Red Piranha
unified threat management

Threat Intelligence Report

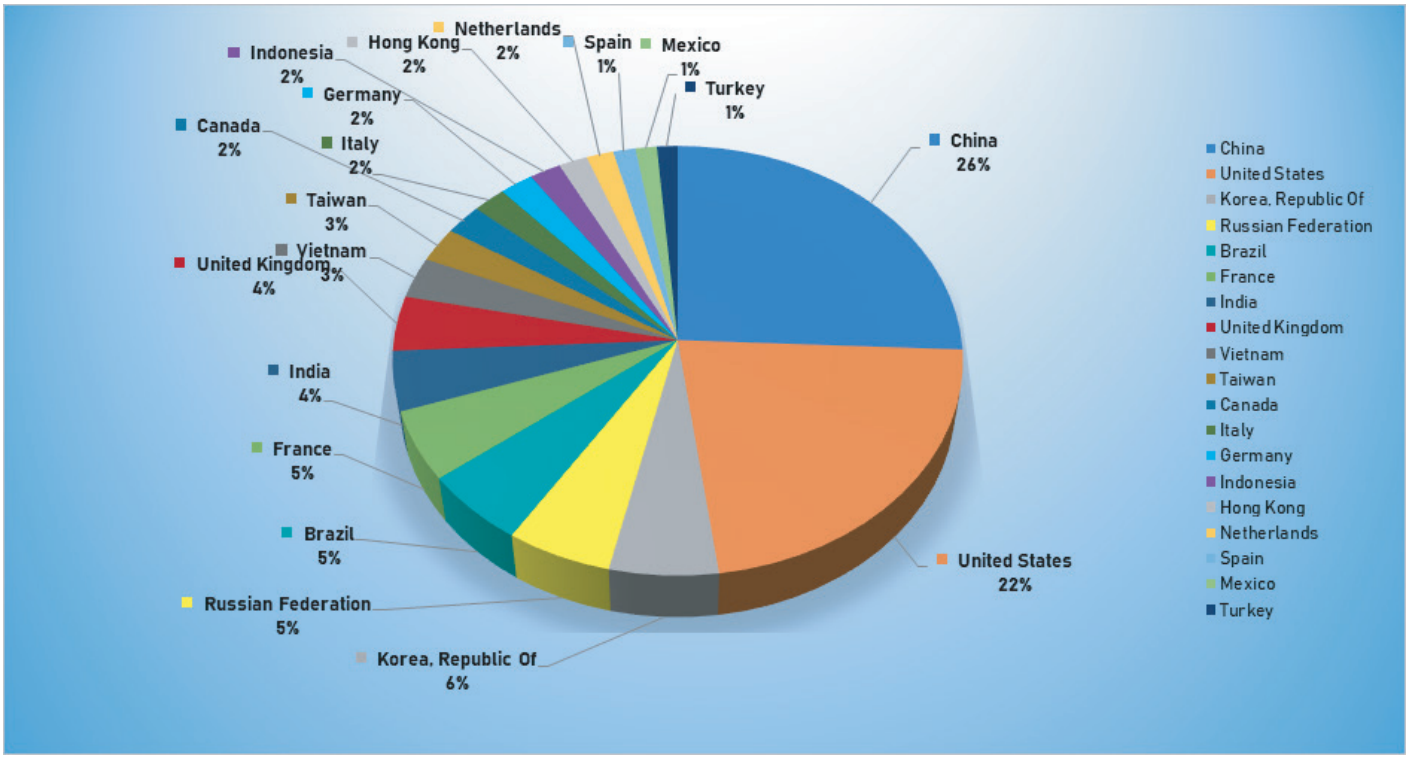
September 30 - October 6, 2019

Trends

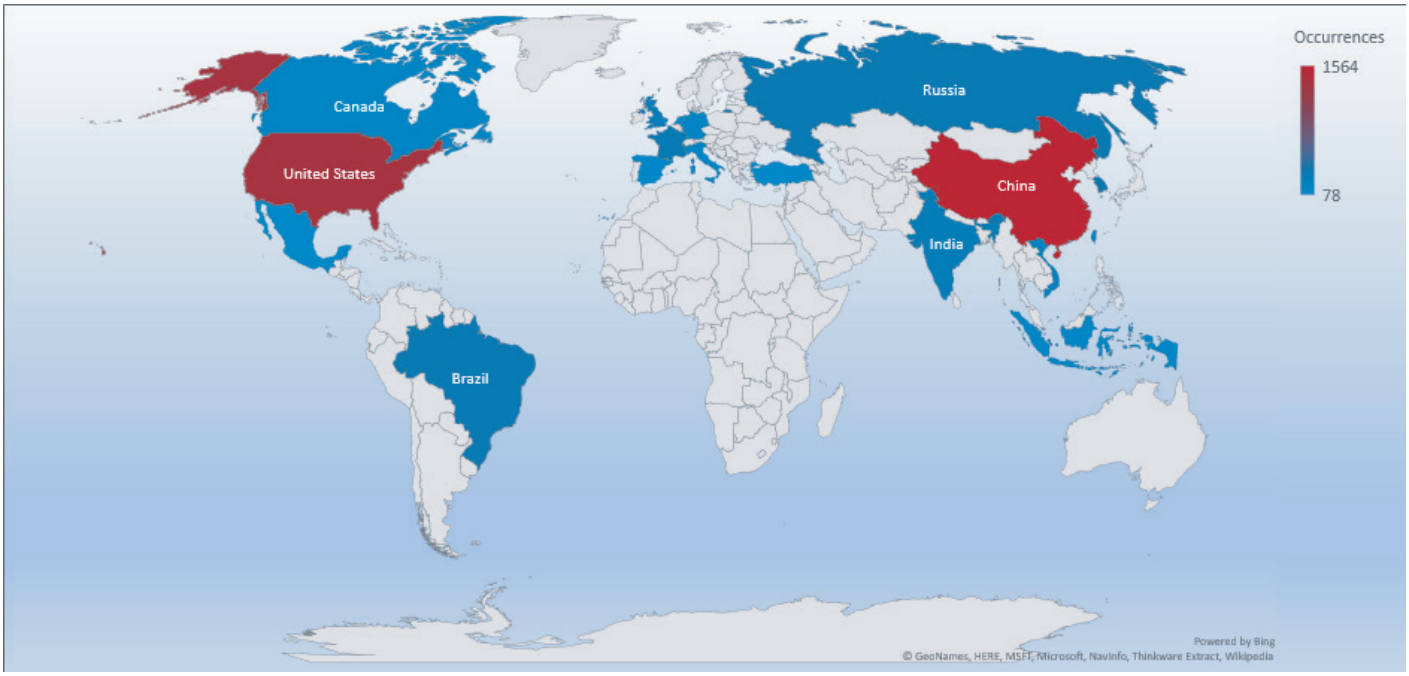
- **The top attacker country was China with 1564 unique attackers (25%)**
- **The top Exploit event was Authentication with 50% of occurrences.**
- **The top Trojan C&C server detected was Heodo with 6 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	1564	25.70%
United States	1350	22.19%
Korea	344	5.65%
Russian Federation	334	5.49%
Brazil	334	5.49%
France	317	5.21%
India	273	4.49%
United Kingdom	251	4.12%
Vietnam	189	3.11%
Taiwan	160	2.63%
Canada	141	2.32%
Italy	127	2.09%
Germany	127	2.09%
Indonesia	119	1.96%
Hong Kong	109	1.79%
Netherlands	102	1.68%
Spain	85	1.40%
Mexico	81	1.33%
Turkey	78	1.28%

