Red Piranha
unified threat management

Threat Intelligence Report

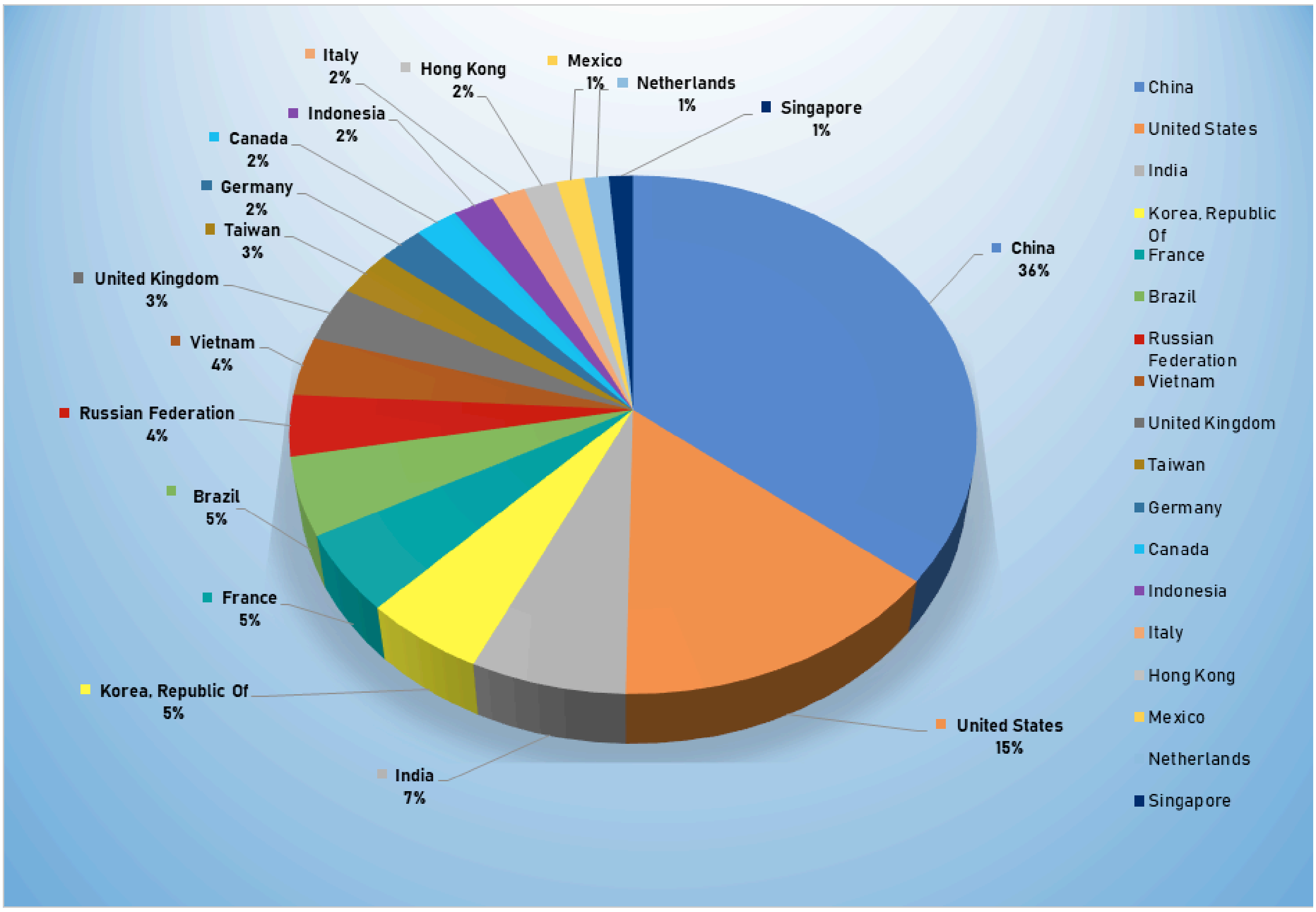
November 18-24 2019

Trends

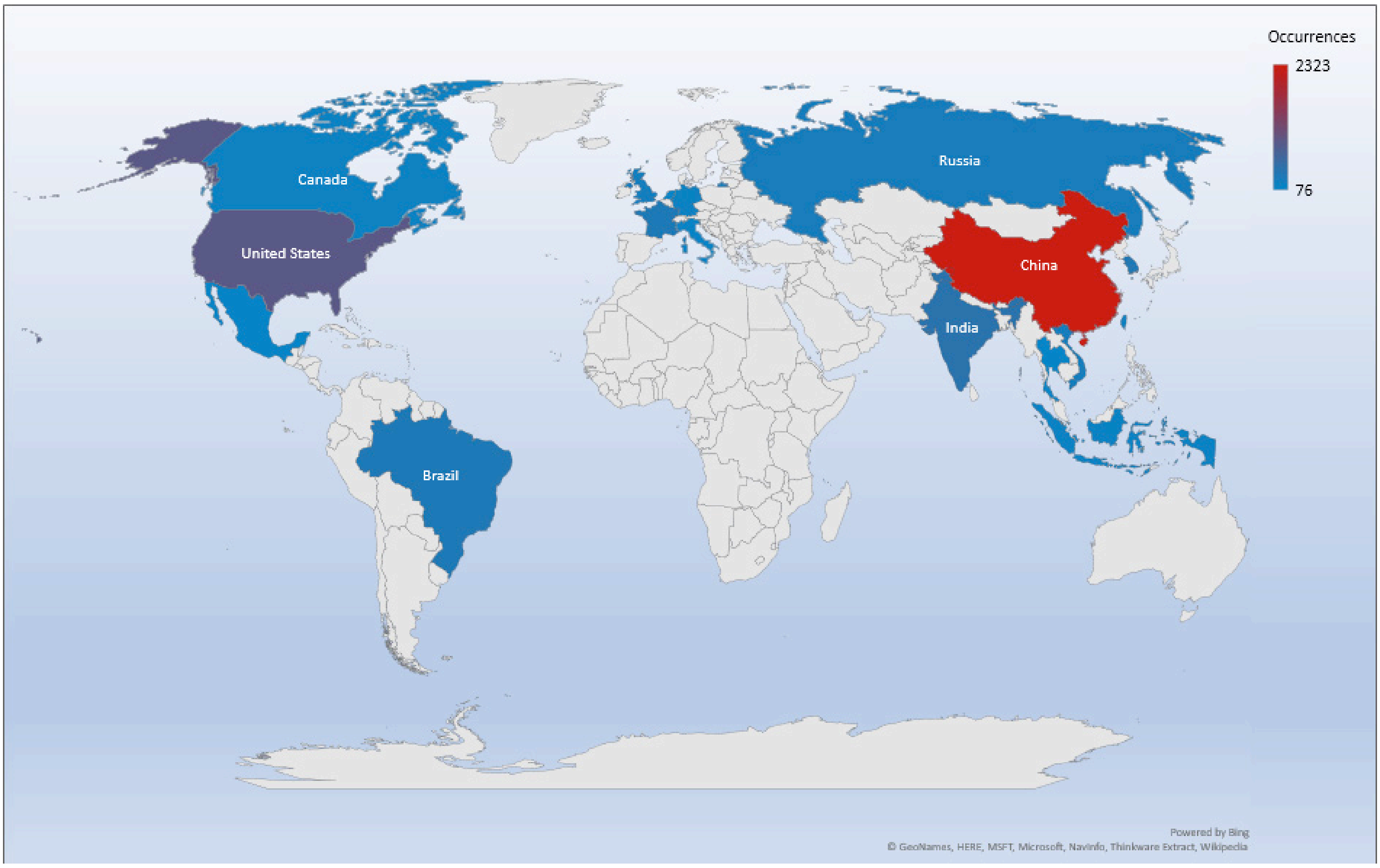
- **The top attacker country was China with 2323 unique attackers (35%).**
- **The top Exploit event was Authentication with 39% of occurrences.**
- **The top Trojan C&C server detected was TrickBot with 30 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	2323	35.38%
United States	941	14.33%
India	435	6.63%
Republic of Korea	340	5.18%
France	323	4.92%
Brazil	318	4.84%
Russian Federation	248	3.78%
Vietnam	239	3.64%
United Kingdom	222	3.38%
Taiwan	185	2.82%
Germany	152	2.32%
Canada	146	2.22%
Indonesia	139	2.12%
Italy	113	1.76%
Hong Kong	110	1.68%
Mexico	93	1.42%
Netherlands	81	1.23%
Singapore	81	1.23%
Thailand	76	1.16%

