Red Piranha
unified threat management

Threat Intelligence Report

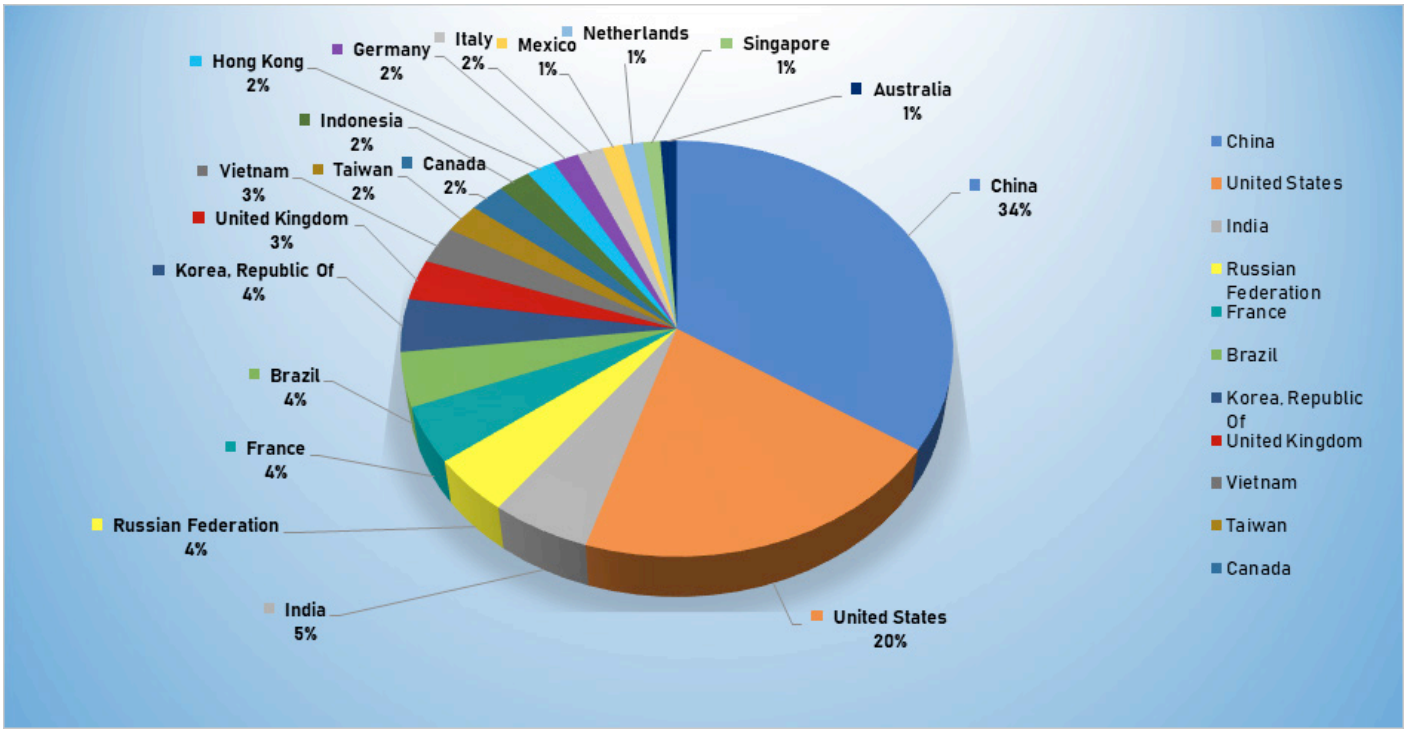
October 28 - November 3 2019

Trends

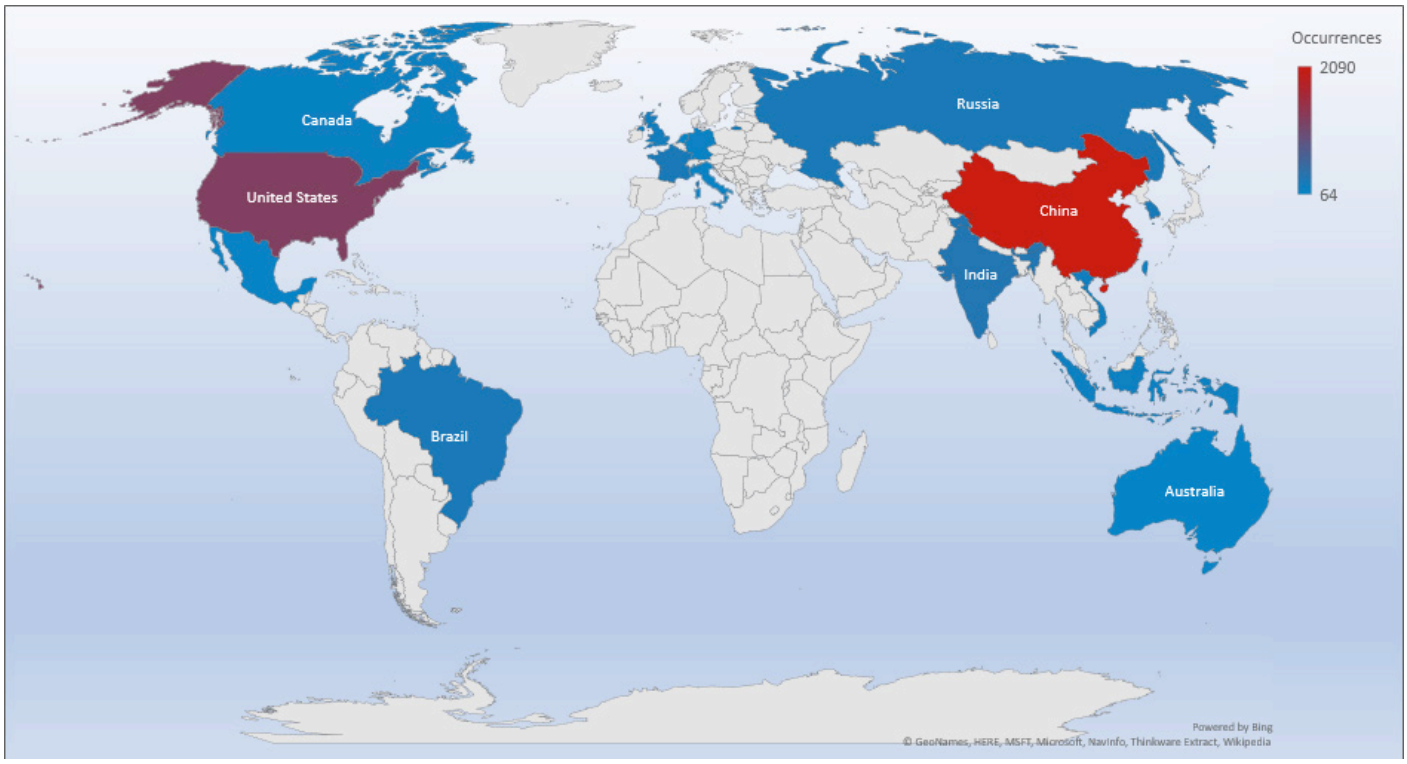
- **The top attacker country was China with 2090 unique attackers (34%).**
- **The top Exploit event was Authentication with 50% of occurrences.**
- **The top Trojan C&C server detected was Trickbot with 65 instances detected.**
- **The most prevalent malware detected was Bitcoin Miner xme64-2141.exe, first seen 10th March 2019.**

Top Attacker by Country

Country	Occurrences	Percentage
China	2090	34.41%
United States	1242	20.45%
India	325	5.35%
Russian Federation	268	4.41%
France	265	4.36%
Brazil	256	4.22%
Korea	250	4.12%
United Kingdom	192	3.16%
Vietnam	177	2.91%
Taiwan	140	2.31%
Canada	137	2.26%
Indonesia	128	2.11%
Hong Kong	112	1.84%
Germany	101	1.66%
Italy	100	1.65%
Mexico	80	1.32%
Netherlands	79	1.30%
Singapore	67	1.10%
Australia	64	1.05%