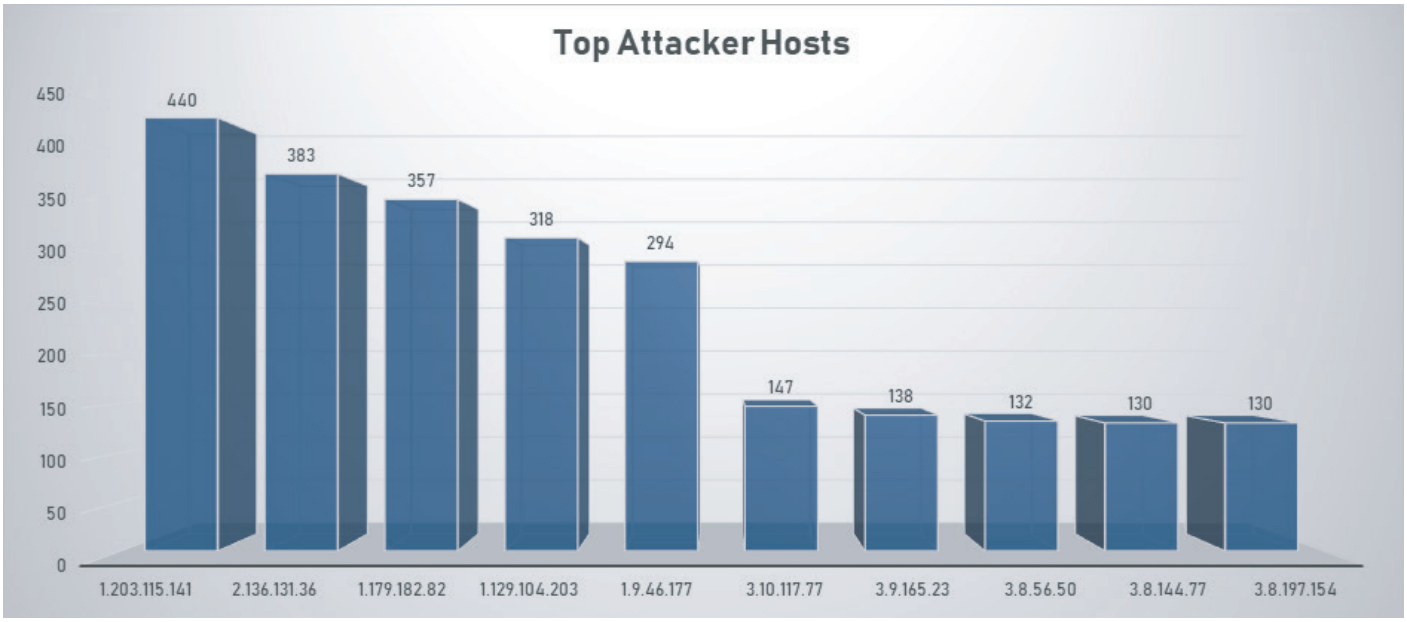


Threat Geo-location



Top Attacking Hosts

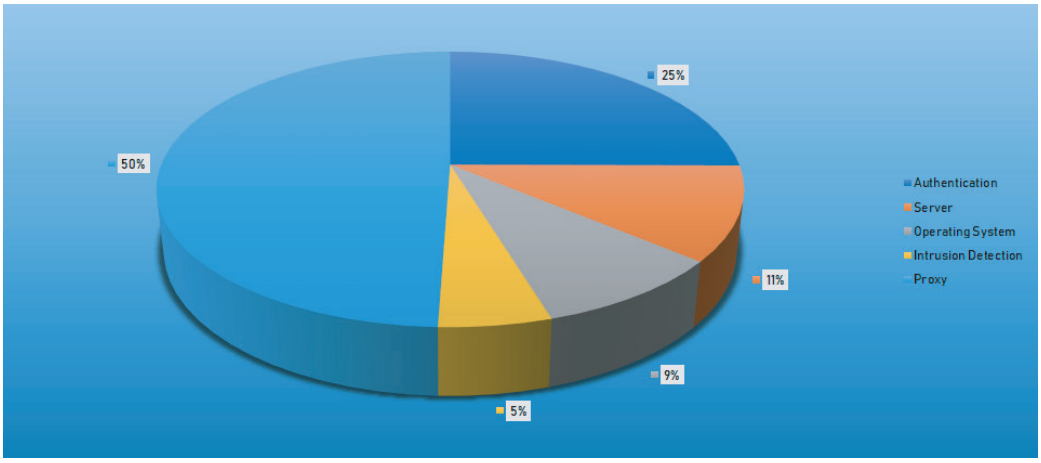
Host	Occurrences
1.203.115.141	440
2.136.131.36	383
1.179.182.82	357
1.129.104.203	318
1.9.46.177	294
3.10.117.77	147
3.9.165.23	138
3.8.56.50	132

