Red Piranha
unified threat management

Threat Intelligence Report

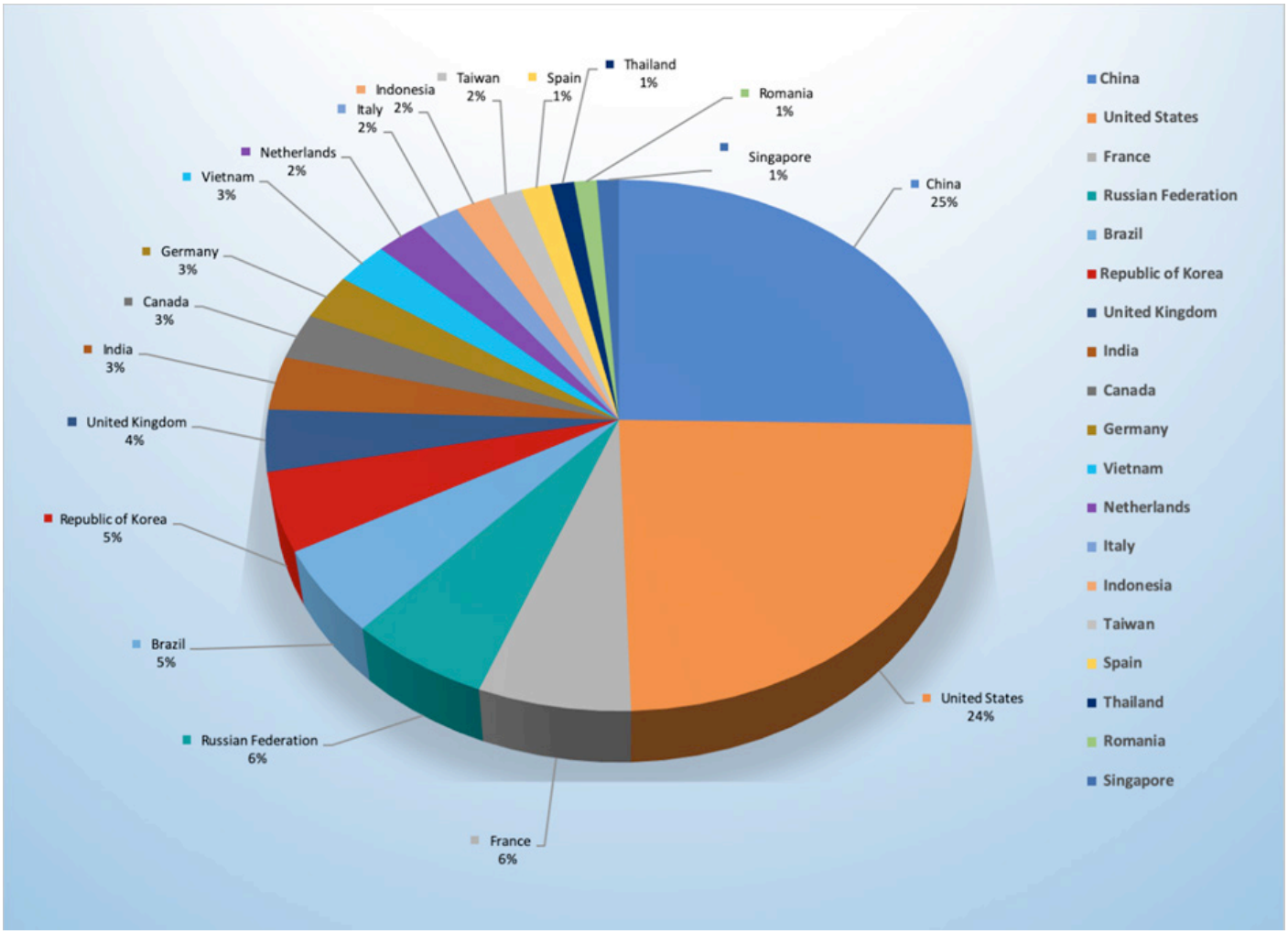
September 23-29, 2019

Trends

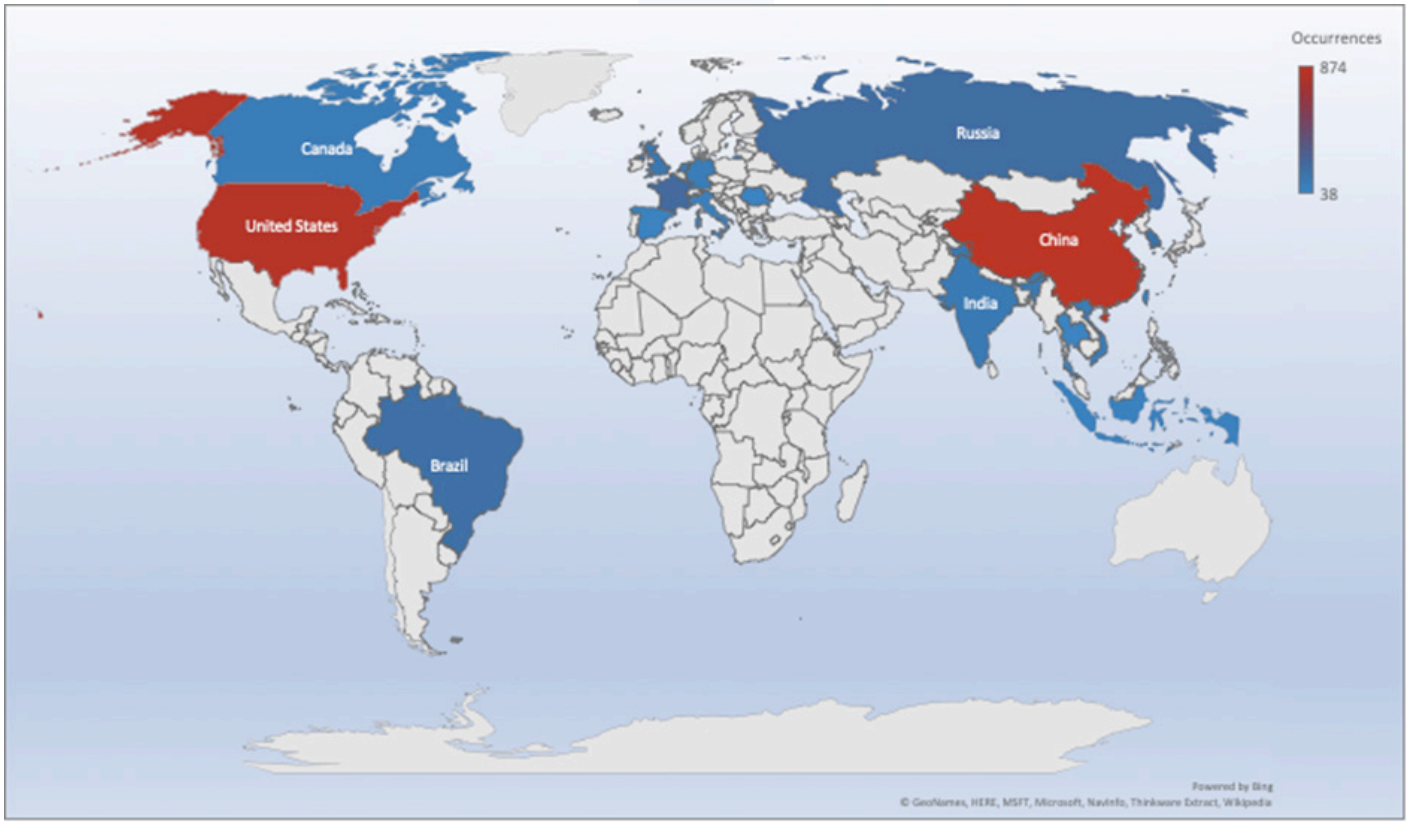
- **The top attacker country was China with 874 unique attackers (33%)**
- **The top Exploit event was Miscellaneous with 65% of occurrences.**
- **The top Trojan C&C server detected was TrickBot with 36 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	874	25.30%
United States	836	24.20%
France	211	6.40%
Russian Federation	205	5.93%
Brazil	181	5.24%
Republic of Korea	166	4.80%
United Kingdom	130	3.76%
India	113	3.27%
Canada	98	2.84%
Germany	97	2.81%
Vietnam	91	2.63%
Netherlands	84	2.43%
Italy	72	2.08%
Indonesia	60	1.74%
Taiwan	58	1.68%
Spain	51	1.48%
Thailand	41	1.19%
Romania	39	1.13%
Singapore	38	1.10%

