TRENDS

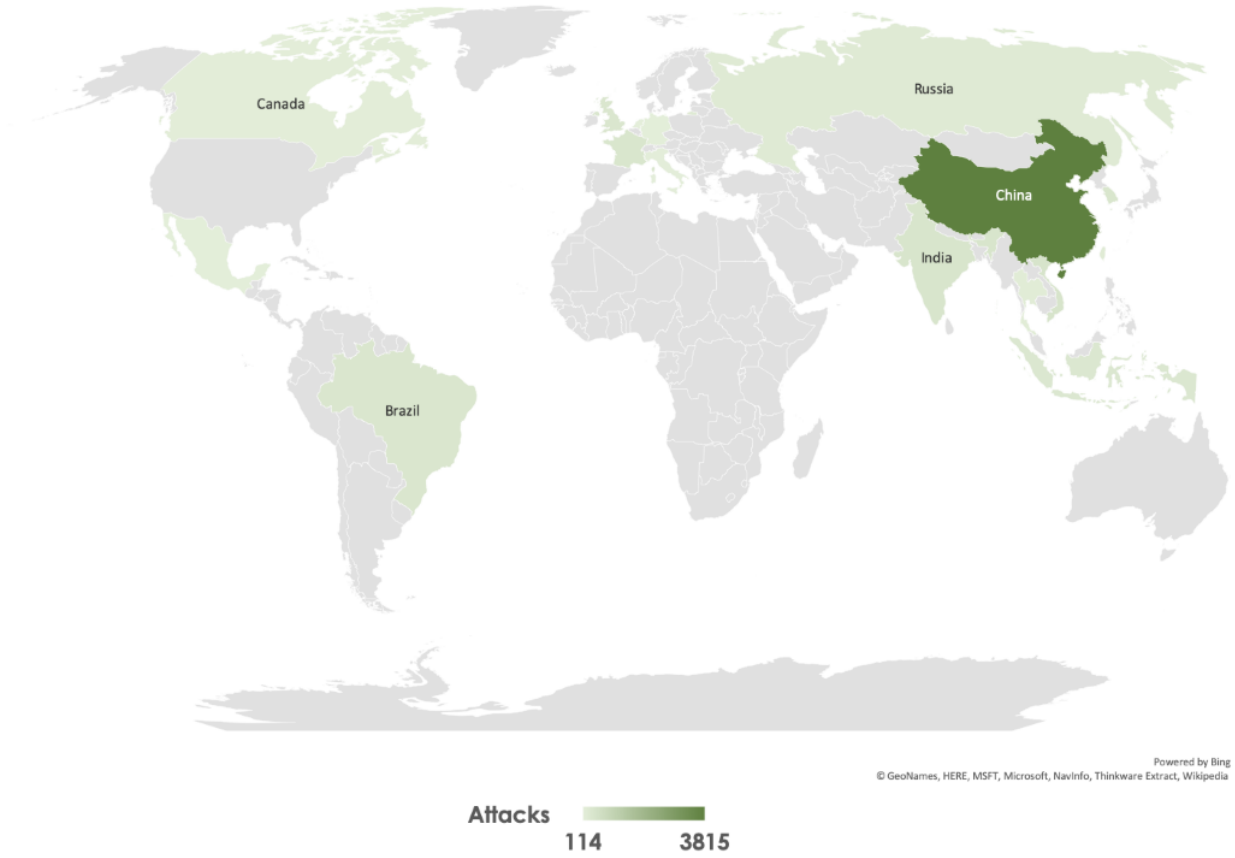
The top attacker country was China with 3815 unique attackers (37%). This represents an important increase of 5% comparing to previous week.