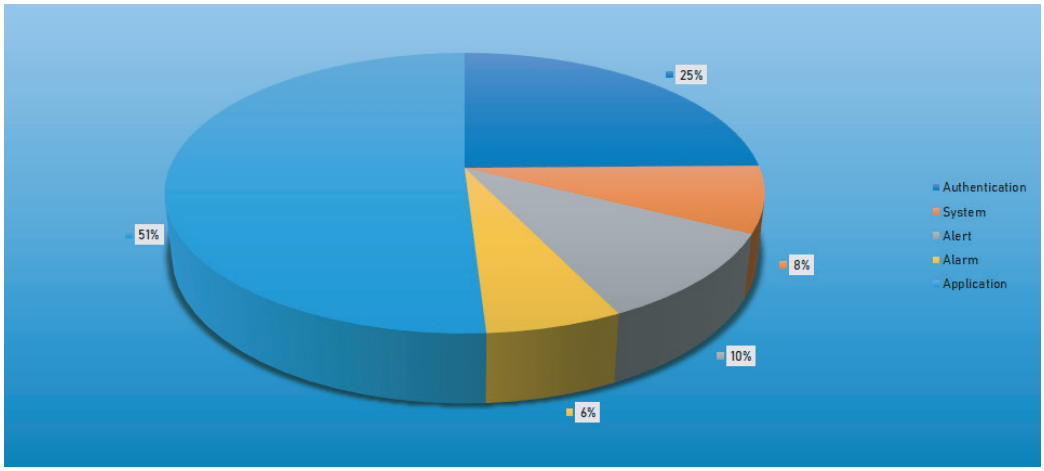


Top Network Attackers

Origin AS	Announcement	Description
AS4847	1.203.0.0/16	CHINANET Beijing Province Network
AS3352	2.136.0.0/16	Red de servicios IP
AS23969	1.179.128.0/17	TOT Public Company Limited

