Red Piranha
unified threat management

Threat Intelligence Report

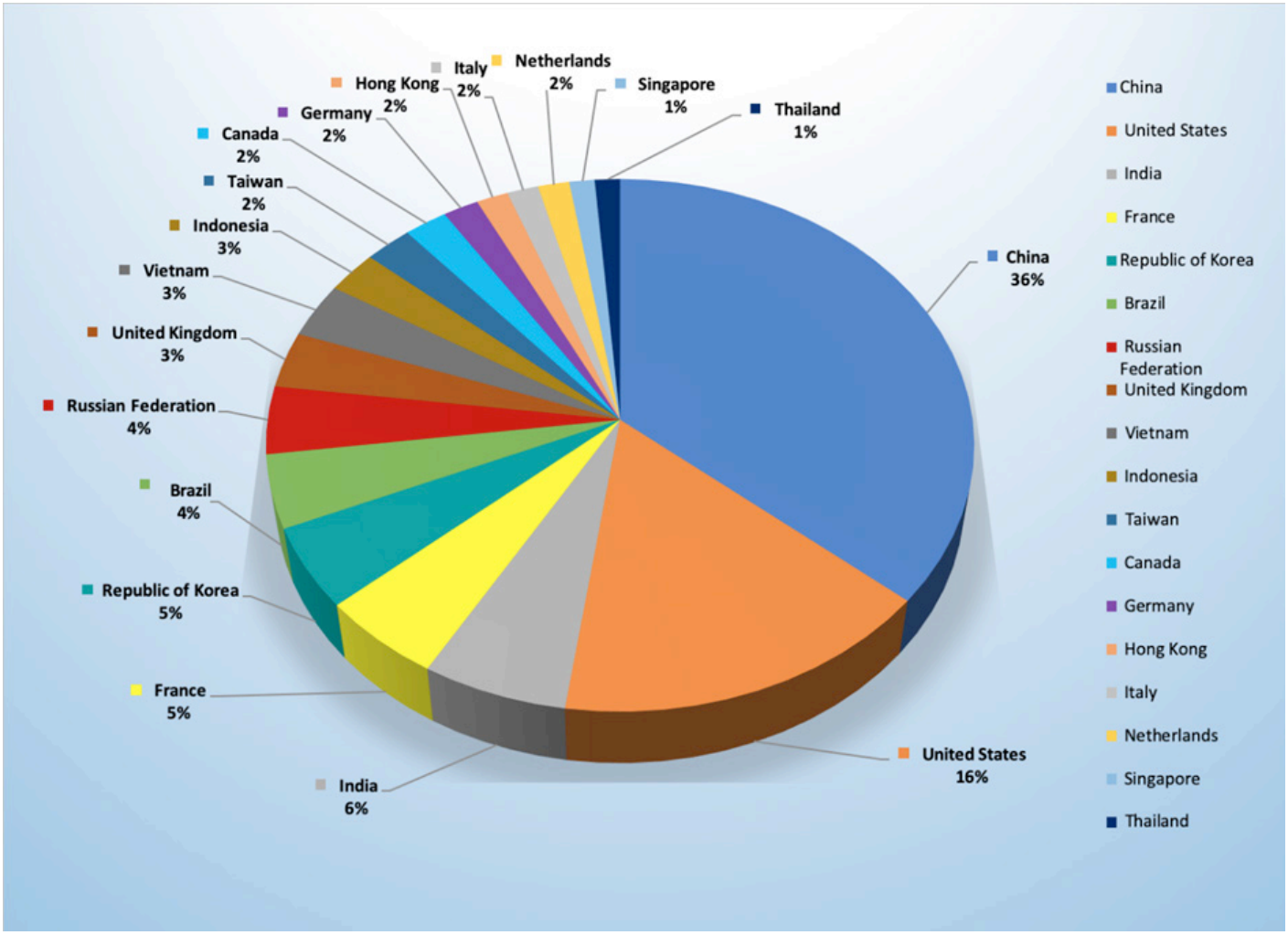
November 11-17 2019

Trends

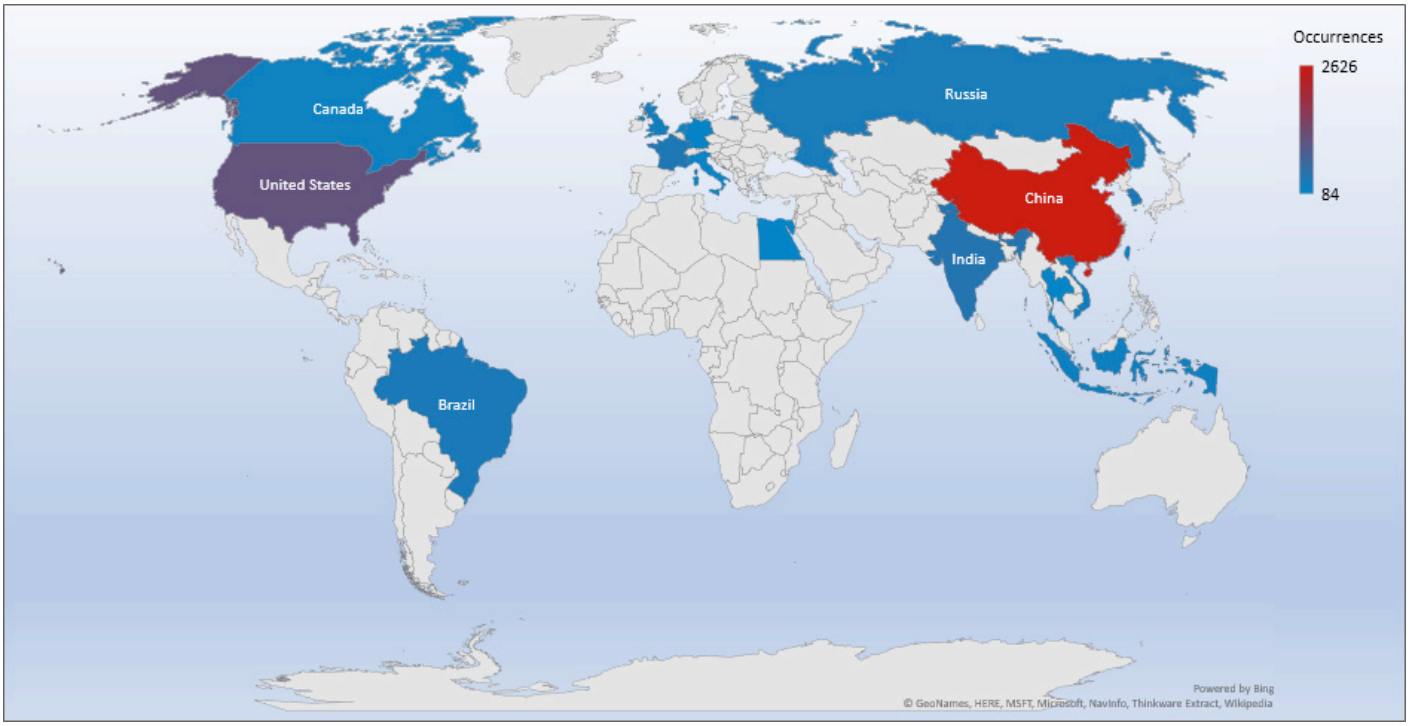
- **The top attacker country was China with 2626 unique attackers (36%).**
- **The top Exploit event was Authentication with 45% of occurrences.**
- **The top Trojan C&C server detected was Anubis with 2 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	2626	35.72%
United States	1172	15.94%
India	443	6.03%
France	378	5.14%
Republic of Korea	358	4.87%
Brazil	323	4.39%
Russian Federation	298	4.05%
United Kingdom	248	3.37%
Vietnam	243	3.31%
Indonesia	188	2.56%
Taiwan	174	2.37%
Canada	158	2.15%
Germany	130	1.77%
Hong Kong	116	1.58%
Italy	114	1.55%
Netherlands	114	1.55%
Singapore	92	1.25%
Thailand	92	1.25%
Egypt	84	1.14%