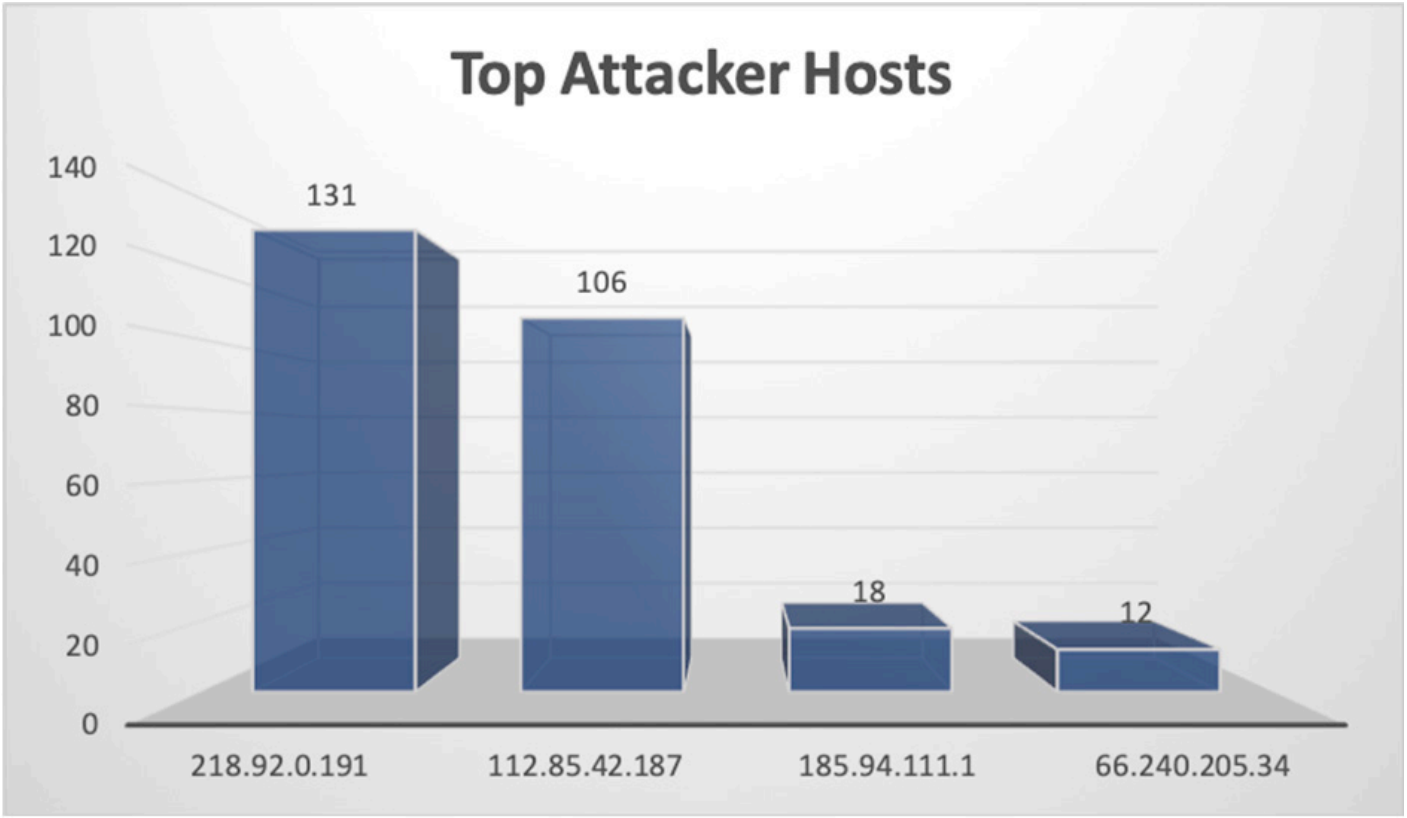


Threat Geo-location



Top Attacking Hosts

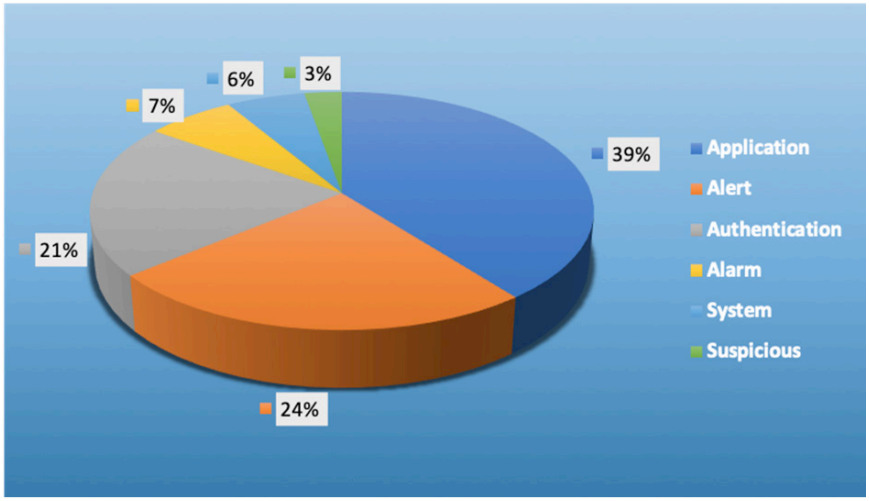
Host	Occurrences
218.92.0.191	131
112.85.42.187	106
185.94.111.1	18
66.240.205.34	12