Top Event NIDS and Exploits



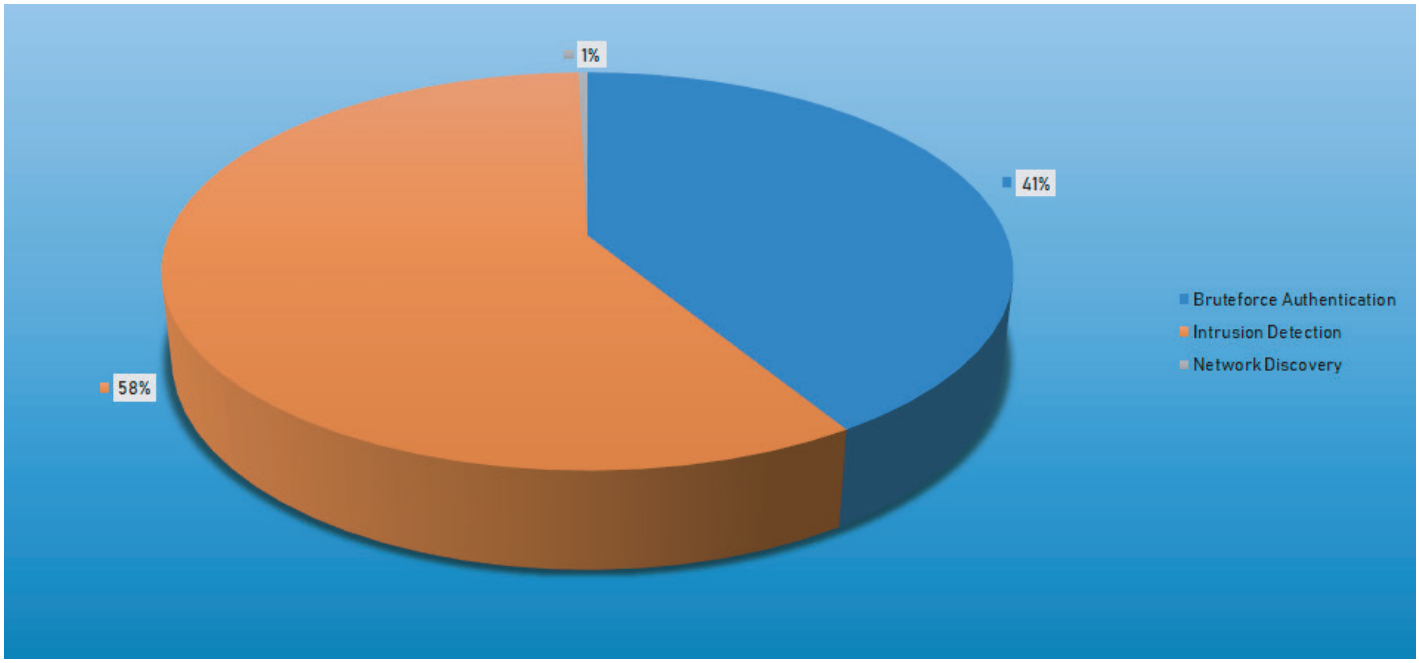


Top Alarms

Type of Alarm	Occurrences
Bruteforce Authentication	2035
Intrusion Detection	2879
Network Discovery	20