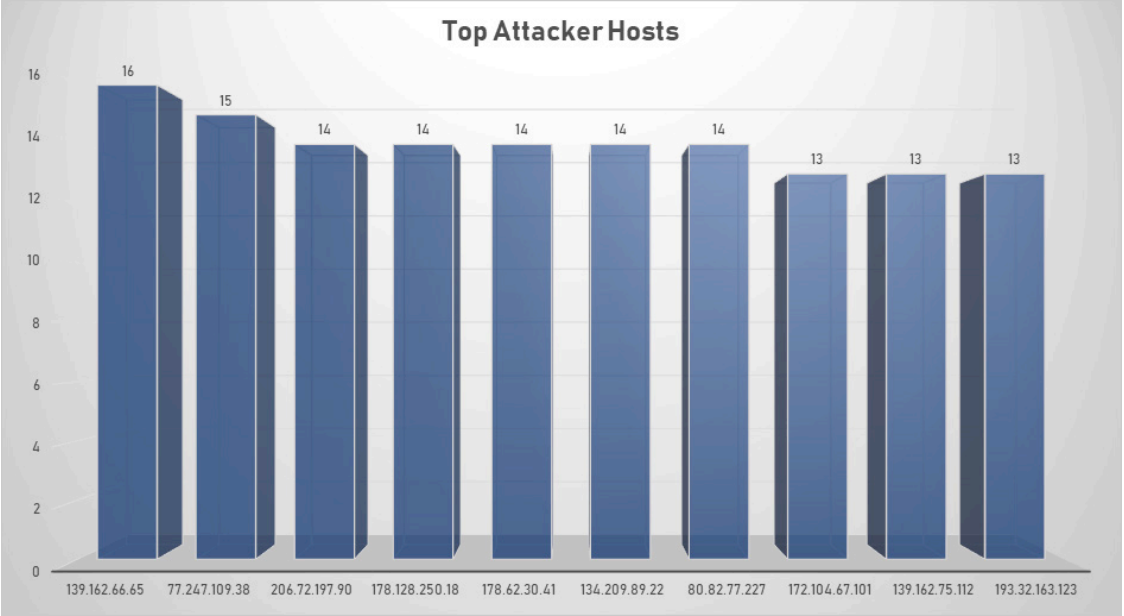


Threat Geo-location



Top Attacking Hosts

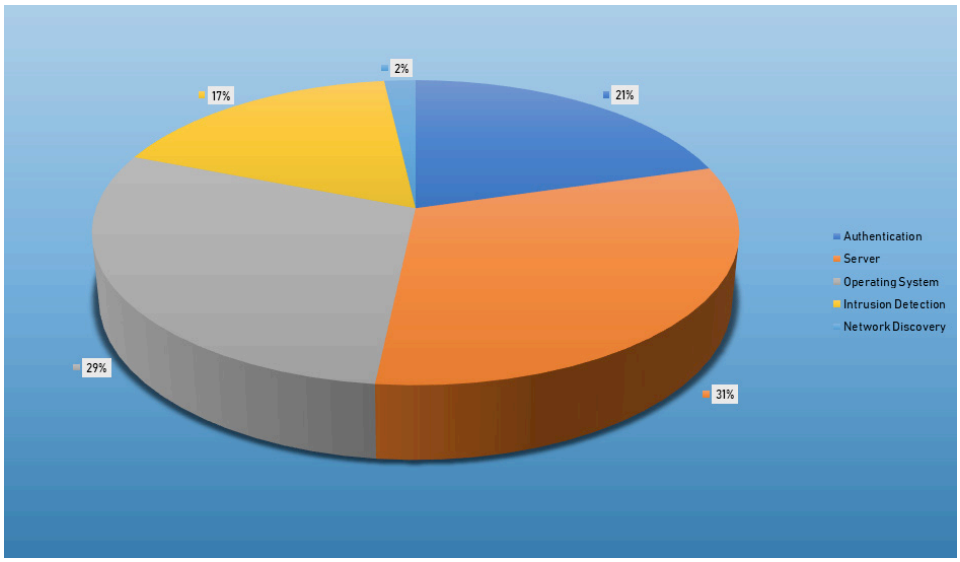
Host	Occurrences
139.162.66.65	16
77.247.109.38	15
206.72.197.90	14
178.128.250.18	14
178.62.30.41	14
134.209.89.22	14
80.82.77.227	14
172.104.67.101	13
139.162.75.112	13
193.32.163.123	3