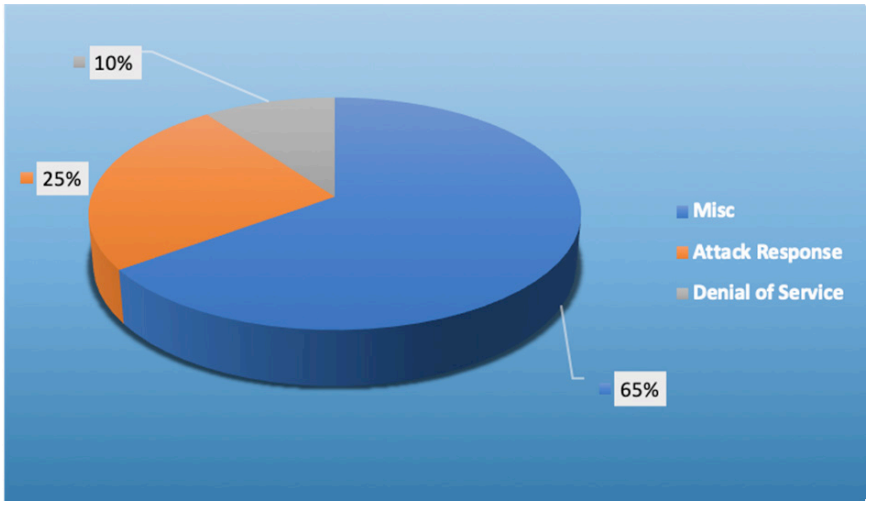


Top Network Attackers

Origin AS	Announcement	Description
AS4134	218.92.0.0/16	CHINANET jiangsu province network
AS4837	12.80.0.0/13	China Unicom Jiangsu province network
AS10439	66.240.192.0/18	CariNet, Inc