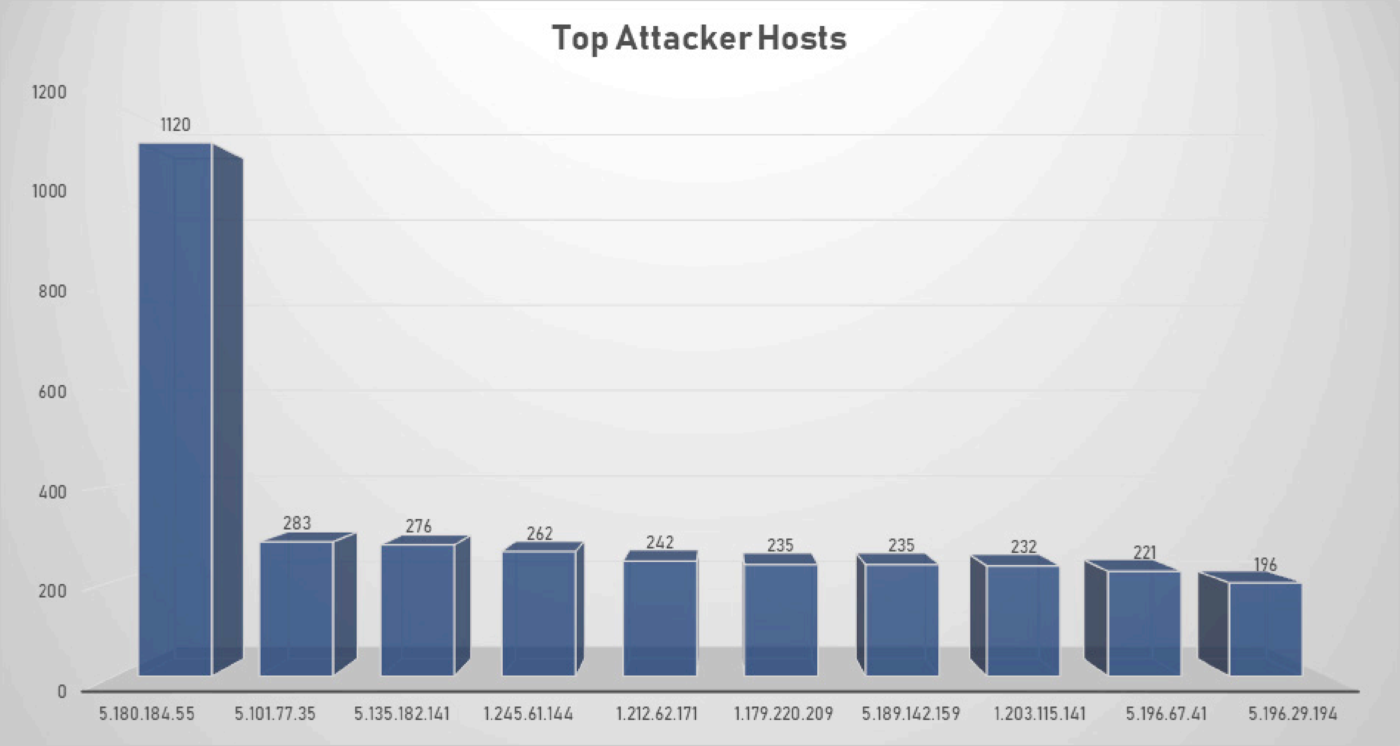


Threat Geo-location



Top Attacking Hosts

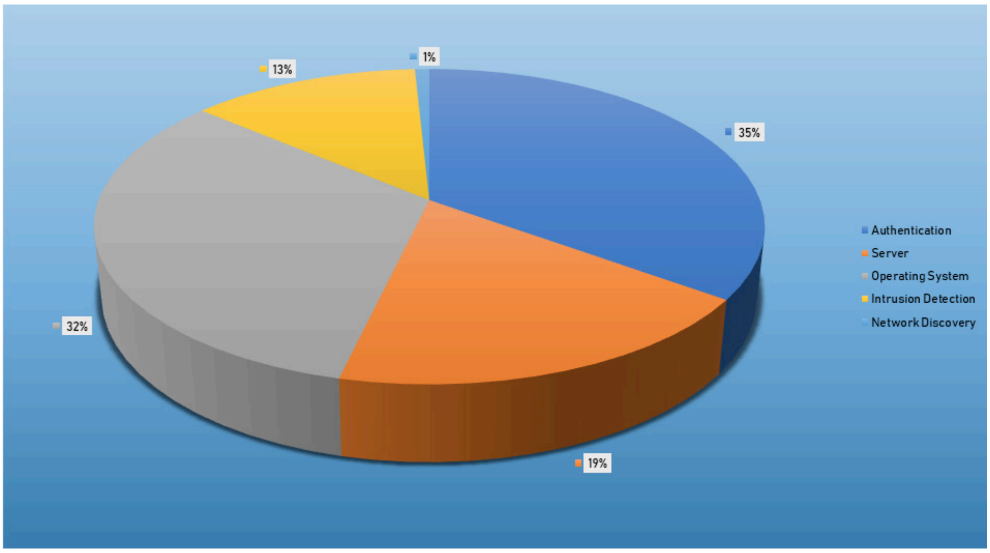
Host	Occurrences
5.180.184.55	1120
5.101.77.35	283
5.135.182.141	276
1.245.61.144	262
1.212.62.171	242
1.179.220.209	235
5.189.142.159	235
1.203.115.141	232
5.196.67.41	221
5.196.29.194	196