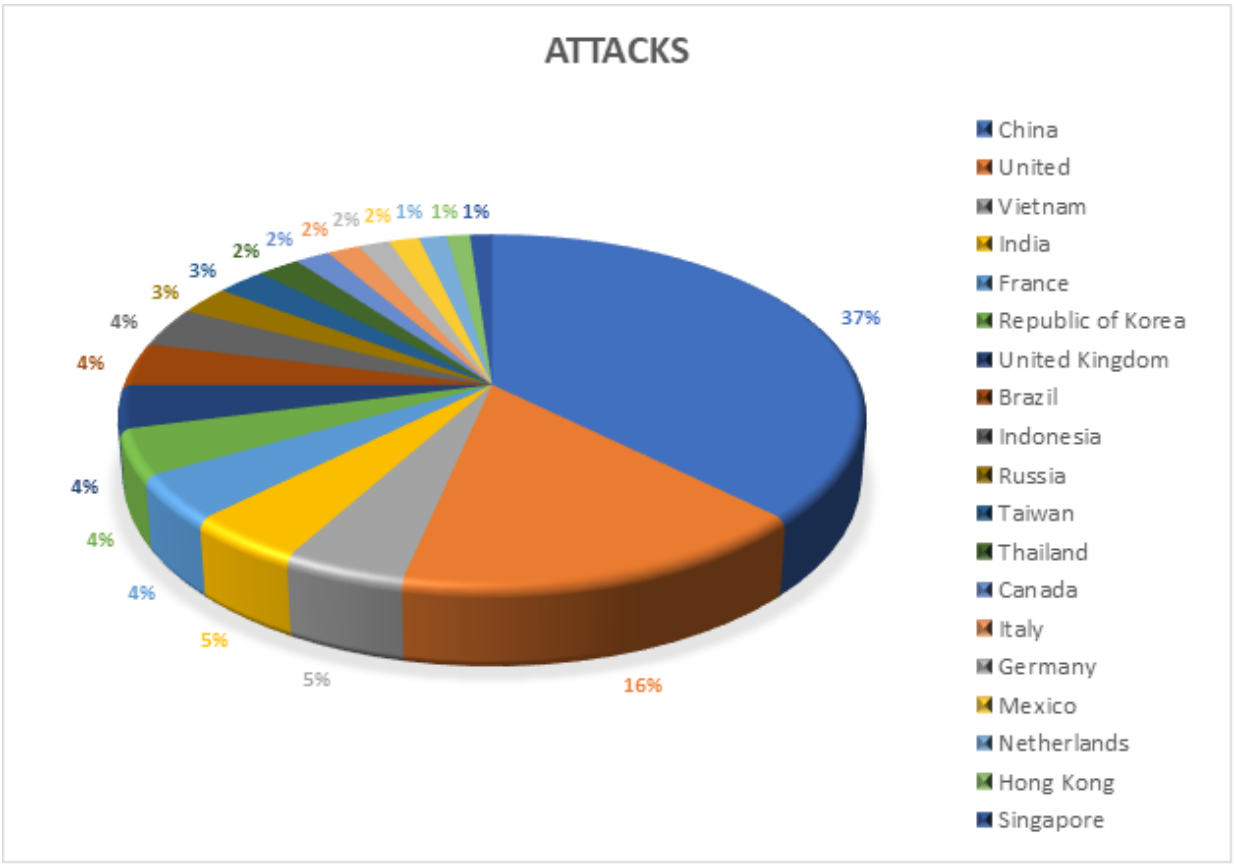
The top Exploit event was Miscellaneous with 55% of occurrences.
The top Trojan C&C server detected was Formbook with an increase of 2% of new IP addresses comparing to last week.

TOP ATTACKER COUNTRIES

COUNTRY	OCCURRENCES	PERCENTAGE%
China	3815	37%
United States	1638	16%
Vietnam	481	5%
India	460	5%
France	431	4%