Top Event NIDS and Exploits



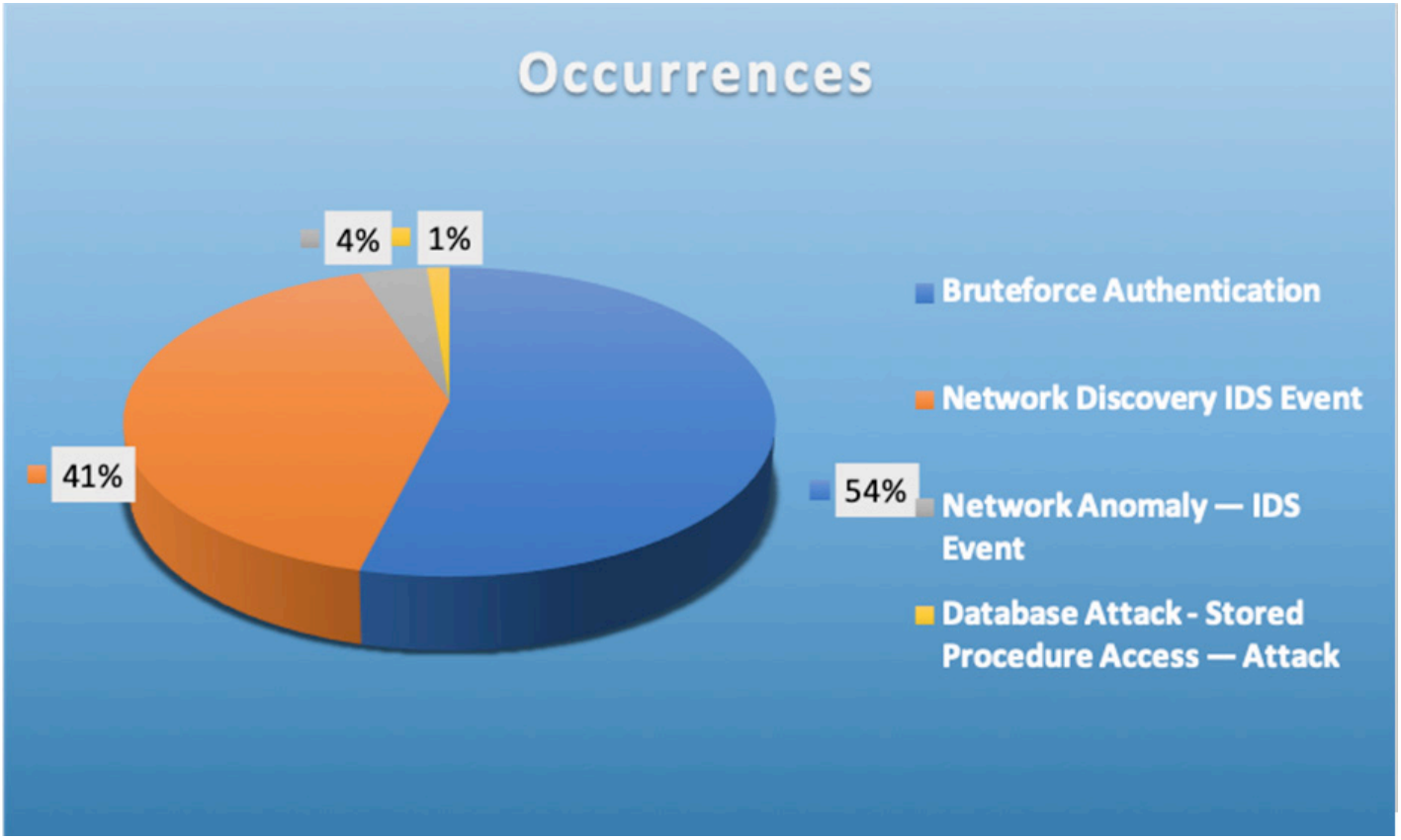


Top Alarms

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

Comparison from last week