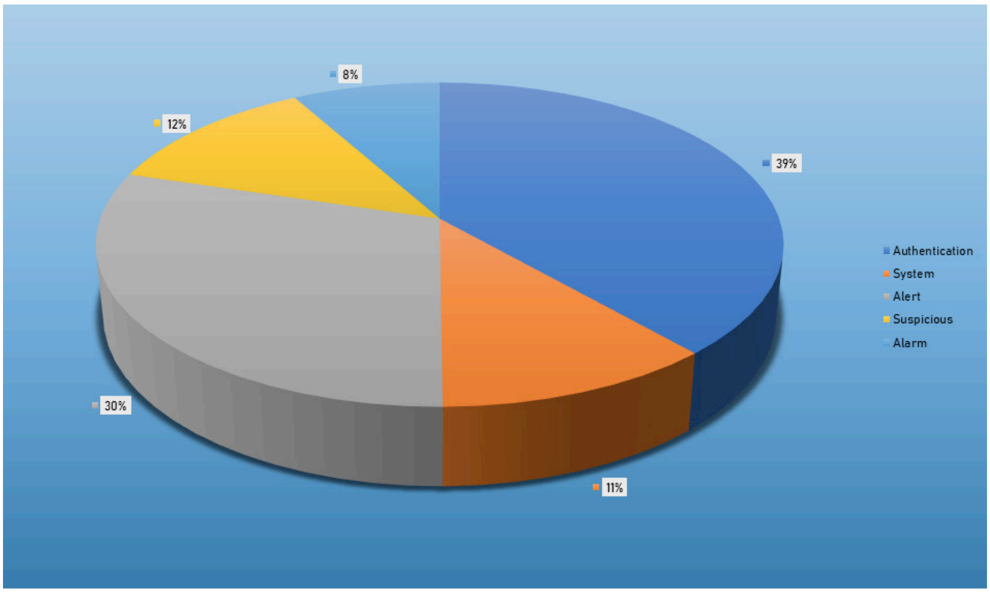


Top Network Attackers

Origin AS	Announcement	Description
AS51559	5.180.184.0/24	UMIT HAN
AS48096	5.101.77.0/24	Enterprise Cloud Ltd.
AS16276	5.135.0.0/16	OVH SAS

