Red Piranha
unified threat management

Threat Intelligence Report

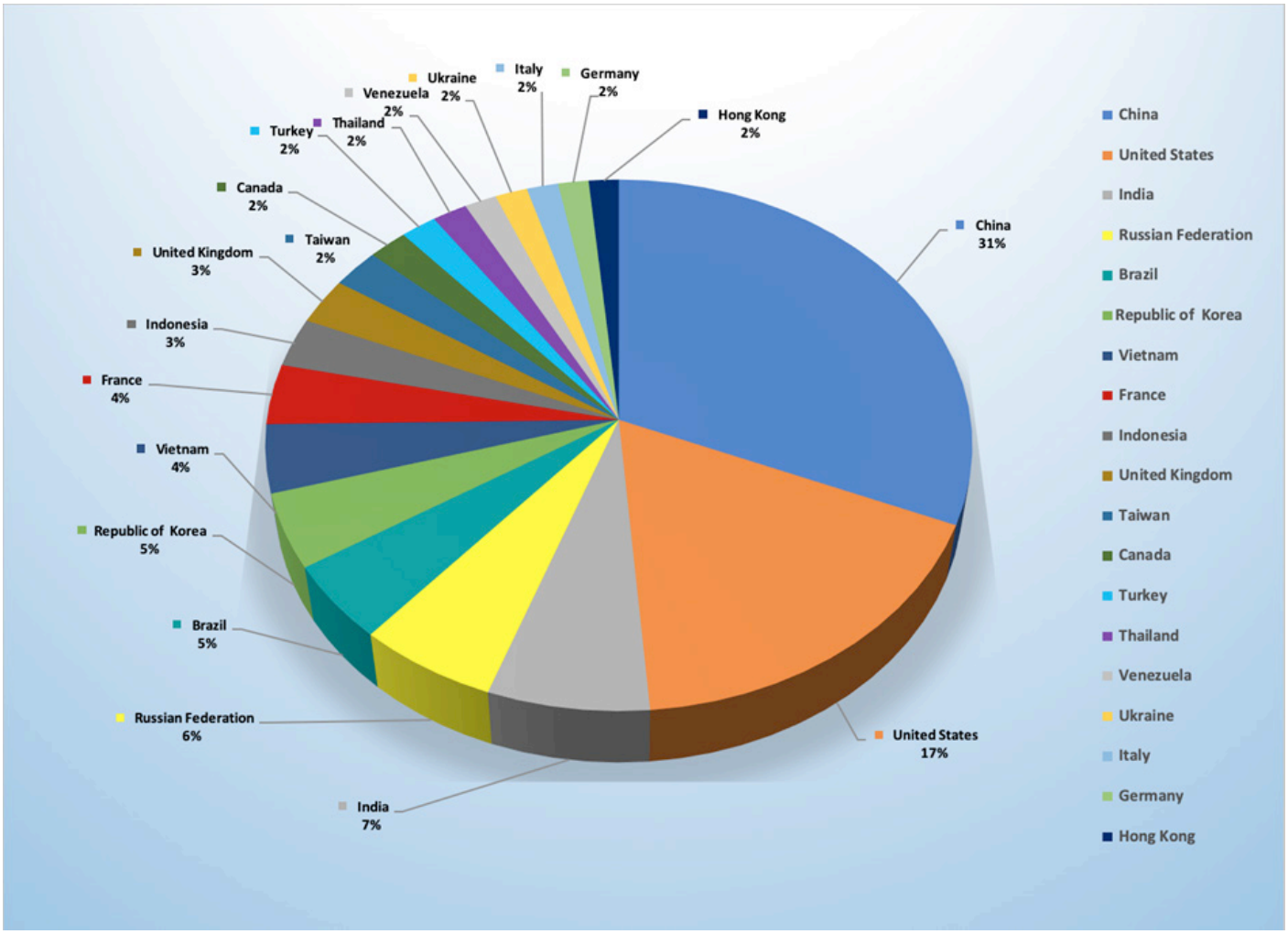
October 14-20, 2019

Trends

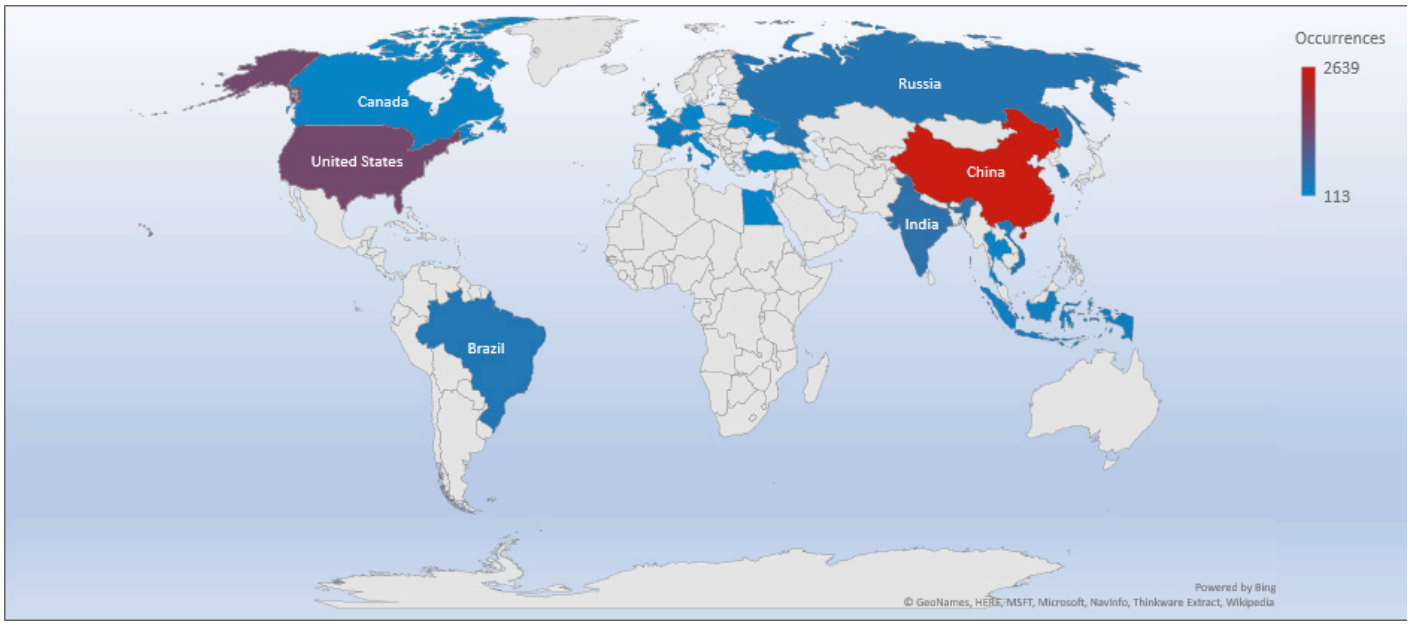
- **The top attacker country was China with 3102 unique attackers (31.30%)**
- **The top Exploit event was Application with 39% of occurrences.**
- **The top Trojan C&C server detected was Trickbot with 36 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	3102	31.30%
United States	1725	17.41%
India	672	6.78%
Russian Federation	580	5.85%
Brazil	467	4.71%
Korea	449	4.53%
Vietnam	411	4.15%
France	363	3.66%
Indonesia	297	3.00%
United Kingdom	280	2.83%
Taiwan	237	2.39%
Canada	196	1.98%
Turkey	179	1.81%
Thailand	174	1.76%
Venezuela	160	1.61%
Ukraine	160	1.61%
Italy	157	1.58%
Germany	151	1.52%
Hong Kong	149	1.50%