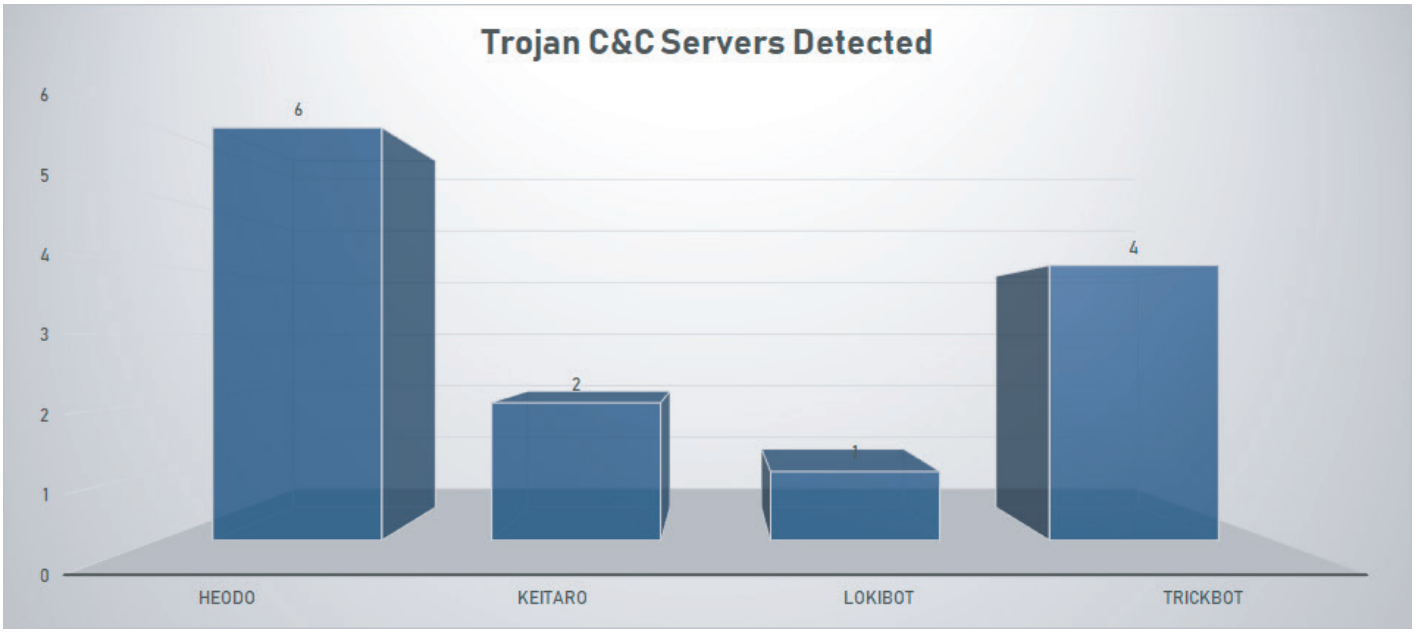
Comparison from last week

Type of Alarm	Occurrences
Bruteforce Authentication	256
Network Discovery IDS Event	195
Network Anomaly - IDS Event	18
Database Attack - Stored Procedure Access - Attack	6



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	6	179.12.170.88, 181.230.126.152, 187.155.233.46, 198.199.88.162, 201.250.11.236, 86.98.25.30
Keitaro	2	5.188.231.211, 5.8.88.124
LokiBot	1	47.254.66.50
TrickBot	4	178.252.26.235, 185.222.202.62, 194.5.250.79, 66.55.71.15



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF 71AFA8-95. SBX.TG	4a5078 0ddb3d b16eba b57b0c a42da0 fb	xme64-2141.exe
Win.Trojan. Generic:: in10.talos	47b97d e62ae8 b2b927 542aa5 d7f3c8 58	qmreportupload.exe
PUA.Win. Trojan.Remote exec::tpd	fbc6bd 8bf115 cb3f93 a520d2 2b054b 90	NA
W32.Agent WDCR:Gen. 21gn.1201	e2ea31 5d9a83 e75770 53f52c 974f6a 5a	c3e530cc005583b 47322b6649ddc0d ab1b64bcf22b124a 492606763c52fb04 8f.bin
W32.Generic :Gen.22fz. 1201	799b30 f47060 ca05d8 0ece53 866e01 cc	mf2016341595.exe

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-1367
Title: Microsoft Internet Explorer Remote Code Execution Vulnerability
Vendor: Microsoft

Description: A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email.

Note: This CVE ID is unique from CVE-2019-1221.
CVSS v2 Base Score: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

ID: CVE-2019-16097
Title: Harbor Remote Privilege Escalation Vulnerability
Vendor: Multi-Vendor

Description: A vulnerability in the POST /api/users API of Harbor may allow for a remote escalation of privilege. A malicious attacker with network access to a Harbor POST /api/users API could self-register a new account with administrative privileges. Successful exploitation of this issue may lead to a complete compromise of the Harbor deployment.

CVSS v2 Base Score: 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

ID: CVE-2019-15943
Title: Counter-Strike Global Offensive Remote Code Execution Vulnerability
Vendor: valvesoftware

Description: Counter-Strike Global Offensive (vphysics.dll) allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, using a crafted map that causes memory corruption vulnerability.

CVSS v2 Base Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ID: CVE-2019-12562
Title: DotNetNuke Store Cross-Site Scripting vulnerability
Vendor: Multi-Vendor

Description: A stored cross site scripting vulenrability in DotNetNuke (DNN) allows remote attackers to store and embed the malicious script into the admin notification page. The exploit could be used to perfom any action with admin privileges such as managing content, adding users, uploading backdoors to the server, etc. Successful exploitation occurs when an admin user visits a notification page with stored cross-site scripting.

CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

ID: CVE-2019-1914
Title: Cisco Small Business 220 Series Smart Switches Command Injection Vulnerability
Vendor: Cisco

Description: A vulnerability in the web management interface of Cisco Small Business 220 Series Smart Switches could allow an authenticated, remote attacker to perform a command injection attack. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a malicious request to certain parts of the web management interface. To send the malicious request, the attacker needs a valid login session in the web management interface as a privilege level 15 user. Depending on the configuration of the affected switch, the malicious request must be sent via HTTP or HTTPS. A successful exploit could allow the attacker to execute arbitrary shell commands with the privileges of the root user.

CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)