Top Event NIDS and Exploits



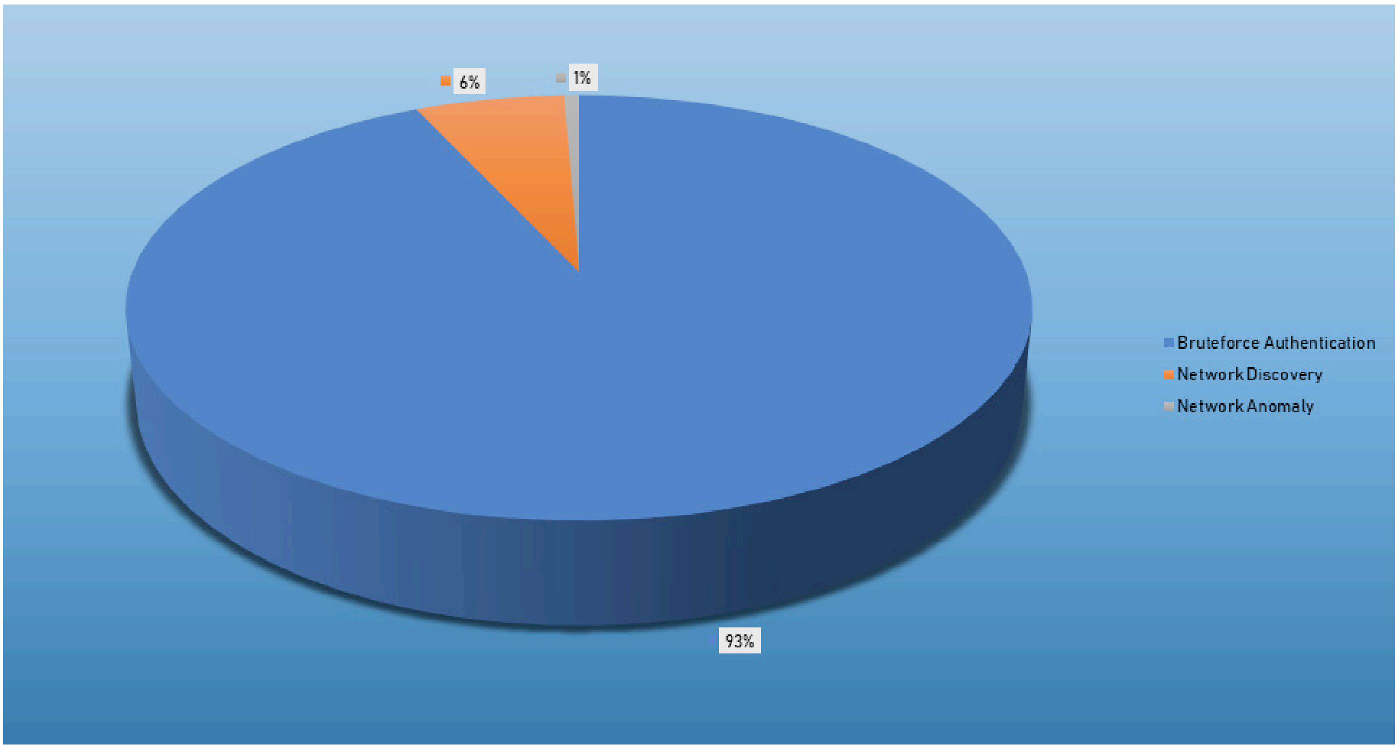


Top Alarms

Type of Alarm	Occurrences
Bruteforce Authentication	4048
Network Discovery	273
Network Anomaly	27

Comparison from last week