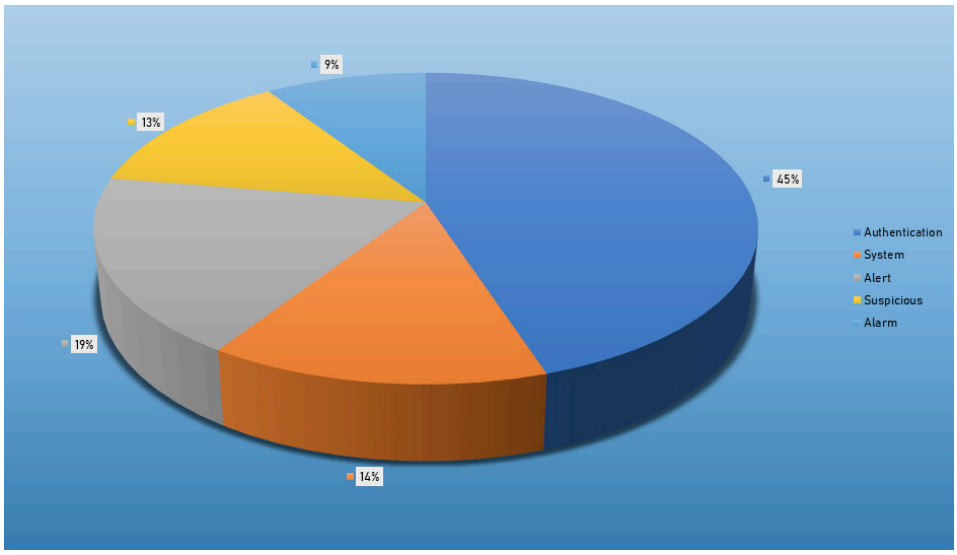


Top Network Attackers

Origin AS	Announcement	Description
AS63949	139.162.64.0/19	Linode LLC
AS209299	77.247.109.0/24	Cloud Star Hosting Services
AS19318	206.72.192.0/20	Interserver Inc
AS14061	178.62.0.0/18	DigitalOcean London
AS202425	80.82.77.0/24	IP Volume inc
AS201912	193.32.163.0/24	PP "Semenyuta Aleksandr Ivanovich

