TRENDS

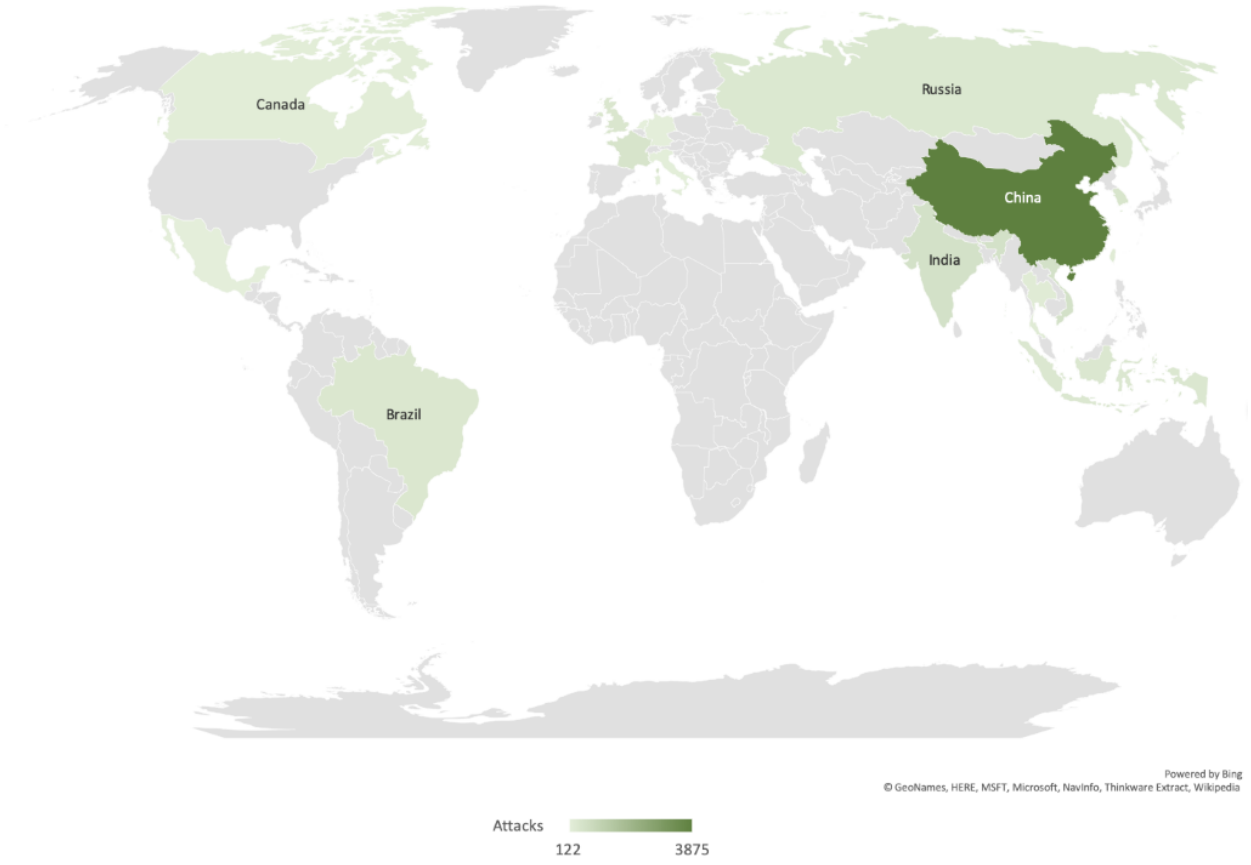
The top attacker country was China with 3875 unique attackers (36%). This represents an important increase of 5% comparing to previous week.