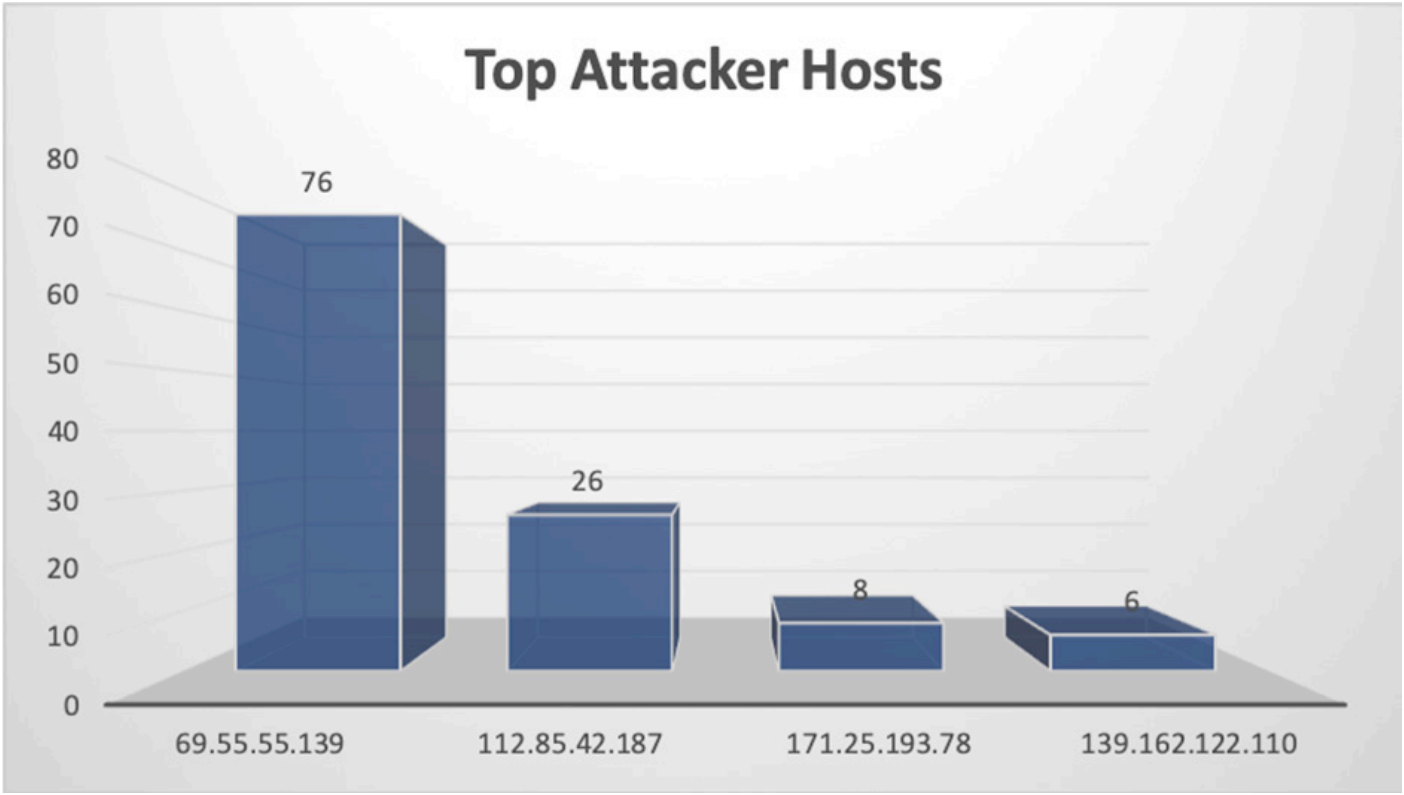


Threat Geo-location



Top Attacking Hosts

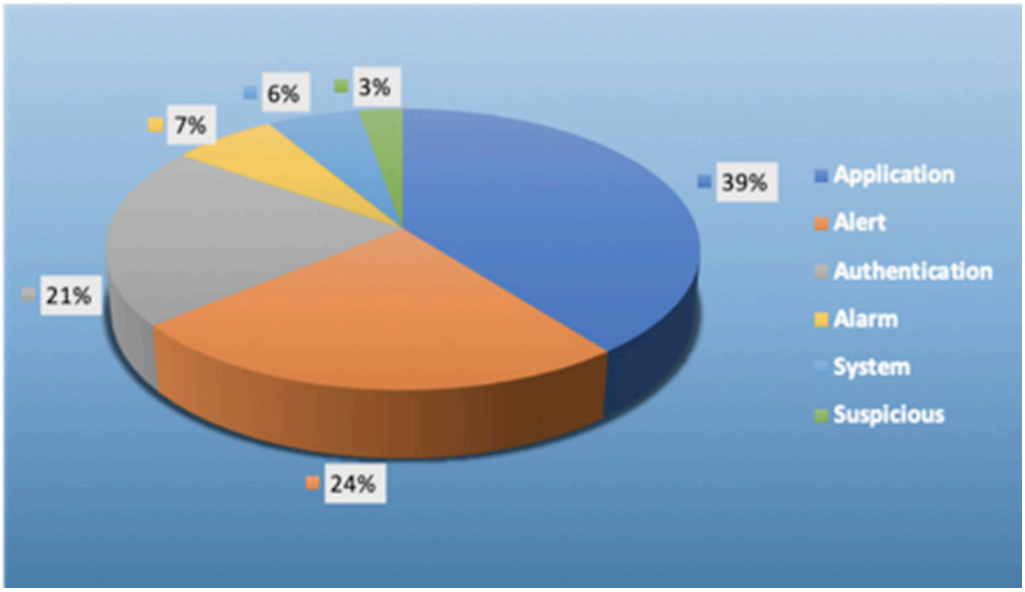
Host	Occurrences
69.55.55.139	76
112.85.42.187	26
171.25.193.78	8
139.162.122.110	6