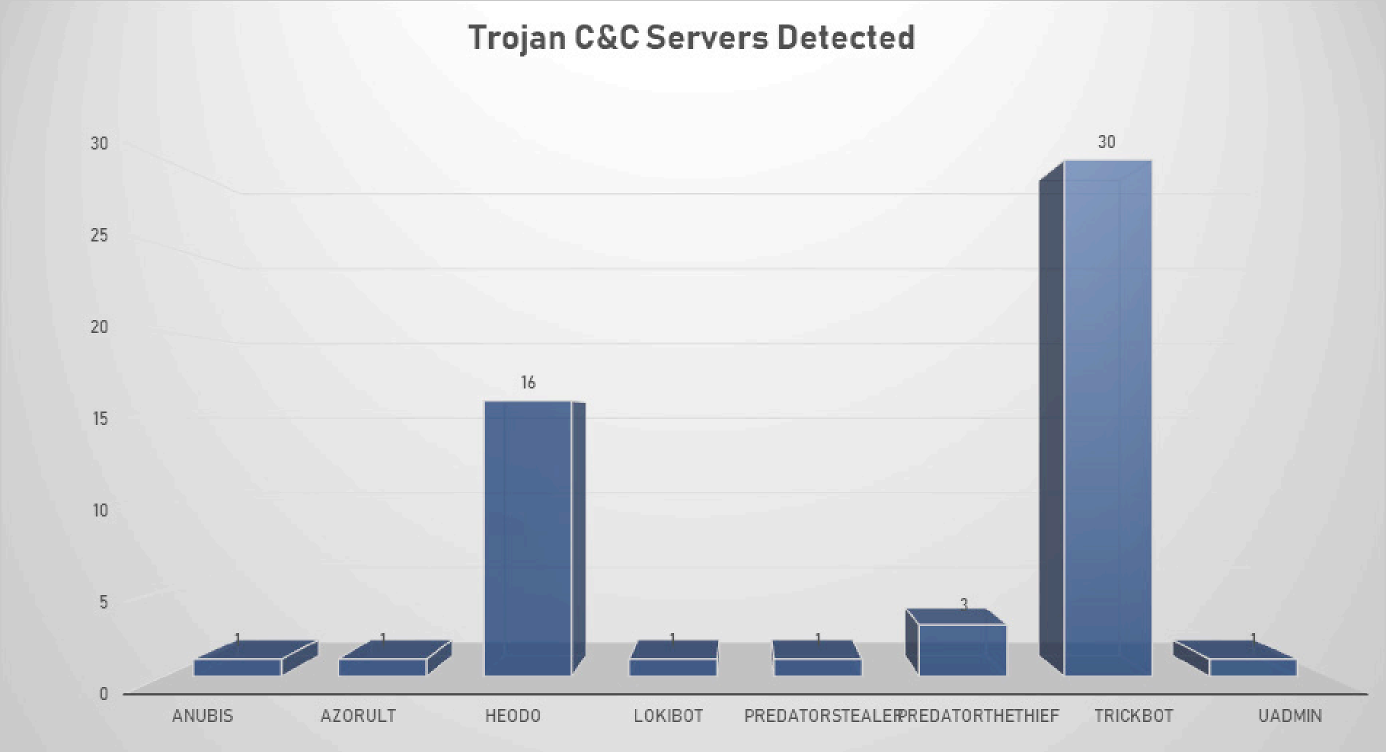
Type of Alarm	Occurrences
Automated Actionable Intelligence HIDS	193
Bruteforce Authentication - SSH	19
Multiple XSS (Cross Site Scripting) attempts from same source IP	3