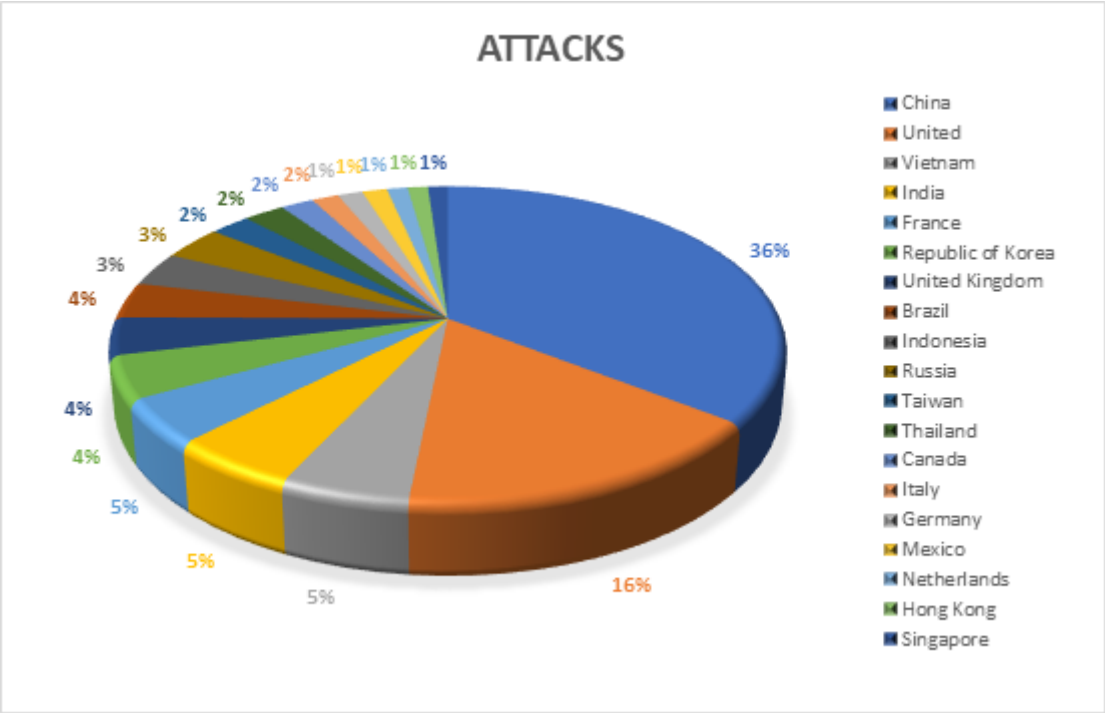
The top Exploit event was Miscellaneous with 50% of occurrences.
The top Trojan C&C server detected was Formbook with 8674 instances detected.

TOP ATTACKER COUNTRIES

COUNTRY	OCCURRENCES	PERCENTAGE%
China	3875	36%
United	1749	16%
Vietnam	590	5%
India	585	5%
France	496	5%
Republic of Korea	477	4%
United Kingdom	418	4%

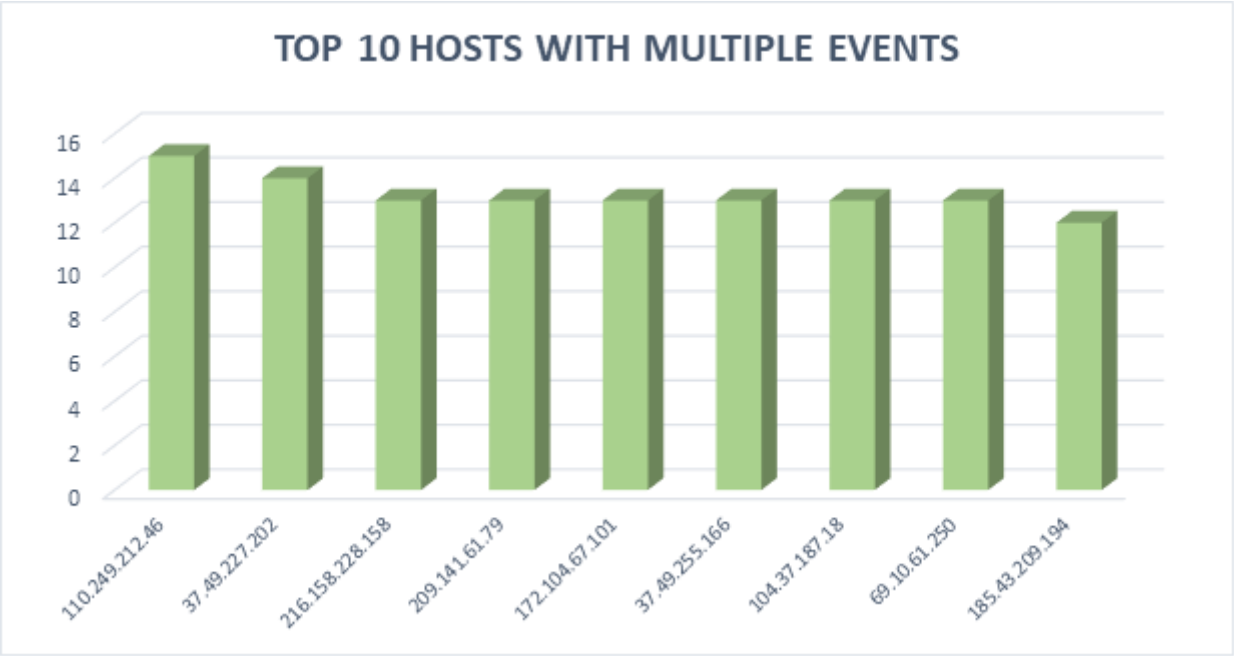
Brazil	399	4%
Indonesia	379	3%
Russia	377	3%
Taiwan	251	2%
Thailand	251	2%
Canada	205	2%
Italy	166	2%
Germany	155	1%
Mexico	152	1%
Netherlands	129	1%
Hong Kong	125	1%
Singapore	122	1%