Top Event NIDS and Exploits



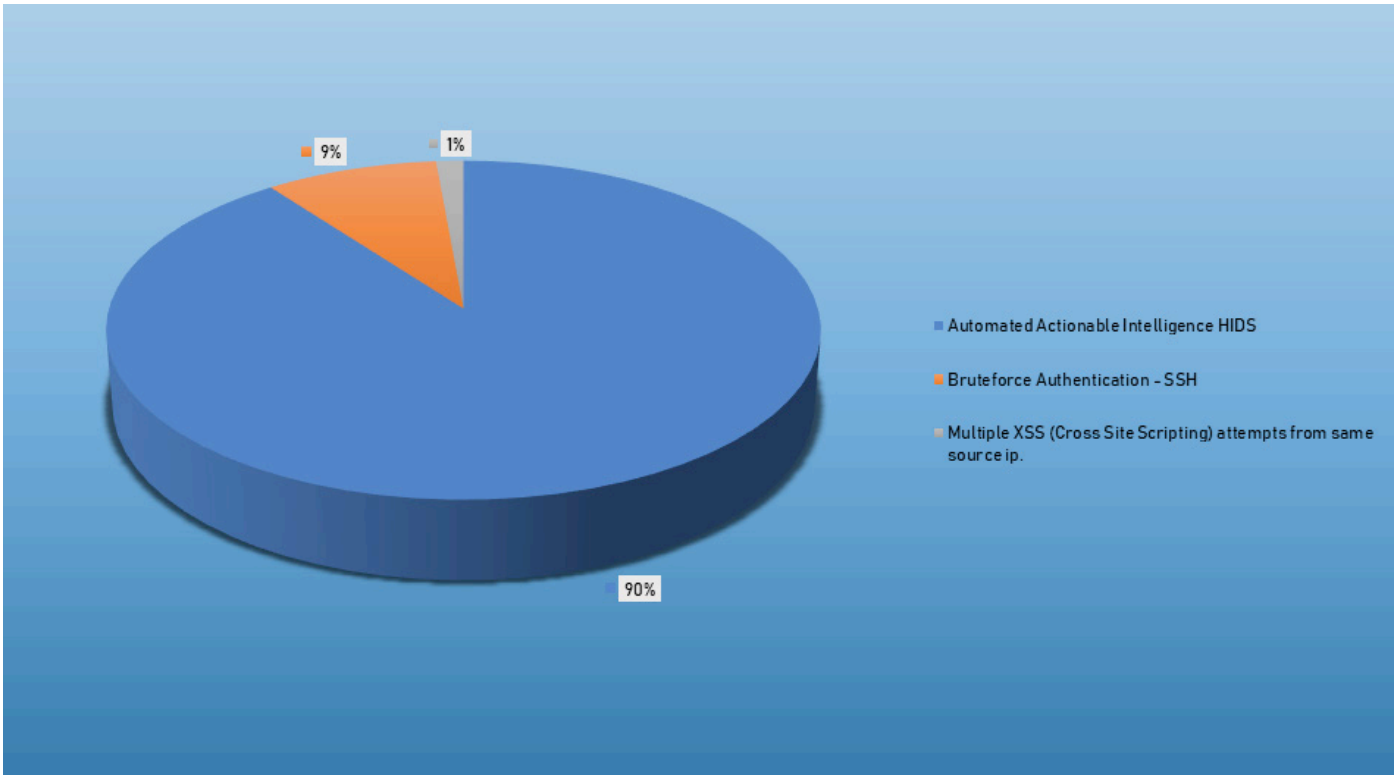


Top Alarms

Type of Alarm	Occurrences
Automated Actionable Intelligence HIDS	193
Bruteforce Authentication - SSH	19
Multiple XSS (Cross Site Scripting) attempts from same source IP	3