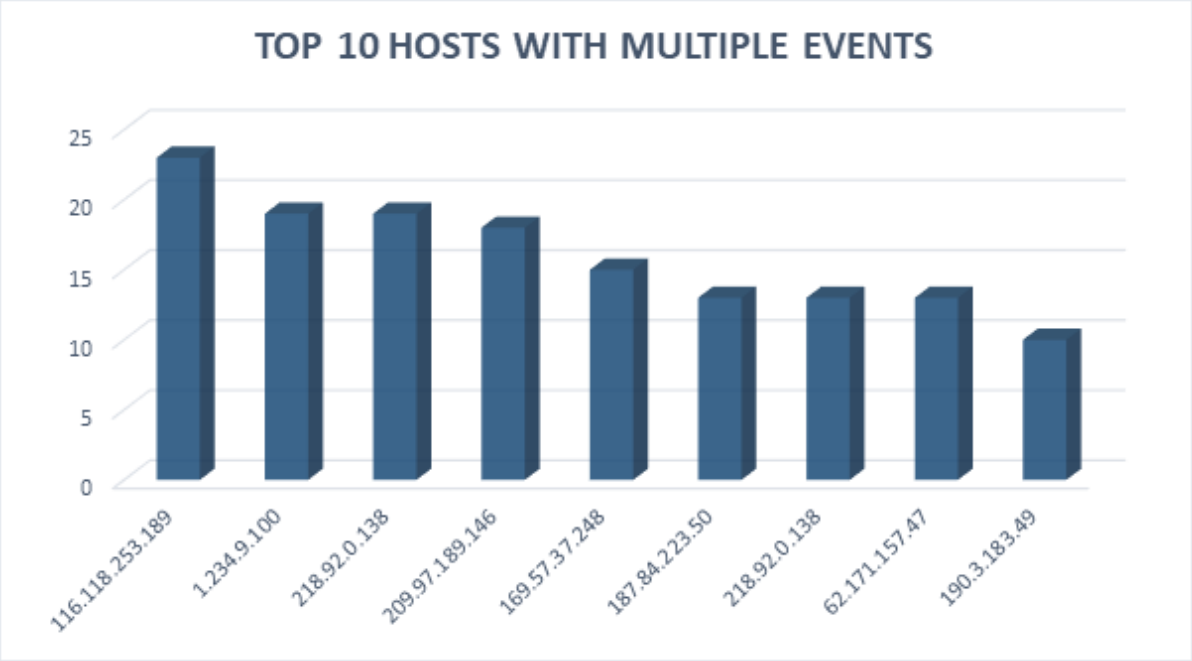
Republic of Korea	428	4%
United Kingdom	406	4%
Brazil	402	4%
Indonesia	371	4%
Russia	268	3%
Taiwan	257	3%
Thailand	218	2%
Canada	179	2%
Italy	169	2%
Germany	160	2%
Mexico	155	2%
Netherlands	143	1%
Hong Kong	119	1%
Singapore	114	1%


Canada
Russia
China
India
Brazil
Powered by Bing
© GeoNames, HERE, MSFT, Microsoft, Navinfo, Thinkware Extract, Wikipedia
Attacks
114
3815


ATTACKS
37%
16%
5%
5%
4%
4%
4%
4%
4%
3%
3%
2%
2%
2%
2%
1%
1%
1%
China
United
Vietnam
India
France
Republic of Korea
United Kingdom
Brazil
Indonesia
Russia
Taiwan
Thailand
Canada
Italy
Germany
Mexico
Netherlands
Hong Kong
Singapore

TOP ATTACKER HOSTS

HOST	OCCURRENCES
116.118.253.189	23
1.234.9.100	19
218.92.0.138	19
209.97.189.146	18
169.57.37.248	15
187.84.223.50	13
218.92.0.138	13
62.171.157.47	13
190.3.183.49	10