TOP ATTACKER HOSTS

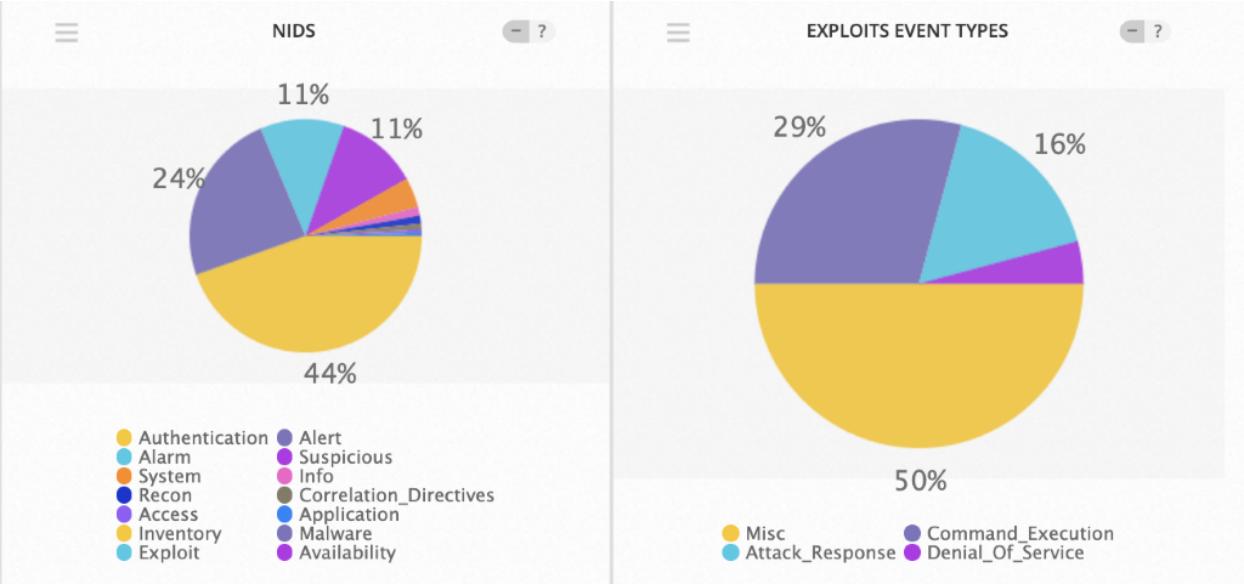
HOST	OCCURRENCES
110.249.212.46	15
37.49.227.202	14
216.158.228.158	13
209.141.61.79	13
172.104.67.101	13
37.49.255.166	13
104.37.187.18	13
69.10.61.250	13
185.43.209.194	12