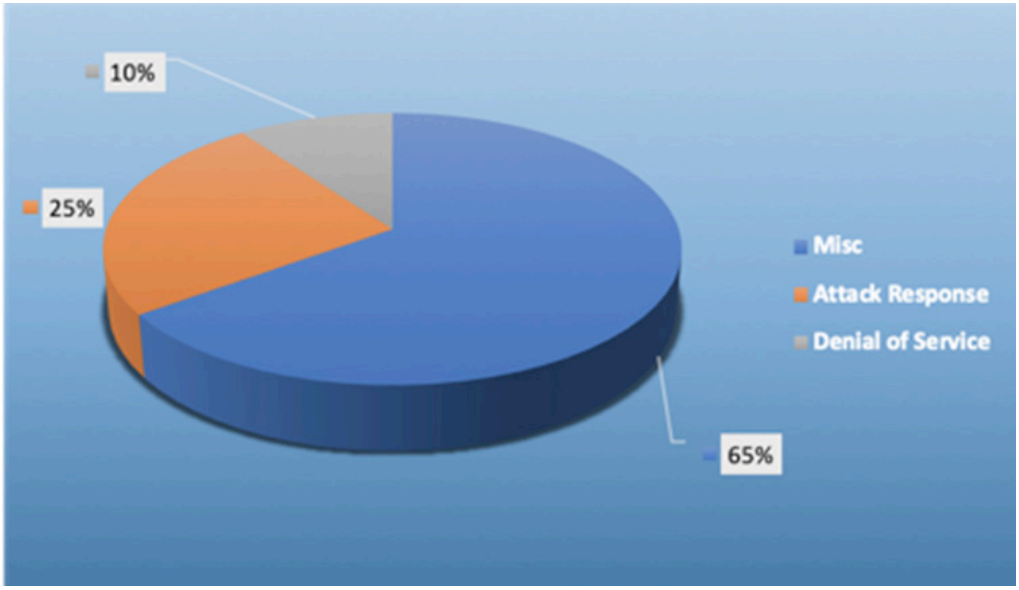


Top Network Attackers

Origin AS	Announcement	Description
AS14061	69.55.54.0/23	ServerStack Inc.
AS4837	112.80.0.0/13	China Unicom Jiangsu Province Network
AS198093	171.25.193.0/24	Foreningen for digitala fri- och rattigheter
AS63949	139.162.96.0/19	Linode, LLC