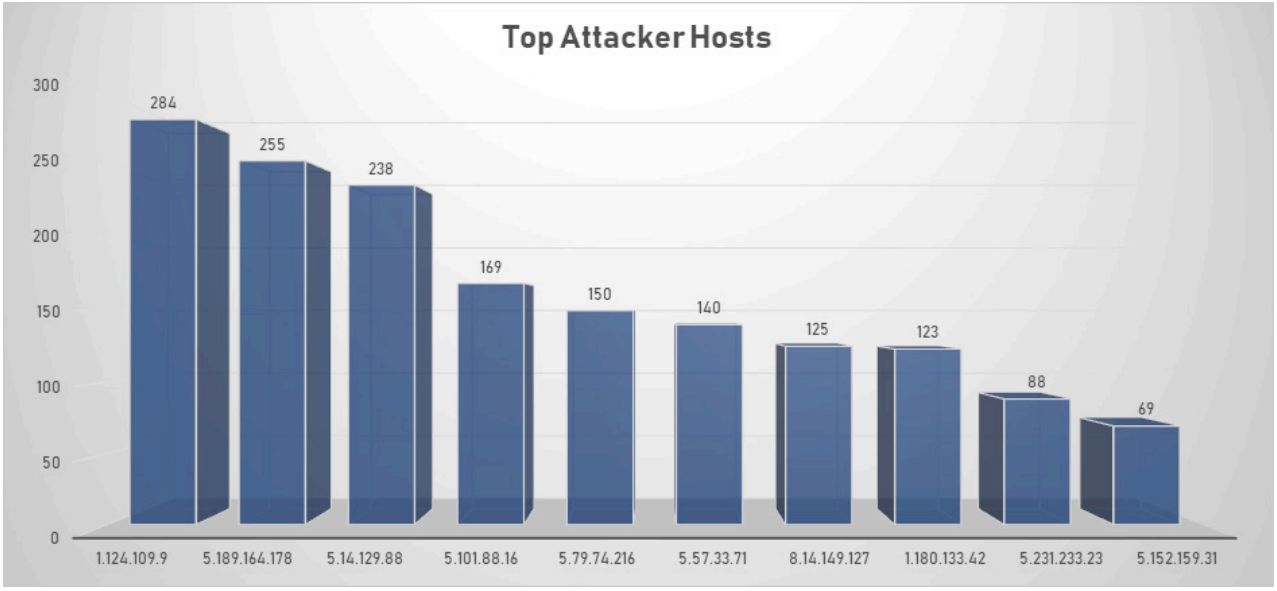


Threat Geo-location



Top Attacking Hosts

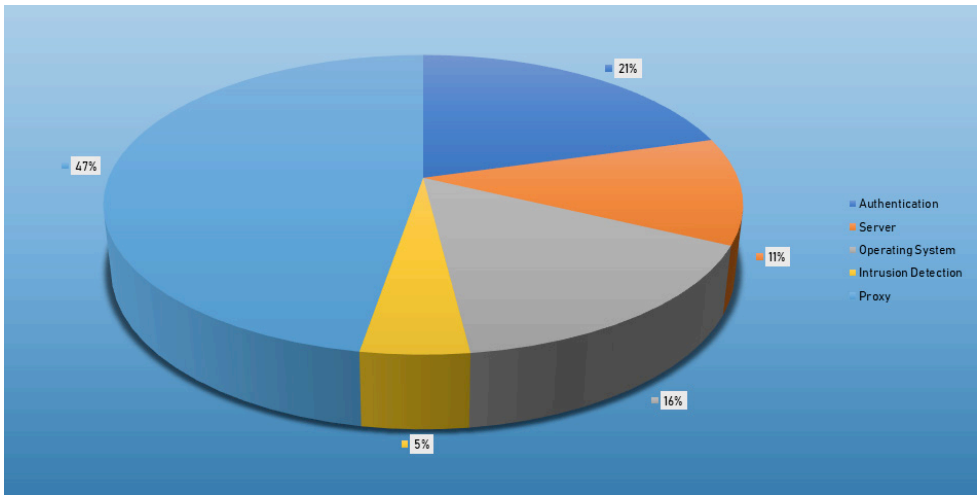
Host	Occurrences
1.124.109.9	284
5.189.164.178	255
5.14.129.88	238
5.101.88.16	169
5.79.74.216	150
5.57.33.71	140
8.14.149.127	125
1.180.133.42	123
5.231.233.23	88
5.152.159.31	69
1.124.109.9	284
5.189.164.178	255