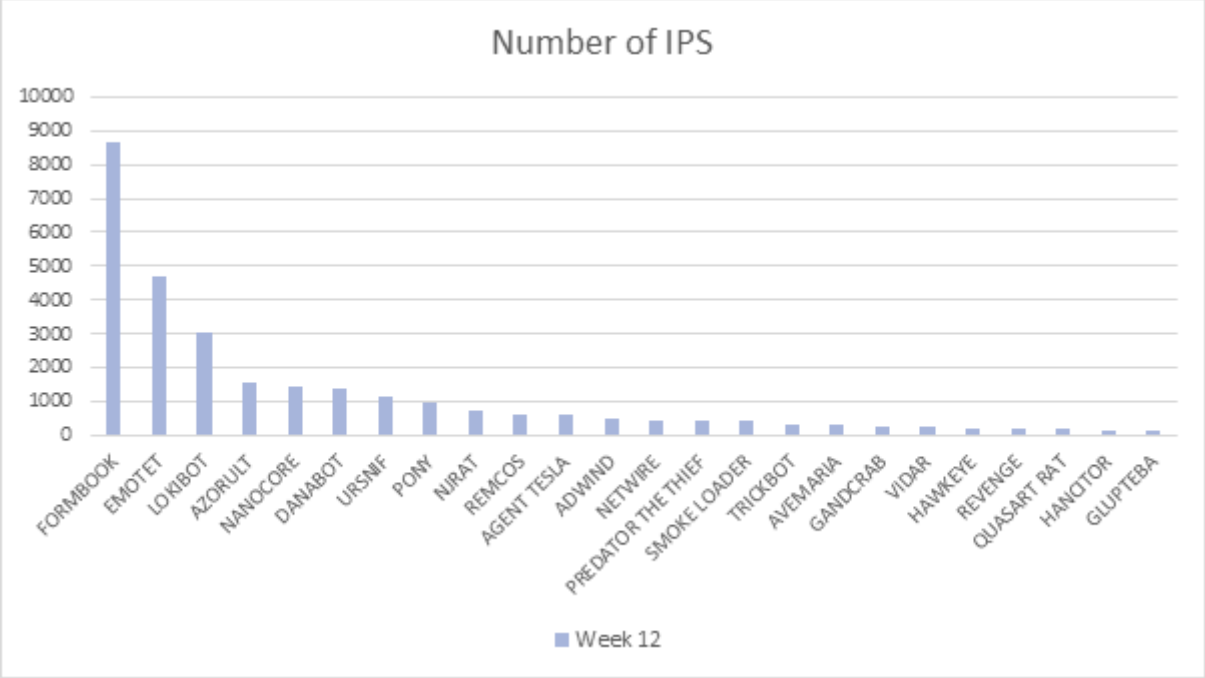
TOP NETWORK ATTACKERS

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

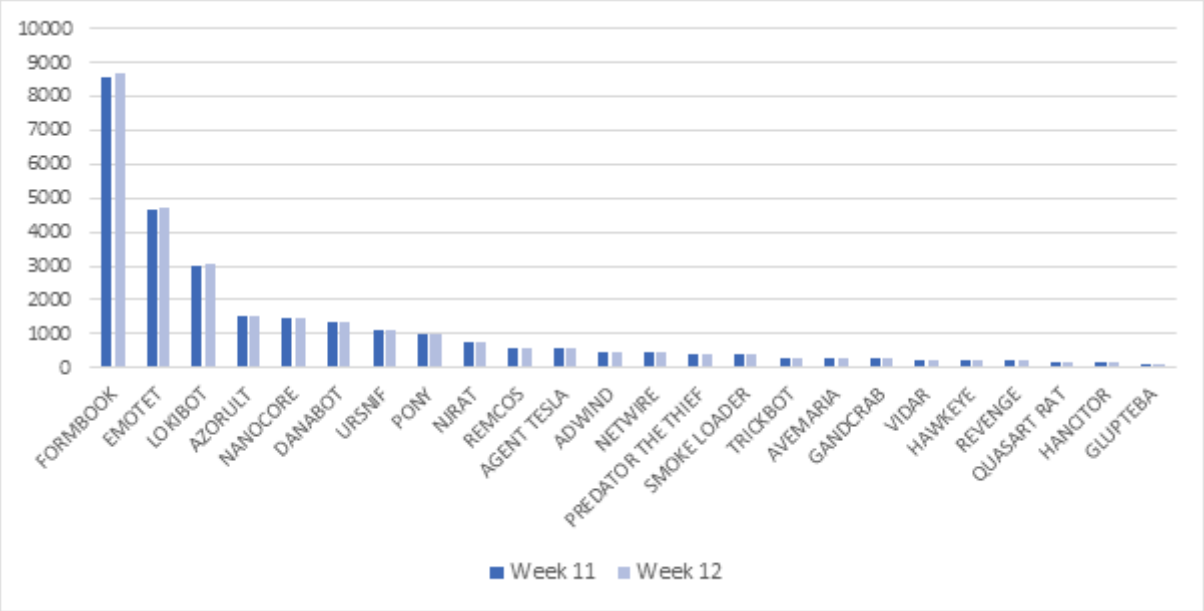


MALWARE	WEEK 12
FORMBOOK	8674
EMOTET	4695
LOKIBOT	3049

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-2020-0688	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links. An attacker who successfully exploited this vulnerability could bypass access restrictions to add or remove files. Vendor: Microsoft	CVSS v3 Base Score: 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-8597	pppd (Point to Point Protocol Daemon) is vulnerable to buffer overflow due to a flaw in Extensible Authentication Protocol (EAP) packet processing in eap_request and eap_response subroutines. The vulnerability is in the logic of the eap parsing code. By sending an unsolicited EAP packet to a vulnerable ppp client or server, an unauthenticated remote attacker could cause memory corruption in the pppd process, which may allow for arbitrary code execution. Vendor: Multi-Vendor	CVSS v3 Base Score: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVE-2020-9334	A stored cross site scripting vulnerability exists in the Envira Photo Gallery plugin for WordPress. Successful exploitation of this vulnerability would allow a authenticated low privileged user to inject arbitrary JavaScript code that is viewed by other users. Vendor: WordPress	CVSS v3 Base Score: 5.4 (AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)
CVE-2020-10189	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic. Vendor: Multi-Vendor	CVSS v3 Base Score: 3.1 (AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2020-1938	Due to a file inclusion defect in the AJP service (port 8009) that is enabled by default in Tomcat, an attacker can construct a malicious request package for file inclusion operation, and then read the web directory file on the affected Tomcat server. Vendor: Apache	CVSS v3 Base Score: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)