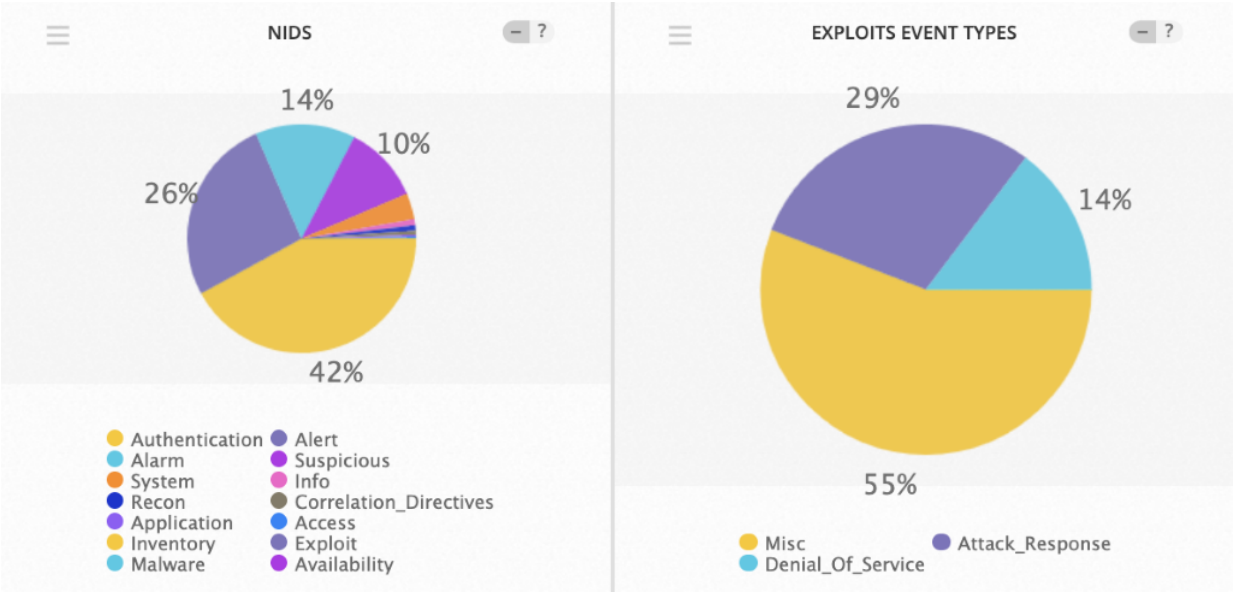


TOP NETWORK ATTACKERS

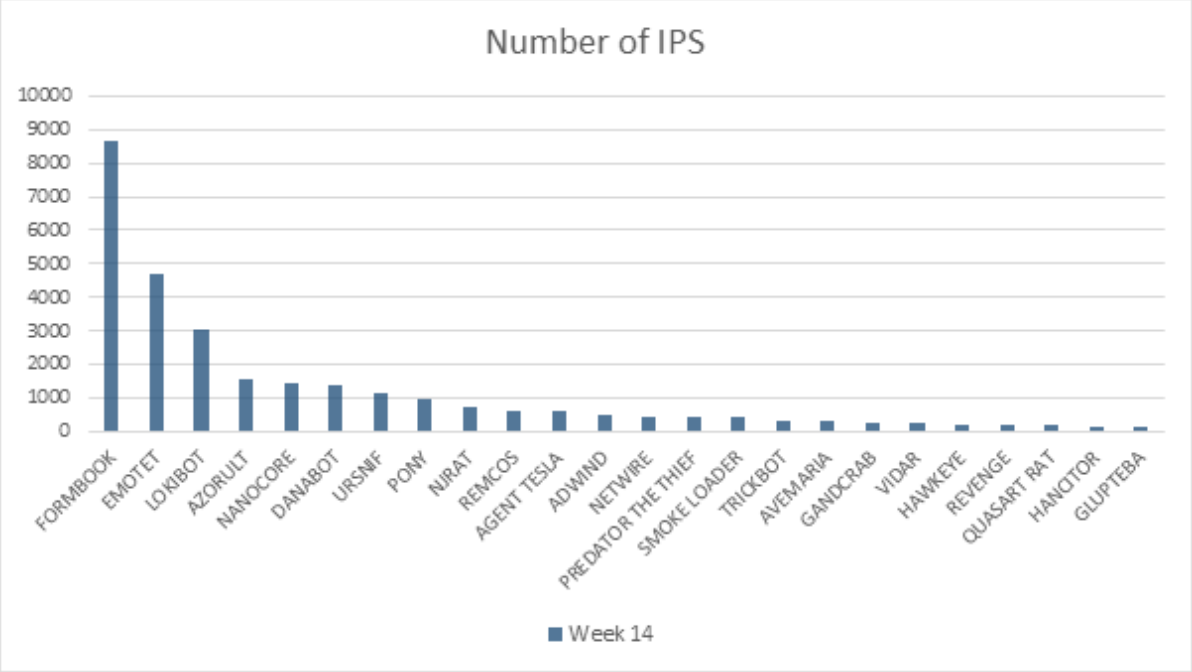
ORIGIN AS	COUNTRY	NAME:

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
AS199883	United Kingdom	ArubaCloud Limited