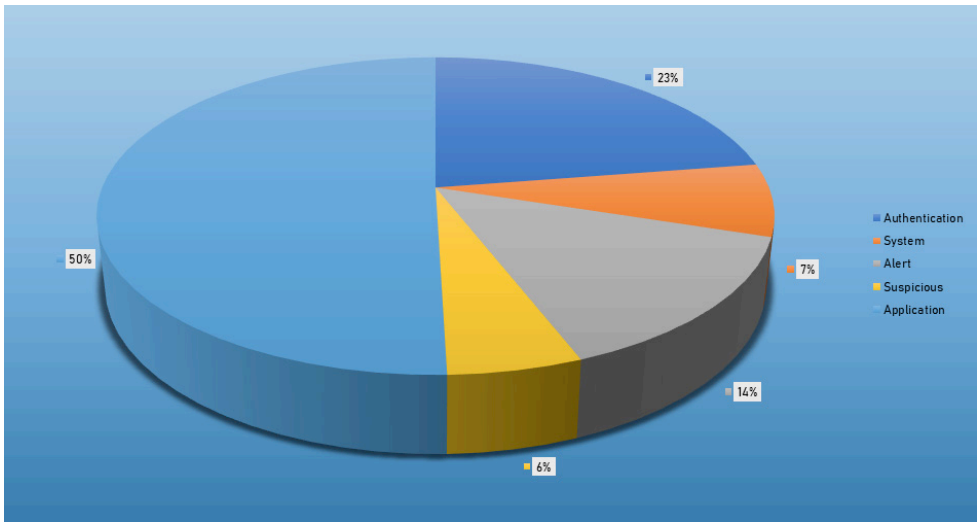


Top Network Attackers

Origin AS	Announcement	Description
AS1221	1.120.0.0/13	Telstra
AS51167	5.189.160.0/20	Contabo GmbH
AS8708	5.12.0.0/14	RCS & RDS SA
AS50113	5.101.88.0/24	PE Sniehur Vladyslavs