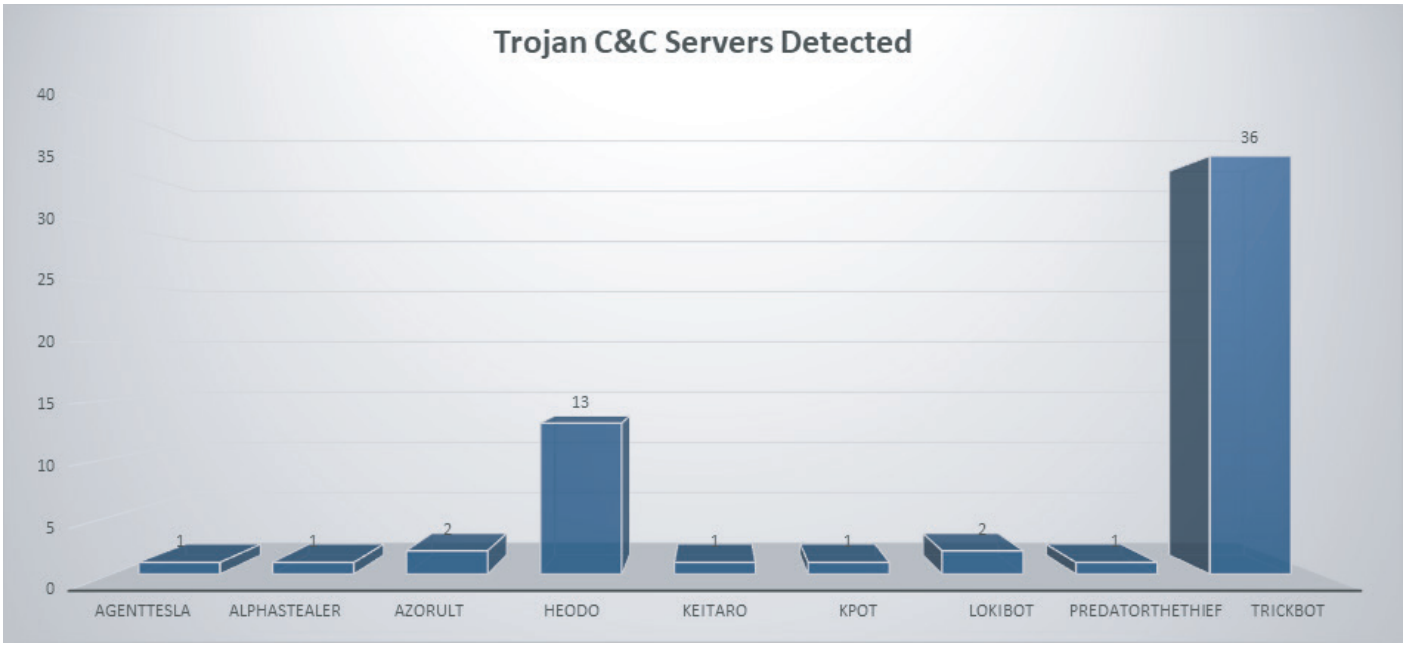
Type of Alarm	Occurrences
WebServer Attack	1433
Bruteforce Authentication	320
Attack Tool Detected	96
Network Discovery	26
Network Anomaly	22
Database attack	2