Top Event NIDS and Exploits



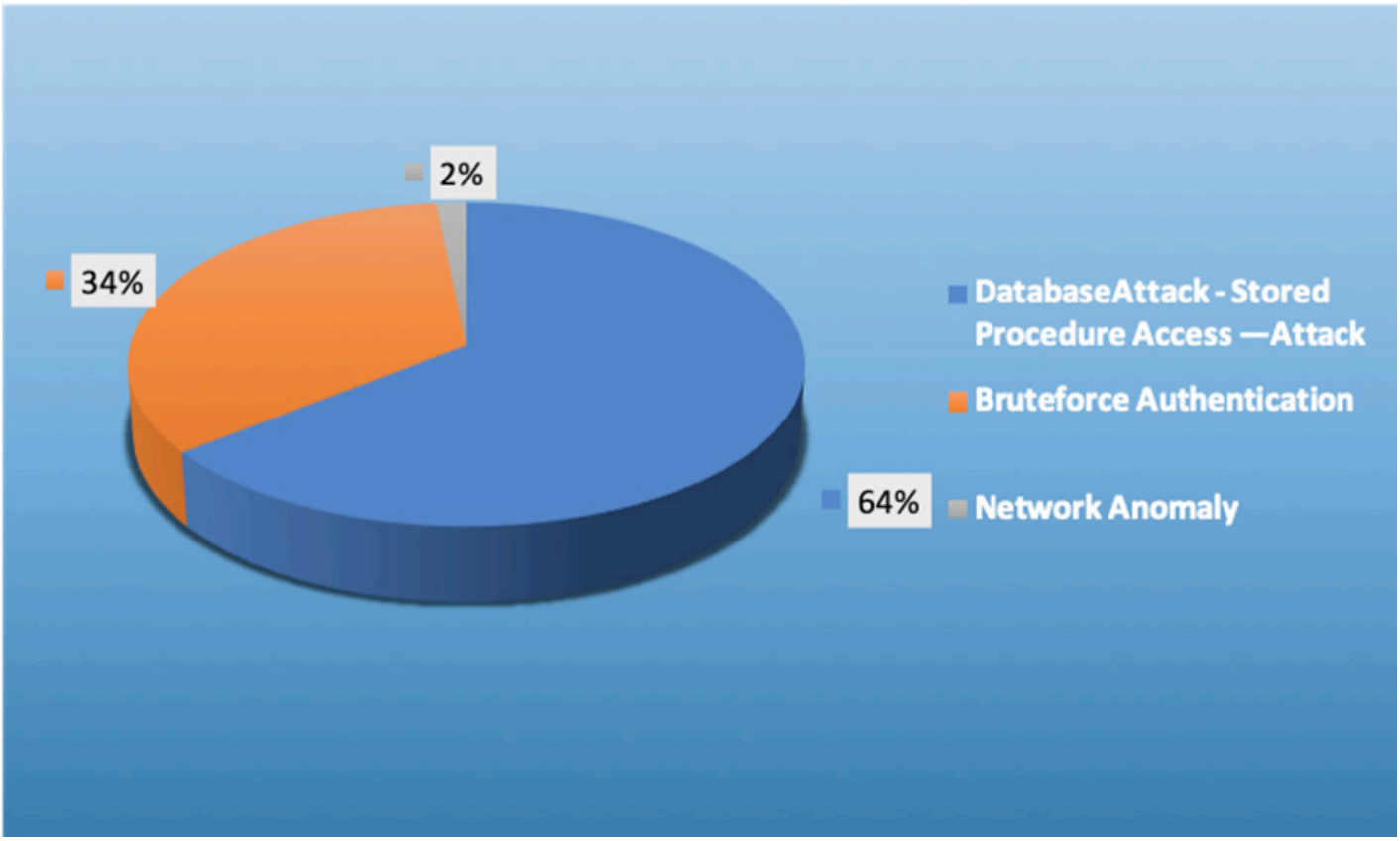


Top Alarms

Type of Alarm	Occurrences
DatabaseAttack - Stored Procedure Access —Attack	81
Bruteforce Authentication	43
Network Anomaly	2