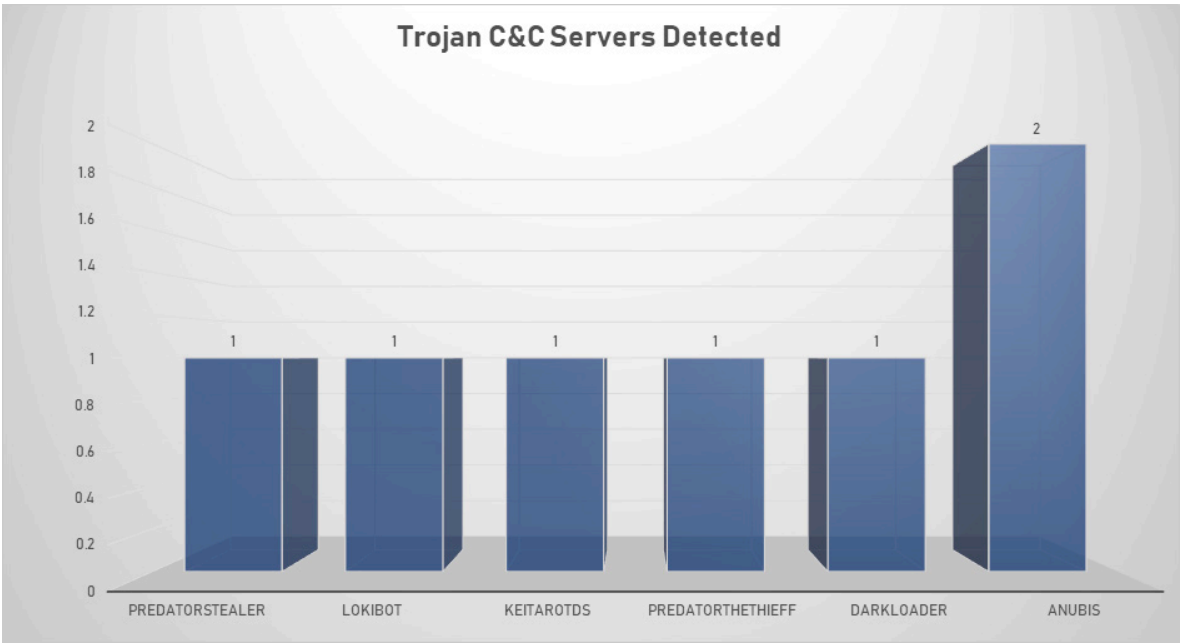
Comparison from last week

Type of Alarm	Occurrences
Bruteforce Authentication	1402
Intrusion Detection	85
Network Discovery	2



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
PredatorStealer	1	185.132.53.138
LokiBot	1	194.67.86.126
KeitaroTDS	1	89.203.198.177
PredatorTheThief	1	45.139.236.64
DarkLoader	1	104.27.174.139
Anubis	2	193.32.161.89, 193.32.161.84



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme64-2141.exe
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload
W32.Generic:Gen.22fz.1201	799b30f47060ca05d80ece53866e01cc	mf2016341595.exe
W32.46B241E3D3-95.SBX.TG	db69eaaea4d49703f161c81e6fdd036f	xme32-2141-gcc.exe
W32.WNCryLdrA:Trojan.22k2.1201	8c80dd97c37525927c1e549cb59bcbf3	eternalblue-2.2.0.exe

CVEs For Which Public Exploits Have Been Detected

CVE-2019-1356
Title: Microsoft Edge based on Edge HTML Information Disclosure Vulnerability
Vendor: Microsoft
Description: An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the user's system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability.
CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVE-2019-1322
Title: Microsoft Windows Elevation of Privilege Vulnerability
Vendor: Microsoft
Description: An elevation of privilege vulnerability exists when Windows improperly handles authentication requests. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could exploit this vulnerability by running a specially crafted application on the victim system.
CVSS v2 Base Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVE-2019-16253
Title: Samsung Mobile Android Samsung TTS Privilege Escalation
Vendor: Samsung
Description: The Samsung Text-to-speech Engine System Component on Android suffers from a local privilege escalation vulnerability. The Text-to-speech Engine application for Android allows a local attacker to escalate privileges, e.g., to system privileges. A successful local attack can obtain system privilege on vulnerable phones.
CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVE-2019-2215
Title: Linux Kernel Use-After-Free Vulnerability
Vendor: Multi-Vendor
Description: A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.
CVSS v2 Base Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVE-2019-3568
Title: WhatsApp VOIP stack buffer overflow vulnerability
Vendor: WhatsApp
Description: A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. Attackers can exploit this issue to execute arbitrary code within the context of the affected application. Failed exploits will result in denial of service condition.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE-2019-16759
Title: vBulletin Remote Code Execution Vulnerability
Vendor: vBulletin
Description: vBulletin allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request. The vulnerability was disclosed through an 18-line exploit that was published on Monday by an unidentified person. The exploit allows unauthenticated attackers to remotely execute malicious code on just about any vBulletin server.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)