Top Event NIDS and Exploits



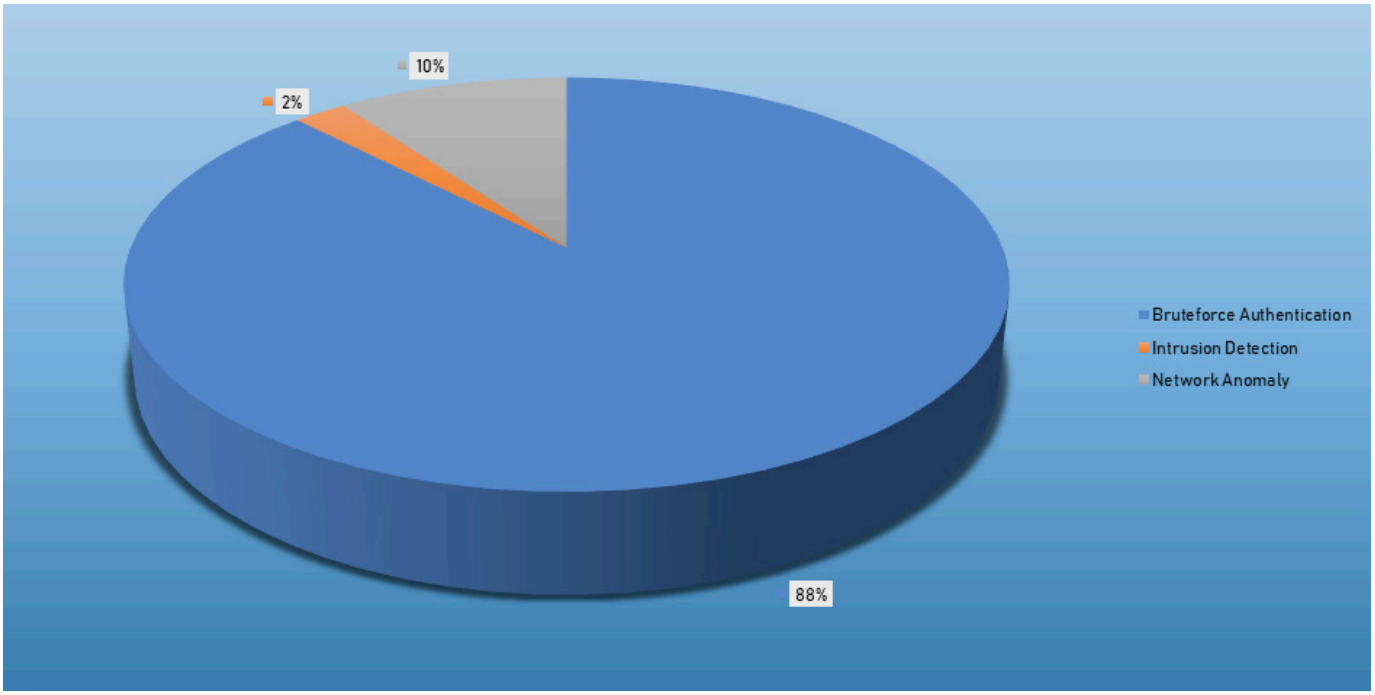


Top Alarms

Type of Alarm	Occurrences
Bruteforce Authentication	3173
Intrusion Detection	83
Network Discovery	361

Comparison from last week

Type of Alarm	Occurrences
Bruteforce Authentication	1772
Intrusion Detection	834
Network Discovery	95