Comparison from last week

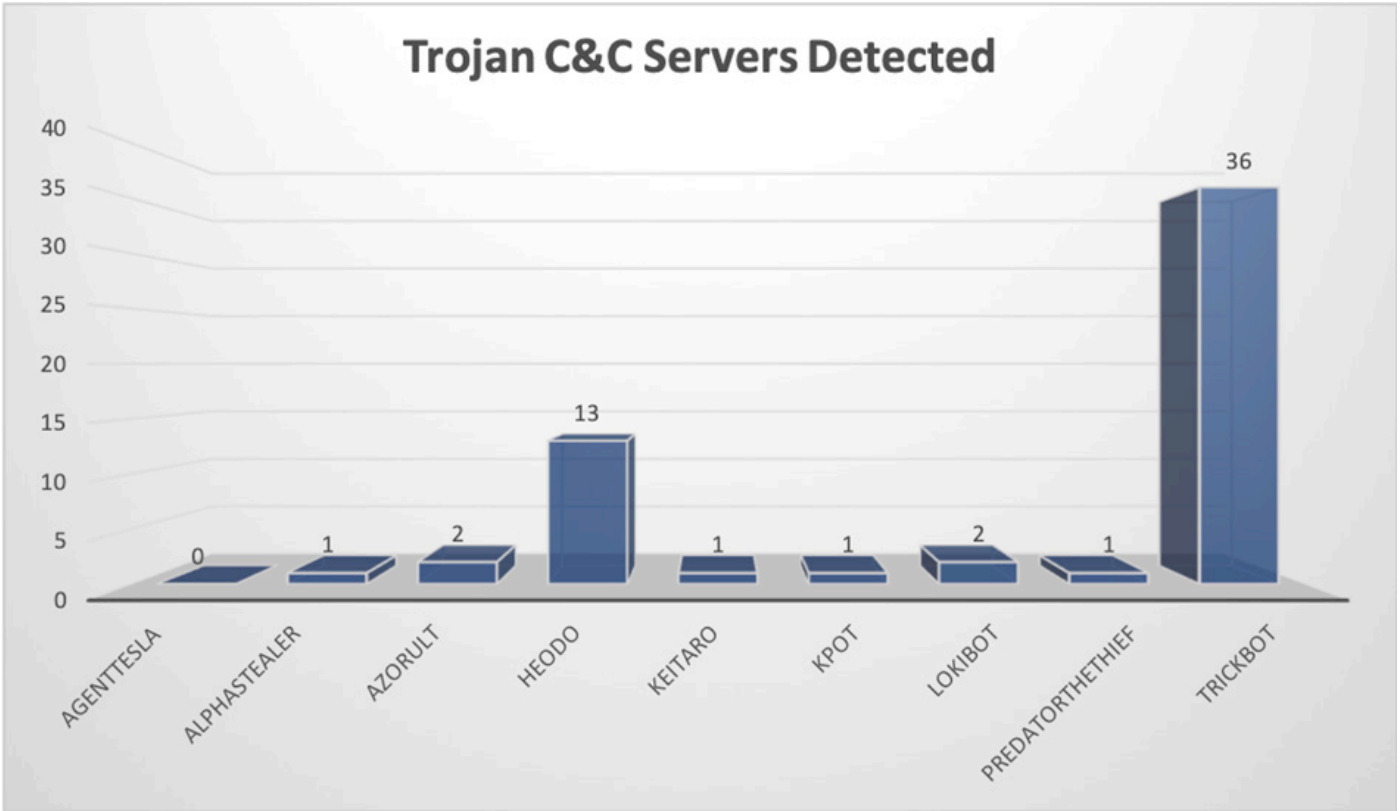
Type of Alarm	Occurrences
Bruteforce Authentication	808687
Intrusion Detection	33223
Network Anomaly	1721987



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.WNCryLdrA:Trojan.22k2.1201	8c80dd97c37525927c1e549cb59bcbf3	Eternalblue-2.2.0.exe
W32.7ACF71AFA8-95.SBX.TG	4a5078 0ddb3d b16eba b57b0c a42da0 fb	xme64-2141.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

ID: CVE-2019-1346
Title: Microsoft Windows Denial of Service Vulnerability
Vendor: Microsoft
Description: The Microsoft Windows kernel suffers from an out-of-bounds read vulnerability in CI!HashKComputeFirstPageHash while parsing a malformed PE file. An attacker who successfully exploited the vulnerability could cause a target system to stop responding.
Note: This CVE ID is unique from CVE-2019-1343, CVE-2019-1347.

CVSS v2 Base Score: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

ID: CVE-2019-1343
Title: Microsoft Windows Denial of Service Vulnerability
Vendor: Microsoft

Description: The Microsoft Windows kernel suffers from a null pointer dereference vulnerability in nt!MiOffsetToProtos while parsing a malformed PE file. A denial of service vulnerability exists when Windows improperly handles objects in memory.
Note: This CVE ID is unique from CVE-2019-1346, CVE-2019-1347.

CVSS v2 Base Score: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

ID: CVE-2019-17503, CVE-2019-17504
Title: Kirona-DRS Information Disclosure Vulnerability
Vendor: Kirona

Description: An information disclosure vulnerability exists in Kirona Dynamic Resource Scheduling (DRS). An unauthenticated user can access /osm/REGISTER.cmd (aka /osm_tiles/REGISTER.cmd) directly that contains sensitive information about the database through the SQL queries within this batch file. This file exposes SQL database information such as database version, table name, column name, etc.

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

ID: CVE-2019-11932
Title: Whatsapp Remote Code Execution Vulnerability
Vendor: Whatsapp

Description: A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif, as used in WhatsApp for Android, allows remote attackers to execute arbitrary code or cause a denial of service.

CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-11932
Title: sudo Security Bypass Vulnerability
Vendor: Multi-Vendor

Description: When sudo is configured to allow a user to run commands as an arbitrary user via the ALL keyword in a Runas specification, it is possible to run commands as root by specifying the user ID -1 or 4294967295. This can be used by a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access as long as the ALL keyword is listed first in the Runas specification.

CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)