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	161.117.182.74
AlphaStealer	1	178.208.83.42
Azorult	2	185.173.178.77, 185.224.138.189
Heodo	13	142.44.162.209, 149.202.153.251, 162.241.130.39, 181.188.149.134, 183.82.97.25, 192.241.175.184, 201.212.57.109, 203.130.0.67, 5.67.96.120, 75.127.14.170, 77.245.101.134, 92.222.125.16, 93.78.205.196
keitaro	1	69.16.254.181
Kpot	1	5.188.60.52
LokiBot	2	161.117.182.74 , 47.88.102.244
PredatorTheThief	1	89.41.173.142

Name	Number Discovered	Location
TrickBot	36	104.168.123.186, 107.155.137.4, 107.172.143.155, 139.60.163.36, 148.251.27.94, 178.170.189.52, 178.33.26.175, 181.113.20.186, 181.129.96.74, 185.141.27.223, 185.141.27.237, 185.215.148.133, 185.251.38.201, 185.252.144.190, 185.66.14.149, 186.46.88.62, 194.5.250.57, 194.5.250.60, 195.123.238.110, 195.123.238.83, 195.123.247.27, 198.12.71.210, 200.116.199.10, 200.21.51.38, 200.29.106.33, 23.94.24.196, 37.18.30.165, 37.228.117.182, 5.101.51.101, 51.77.202.8, 51.77.254.186, 64.44.51.126, 79.124.49.209, 79.124.49.210, 92.243.92.8, 92.38.171.26



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF71AFA8-95.SBX.TG	4a5078 0ddb3d b16eba b57b0c a42da0 fb	xme64-2141.exe
Win.Trojan.Generic::in10.talos	47b97d e62ae8 b2b927 542aa5 d7f3c8 58	qmreportupload.exe
W32.Generic:Gen.22fz.1201	799b30 f47060 ca05d8 0ece53 866e01 cc	mf2016341595.exe
W32.AgentWDCR:Gen.21gn.1201	e2ea31 5d9a83 e75770 53f52c 974f6a 5a	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin
W32.46B241E3D3-95.SBX.TG	db69ea aea4d4 9703f1 61c81e 6fdd03 6f	xme32-2141-gcc.exe

CVEs For Which Public Exploits Have Been Detected

Title: Microsoft SharePoint Persistent Cross-Site Scripting Vulnerability
Vendor: Microsoft
Description: A cross-site-scripting vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. An authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected SharePoint server. The attacks could allow the attacker to read content that the attacker is not authorized to read, use the victim's identity to take actions on the SharePoint site on behalf of the user, such as change permissions and delete content, and inject malicious content in the browser of the user.
CVSS v2 Base Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

ID: CVE-2019-1579
Title: HPE Intelligent Management Center Information Disclosure Vulnerability
Vendor: HPE
Description: An information disclosure vulnerability exists in HPE Intelligent Management Center due to improper validation of user-supplied data. An unauthenticated, remote attacker can exploit this to allow unauthenticated access.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

ID: CVE-2019-16531
Title: LayerBB Cross-Site Request Forgery Vulnerability
Vendor: LayerBB
Description: LayerBB has multiple Cross site request forgery issues such as editing user profiles and forums. These can be demonstrated by changing the System Settings via admin/general.php.
CVSS v2 Base Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ID: CVE-2019-16399
Title: Western Digital My Book World II NAS Authentication Bypass Vulnerability
Vendor: Western Digital
Description: An Authentication Bypass Vulnerability exists in Western Digital WD My Book World, which allows an attacker to access the /admin/ directory without credentials. An attacker can easily enable SSH from /admin/system_advanced.php?lang=en and login with the default root password welc0me.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Title: Microsoft Windows AppXSvc Elevation of Privilege Vulnerability
Vendor: Microsoft
Description: An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'.
Note: This CVE ID is unique from CVE-2019-1215, CVE-2019-1278, CVE-2019-1303.
CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)