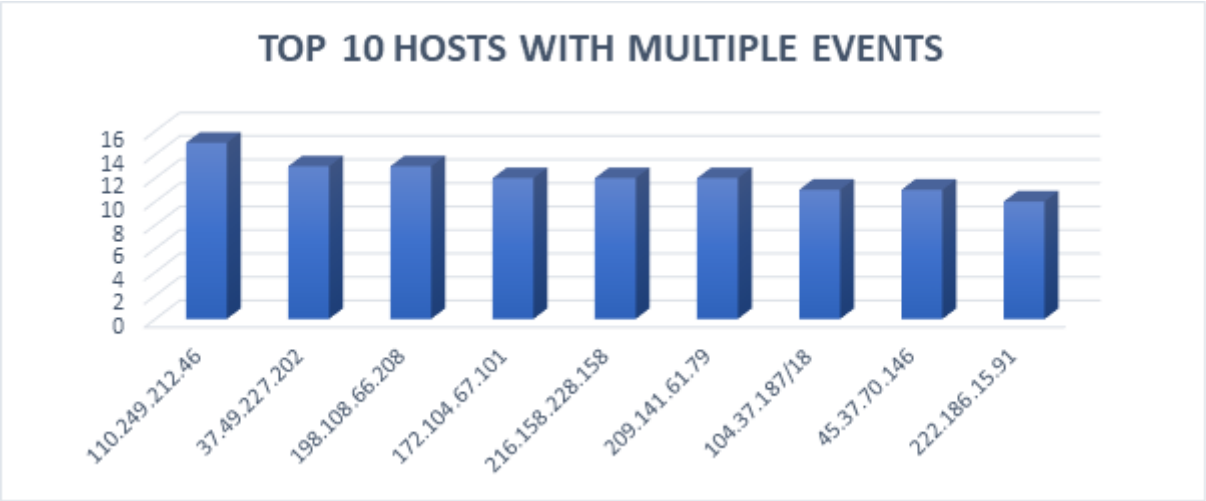
Taiwan	373	4.40%
Russian	345	4%
France	318	3.70%
United Kingdom	247	2.90%
Indonesia	185	2.20%
Mexico	182	2.10%
Italy	170	2%
Germany	151	1.80%
Turkey	149	1.70%
Thailand	139	1.60%
Canada	132	1.50%
Hong Kong	116	1.40%
Malaysia	115	1.30%





TOP ATTACKER HOSTS

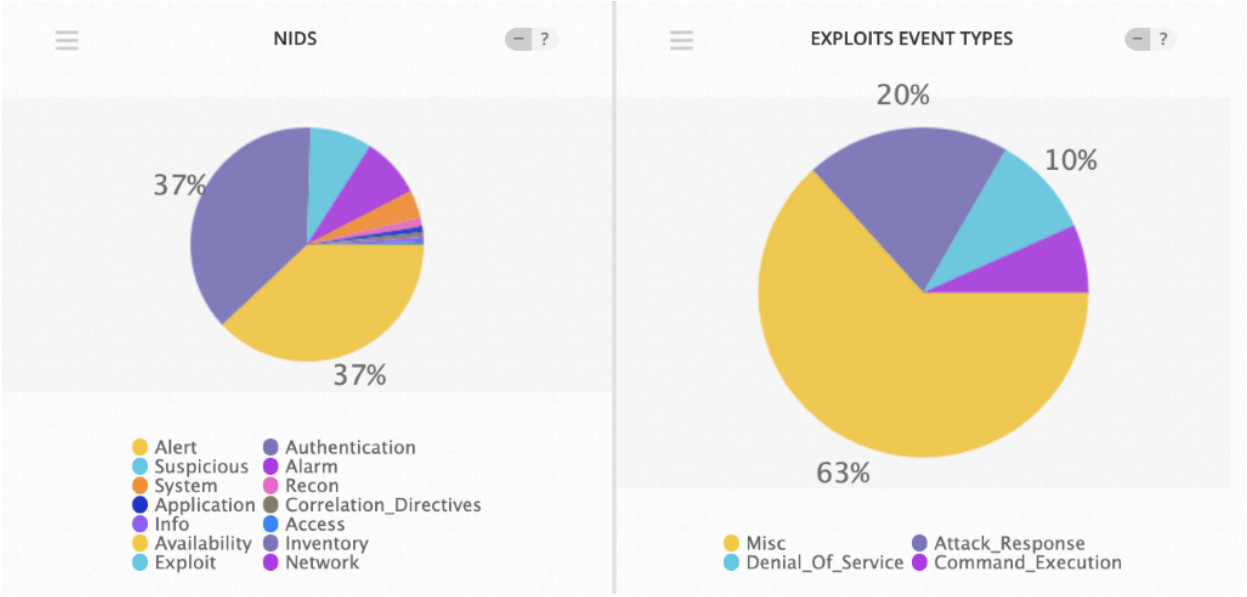
HOST	OCCURRENCES
110.249.212.46	15
37.49.227.202	13
198.108.66.208	13
172.104.67.101	12
216.158.228.158	12
209.141.61.79	12
104.37.187.18	11
45.37.70.146	11
222.186.15.91	10