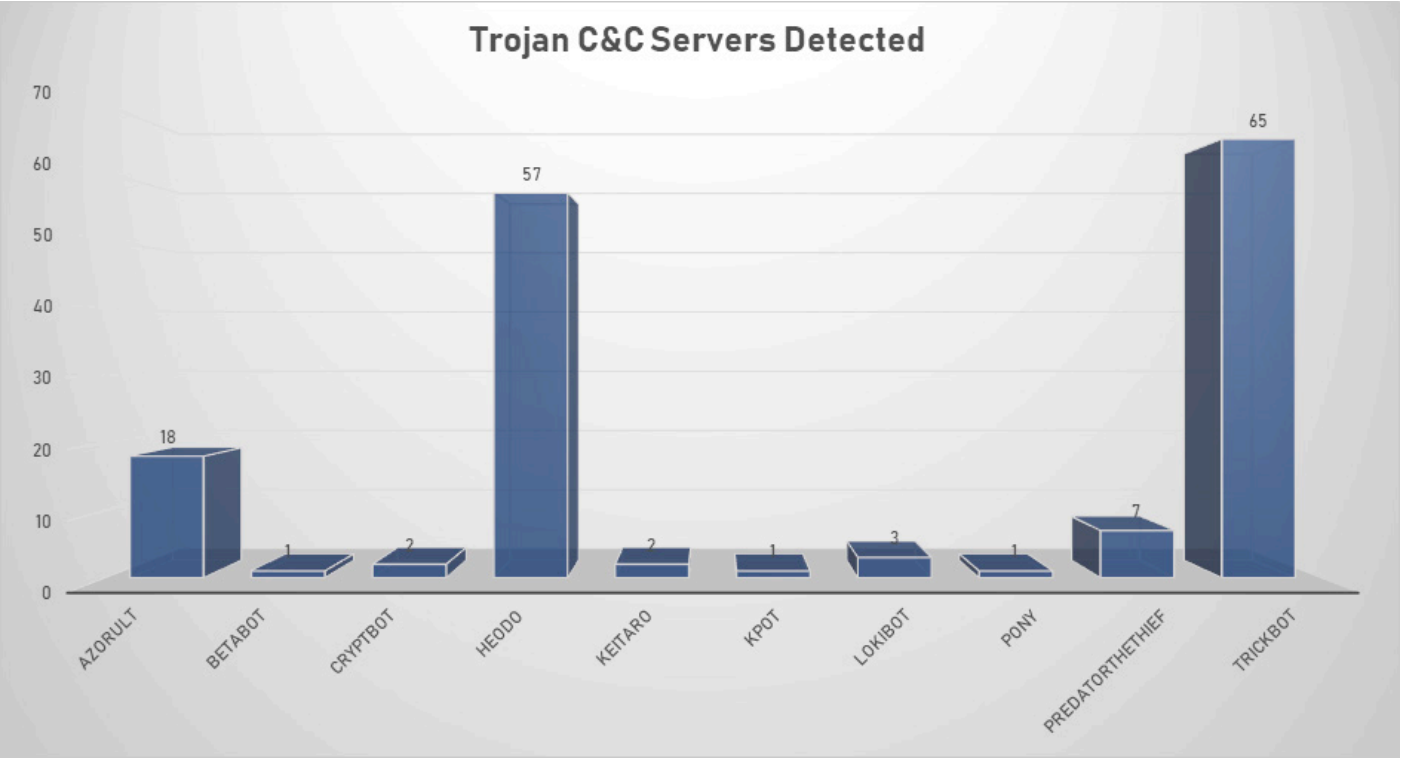


Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	18	167.86.123.249, 185.212.130.104, 185.212.130.17, 185.212.130.34, 185.212.130.39, 185.212.130.50, 185.212.130.54, 185.212.130.56, 185.212.130.69, 185.212.130.70, 185.212.130.74, 185.212.130.78, 185.212.130.8, 185.212.130.87, 194.67.90.231, 45.86.180.5, 93.189.43.82, babillonnglobal.xyz
Betabot	1	111.90.142.117
CryptBot	2	185.151.245.99 , 195.133.144.68
Heodo	57	133.167.80.63, 144.139.158.155, 144.76.62.10, 148.72.151.34, 173.249.157.58, 173.249.47.77, 179.12.170.88, 181.16.17.210, 181.197.2.80, 181.230.126.152, 181.29.164.248, 181.47.235.26, 184.82.233.15, 185.45.24.254, 186.109.91.136, 186.23.132.93, 186.92.11.143, 187.155.233.46, 187.193.89.61, 189.159.113.125, 189.166.13.109, 189.218.243.150

Name	Number Discovered	Location
Heodo		189.253.27.123, 190.113.146.128, 190.120.104.21, 190.166.25.99, 190.217.1.149, 190.228.212.165, 198.199.114.69, 198.199.88.162, 200.30.227.135, 200.90.86.170, 201.106.32.171, 201.184.105.242, 201.213.32.59, 201.250.11.236, 201.250.54.115, 203.99.188.11, 203.99.188.203, 213.138.100.98, 216.98.148.181, 23.229.115.217, 23.239.29.211, 24.45.195.162, 37.187.2.199, 45.33.54.74, 45.56.122.75, 68.183.190.199, 70.32.94.58, 79.127.57.43, 85.25.255.207, 85.25.92.96, 86.98.25.30, 91.109.5.28, 91.204.163.19, 91.83.93.105, 96.20.84.254
Kpot	1	111.90.142.117
LokiBot	3	194.67.206.57, 47.254.66.50, 91.211.245.184
Pony	1	137.59.54.74
PredatorTheThief	7	129.226.56.28, 193.124.186.171, 5.188.60.6, 5.8.88.64, 91.243.80.13, 92.63.197.238, 45.128.184.2
TrickBot	65	101.108.92.111, 104.244.76.156, 107.172.248.84, 128.201.174.107, 144.91.79.12, 144.91.79.9, 170.82.156.53, 172.245.97.148, 178.252.26.235, 181.10.207.234, 181.112.52.26, 185.142.99.61, 185.14.31.109, 185.164.32.113, 185.222.202.192, 185.222.202.223, 185.222.202.62, 185.222.202.76, 185.244.150.142, 185.251.38.165, 185.62.188.117, 185.68.93.43, 185.79.243.37, 186.47.122.182, 188.137.81.201, 190.111.255.219, 190.152.125.22, 194.5.250.79, 194.5.250.83, 194.5.250.89, 194.5.250.94, 194.5.250.95,