TOP EVENTS NIDS AND EXPLOITS



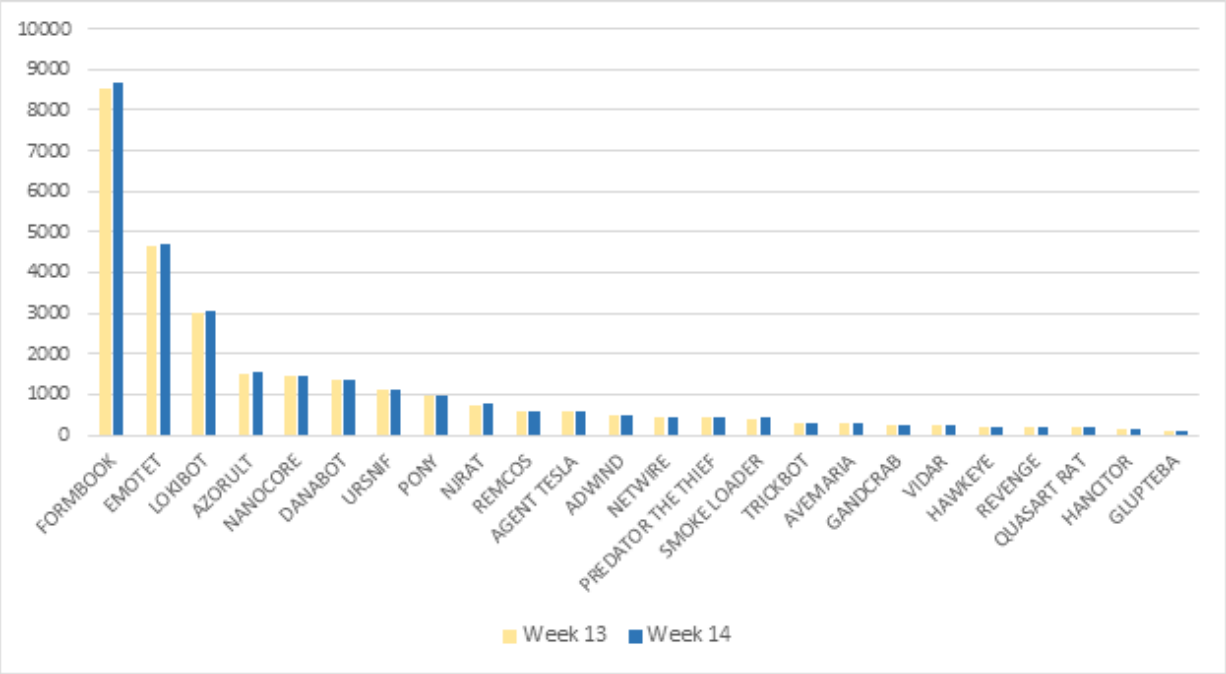
REMOTE ACCESS TROJAN C&C SERVERS FOUND



MALWARE	WEEK 14
FORMBOOK	8992
EMOTET	4695
LOKIBOT	3049
AZORULT	1534
NANOCORE	1455
DANABOT	1351
URSNIF	1126
PONY	977
NJRAT	755
REMCOS	604
AGENT TESLA	597
ADWIND	467
NETWIRE	443
PREDATOR THE THIEF	421
SMOKE LOADER	415

TRICKBOT	306
AVEMARIA	288
GANDCRAB	266
VIDAR	228
HAWKEYE	218
REVENGE	196
QUASART RAT	185
HANCITOR	145
GLUPTEBA	104
RACOON	95
DRIDEX	88
FLAWEDAMMYY	59
ICEID	63
ORCUS RAT	43
GOOTKIT	39
NEMTY	29
WANNACRY	21
TROLDESH	3
SODINOKIBI	0

Comparing to last week:



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
aa9bb66a406b5519e2063a65479dab90	output.148937912.txt	N/A	Win.Dropper.Generic::vv
7c38a43d2ed9af80932749f6e80fea6f	wup.exe	N/A	PUA.Win.File.Coinminer::1201
88cbadec77cf90357f46a3629b6737e6	FlashHelperServices.exe	Flash Helper Services	PUA.Win.File.2144flashplayer::tpd

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 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)
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)
CVE-2020-1893	Insufficient boundary checks when decoding JSON in TryParse 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)