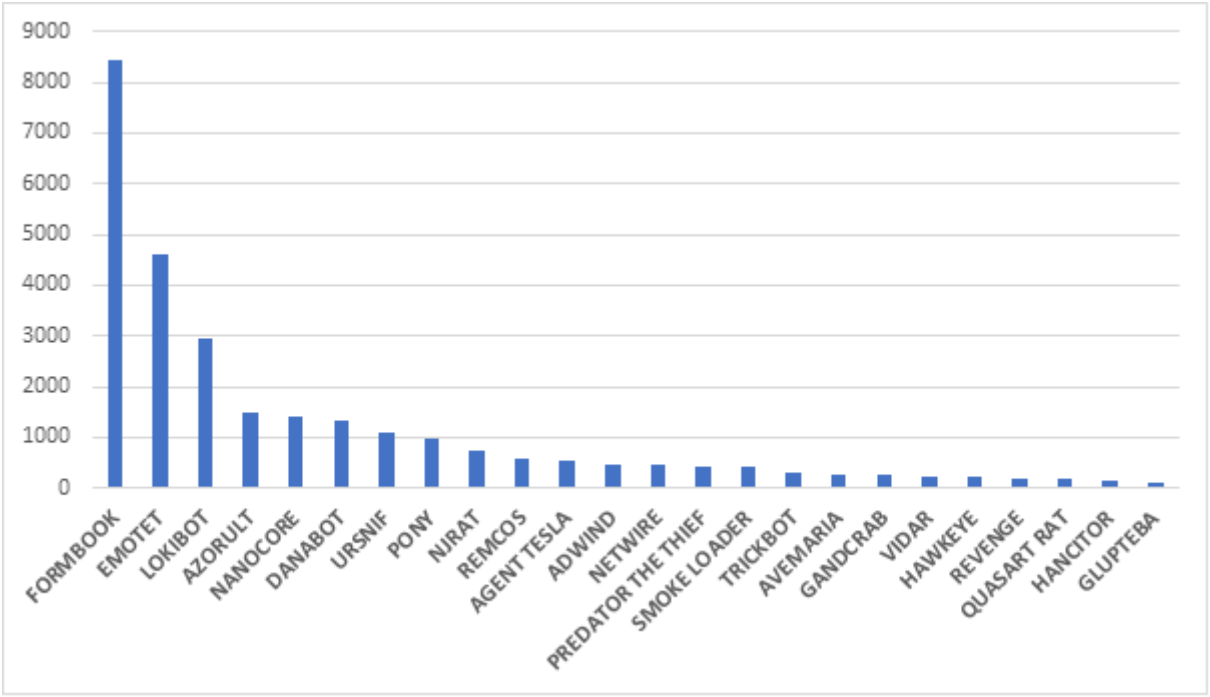
TOP NETWORK ATTACKERS

ORIGIN AS	COUNTRY	NAME:
AS4837	China	China Unicom Hebei province network
AS208666	Netherlands	XEMU
AS237	United States	Merit Network Inc
AS63949	United States	Linode
AS19318	United States	Interserver, Inc
AS53667	United States	FranTech Solutions
AS11426	United States	Charter Communications Inc
AS23650	China	CHINANET jiangsu province network

TOP EVENTS NIDS AND EXPLOITS



REMOTE ACCESS TROJAN C&C SERVERS FOUND



TROJAN, C&C SERVERS	NUMBERS OF IPS
FORMBOOK	8428
EMOTET	4621
LOKIBOT	2939

AZORULT	1504
NANOCORE	1415
DANABOT	1343
URSNIF	1078
PONY	969
NJRAT	731
REMCOS	584
AGENT TESLA	553
ADWIND	463
NETWIRE	443
PREDATOR THE THIEF	411
SMOKE LOADER	407
TRICKBOT	302
AVEMARIA	276
GANDCRAB	266
VIDAR	226
HAWKEYE	216
REVENGE	190
QUASART RAT	185
HANCITOR	145
GLUPTEBA	94

COMMON MALWARE

MD5	TYPICAL FILENAME	CLAIMED PRODUCT	DETECTION NAME

47b97de62ae8b2b927542aa5d7f3c858	qmreportupload.exe	qmreportupload	Win.Trojan.Generic::in10.talos
8c80dd97c37525927c1e549cb59bcbf3	eternalblue-2.2.0.exe	N/A	W32.85B936960F.5A5226262.auto.Talos
e2ea315d9a83e7577053f52c974f6a5a	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	W32.AgentWDCR:Gen.21gn.1201
88cbadec77cf90357f46a3629b6737e6	FlashHelperServices.exe	Flash Helper Services	PUA.Win.File.2144flashplayer::tpd
799b30f47060ca05d80ece53866e01cc	mf2016341595.exe	N/A	W32.Generic:Gen.22fz.1201

CVES FOR WHICH PUBLIC EXPLOITS HAVE BEEN DETECTED

CVE	DESCRIPTION	CVSS SCORE
CVE-2020-4198	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174909.	V3.1: 5.4 MEDIUM
	Published: March 03, 2020; 09:15:11 AM -05:00	V2: 3.5 LOW

CVE-2020-5403	Reactor Netty HttpServer, versions 0.9.3 and 0.9.4, is exposed to a URISyntaxException that causes the connection to be closed prematurely instead of producing a 400 response.	(not available)
	Published: March 03, 2020; 02:15:15 PM -05:00	
CVE-2020-5404	The HttpClient from Reactor Netty, versions 0.9.x prior to 0.9.5, and versions 0.8.x prior to 0.8.16, may be used incorrectly, leading to a credentials leak during a redirect to a different domain. In order for this to happen, the HttpClient must have been explicitly configured to follow redirects.	(not available)
	Published: March 03, 2020; 01:15:12 PM -05:00	
CVE-2020-1893	Insufficient boundary checks when decoding JSON inTryParse reads out of bounds memory, potentially leading to DOS. This issue affects HHVM 4.45.0, 4.44.0, 4.43.0, 4.42.0, 4.41.0, 4.40.0, 4.39.0, versions between 4.33.0 and 4.38.0 (inclusive), versions between 4.9.0 and 4.32.0 (inclusive), and versions prior to 4.8.7.	(not available)
	Published: March 03, 2020; 10:15:12 AM -05:00	