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	1	188.120.254.18
AZORult	1	104.168.65.2
Heodo	16	107.170.24.125, 139.162.75.91, 149.202.197.94, 164.132.75.130, 172.104.233.225, 181.91.215.151, 182.48.194.6, 189.252.3.161, 190.147.215.53, 190.189.79.73, 198.58.120.26, 209.97.168.52, 217.26.163.82, 222.239.249.166, 50.116.86.205, 90.77.228.193
Lokibot	1	45.143.138.40
PredatorStealer	1	185.132.53.138
PredatorTheThief	3	188.225.85.87, 45.143.138.39, 47.254.232.105

Name	Number Discovered	Location
TrickBot	30	103.196.211.212, 107.172.39.48, 108.170.52.149, 117.196.233.79, 146.185.253.170, 164.68.96.155, 185.203.243.138, 185.222.202.183, 185.99.2.169, 185.99.2.242, 185.99.2.245, 192.3.104.48, 192.3.247.106, 192.3.73.164, 195.123.220.184, 195.123.220.193, 212.73.150.127, 212.73.150.233, 212.80.218.237, 23.94.3.13, 5.182.211.61, 51.89.115.100, 51.89.115.113, 5.2.76.193, 81.177.180.252, 85.217.171.229, 89.32.41.104, 91.92.136.82, 93.189.42.182, 94.103.82.99
Uadmin	1	45.141.86.9
Anubis	1	188.120.254.18



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme64-2141.exe
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload
W32.GenericKD:Attribute.22lk.1201	74f4e22e5be90d152521125eaf4da635	jsonMerge.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-2019-17671
Title: WordPress Core Stored Cross-Site Scripting (XSS) vulnerability
Vendor: Wordpress

Description: A stored Cross-Site Scripting vulnerability within the WordPress Customizer that allows authenticated users to make changes to the WordPress theme to directly customize the interface. This vulnerability could allow unauthenticated users to view private or draft posts, which otherwise would not be viewable.

CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE-2019-10098
Title: Apache Httpd mod_rewrite Open Redirects Vulnerability
Vendor: Multi-Vendor

Description: In Apache HTTP server, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

CVSS v2 Base Score: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVE-2019-10092
Title: Apache Httpd mod_proxy - Error Page Cross-Site Scripting Vulnerability
Vendor: Multi-Vendor

Description: In Apache HTTP Server, a limited cross site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

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

CVE-2019-1821
Title: Cisco Prime Infrastructure Health Monitor HA TarArchive - Directory Traversal / Remote Code Execution
Vendor: Cisco

Description: A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated remote attacker to execute code with root-level privileges on the underlying operating system. This vulnerability exist because the software improperly validates user-supplied input. An attacker could exploit this vulnerability by uploading a malicious file to the administrative web interface. A successful exploit could allow the attacker to execute code with root level privileges on the underlying operating system.

CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE-2019-1322
Title: Microsoft Windows 'COMahawk' Local Privilege Escalation Vulnerability
Vendor: Microsoft

Description: An elevation of privilege vulnerability exists when Windows improperly handles authentication requests. An attacker could exploit this vulnerability by running a specially crafted application on the victim system. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.

CVSS v2 Base Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVE-2019-11932
Title: nipper-ng Remote Stack Buffer Overflow Vulnerability
Vendor: nipper-ng project

Description: A stack based buffer overflow in the processPrivilage() function in IOS/process-general.c in allows remote attackers (serving firewall configuration files) to achieve Remote Code Execution or Denial Of Service via a crafted file.

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