Name	Number Discovered	Location
TrickBot		195.123.220.88, 195.123.238.191, 195.123.247.99, 198.24.134.7, 198.98.51.83, 199.195.254.138, 200.127.121.99, 201.187.105.123, 201.210.120.239, 212.22.75.94, 212.80.216.58, 23.94.233.194, 31.202.132.155, 31.214.138.207, 38.132.99.147, 45.142.213.58, 45.66.11.116, 45.80.148.30, 46.174.235.36, 46.21.153.17, 46.21.153.5, 5.185.67.137, 66.55.71.106, 66.55.71.15, 78.24.217.84, 81.177.26.27, 81.190.160.139, 85.11.116.194, 85.143.218.203, 89.228.243.148, 89.25.238.170, 92.242.40.148, 94.156.144.3



Common Malware

Malware Type	MD5	Typical Filename
W32.7AC F71AFA8-95.SBX.TG	4a5078 0ddb3d b16eba b57b0c a42da0 fb	xme64-2141.exe
Win.Trojan. Generic	47b97d e62ae8 b2b927 542aa5 d7f3c8 58	qmreportupload
W32.46B 241E3D3-95.SBX.TG	db69ea aea4d4 9703f1 61c81e 6fdd03 6f	xme32-2141-gcc.exe
W32.WNC ryLdrA: Trojan. 22k2.1201	8c80dd 97c375 25927c 1e549c b59bcb f3	Eternalblue-2.2.0.exe
W32.Generic KD:Attribute. 22lk.1201	74f4e2 2e5be9 0d1525 21125e af4da6 35	jsonMerge.exe

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-11043
Title: PHP 7 Remote Code Execution Vulnerability
Vendor: Multi-Vendor
Description: The vulnerability resides in the "env_path_info" underflow in PHP-FPM . It contains pointer arithmetics that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the "path_info" variable. The vulnerability allows an attacker to run arbitrary commands on a vulnerable server by a specially crafted URL.
CVSS v2 Base Score: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

ID: CVE-2019-16662
Title: rConfig Remote Code Execution Vulnerability
Vendor: Multi-Vendor
Description: An issue was discovered in rConfig where an attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-7609
Title: Kibana Timelion Remote Code Execution Vulnerability
Vendor: Elastic
Description: Kibana Timelion visualizer is exposed to an arbitrary code execution vulnerability. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-14287
Title: SUDO Security Policy 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. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u #$((0xffffffff))" command. An attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID.
CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

ID: CVE-2019-1306
Title: Azure DevOps and Team Foundation Server Remote Code Execution Vulnerability
Vendor: Microsoft
Description: Remote code execution vulnerability exists when Azure DevOps Server (ADO) and Team Foundation Server (TFS) fail to validate input properly. An attacker who successfully exploited this vulnerability could execute code on the server in the context of the TFS or ADO service account. To exploit the vulnerability, an attacker would need to upload a specially crafted file to a vulnerable ADO or TFS server repo and wait for the system to index the file.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-8460
Title: OpenBSD TCP SACK Denial of Service Vulnerability
Vendor: OpenBSD
Description: OpenBSD kernel can be forced to create long chains of TCP SACK holes that cause very expensive calls to tcp_sack_option() for every incoming SACK packet which can lead to a denial of service vulnerability. The SACK holes sorted list is bounded in the TCP established state of the connection by (1) the size of the pool (up to 32K entries), and (2) by the TCP retransmit timer (whose interval could be up to 64 seconds). This means that an attacker could manipulate the connection's window scaling and RTT, forcing the victim to send a large amount of not-ACKed data and increase its retransmission timeout. This in turn enables the attacker to send a large number of SACKs. As the sorted list of SACK holes becomes larger, inserting additional elements becomes more expensive, resulting in higher and higher CPU consumption that may eventually lead to a denial of service vulnerability.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

ID: CVE-2019-10149
Title: Exim Remote Command Execution Vulnerability
Vendor: Exim
Description: Exim is exposed to remote command execution vulnerability. Successfully exploiting this issue may allow an attacker to execute arbitrary commands as root. Improper validation of recipient address in deliver message() function in /src/deliver.c may lead to remote command execution.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-16920
Title: D-Link Unauthenticated Remote Code Execution Vulnerability
Vendor: D-Link
Description: Unauthenticated remote code execution occurs in D-Link products. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)