Red Piranha
unified threat management

Threat Intelligence Report

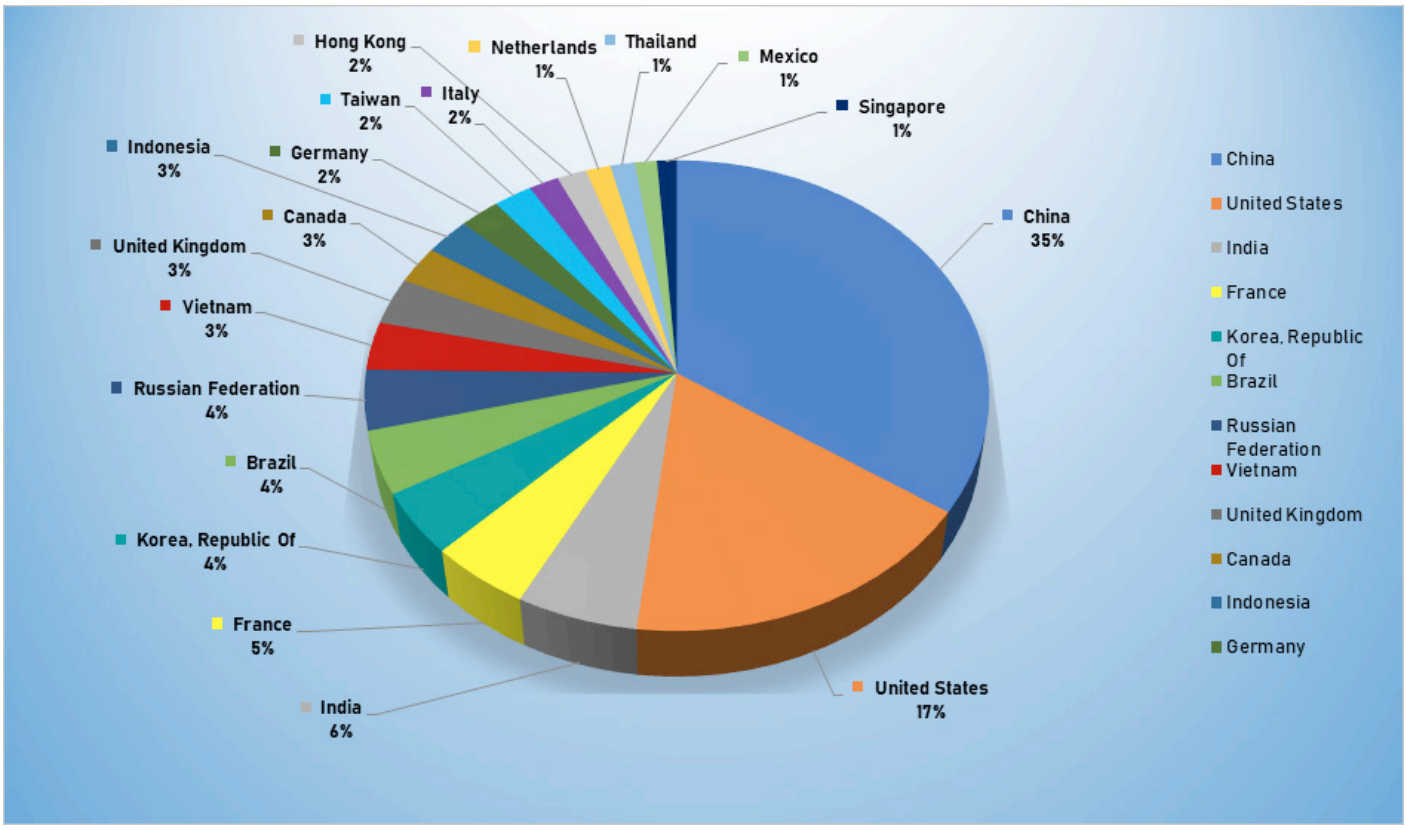
November 4-10 2019

Trends

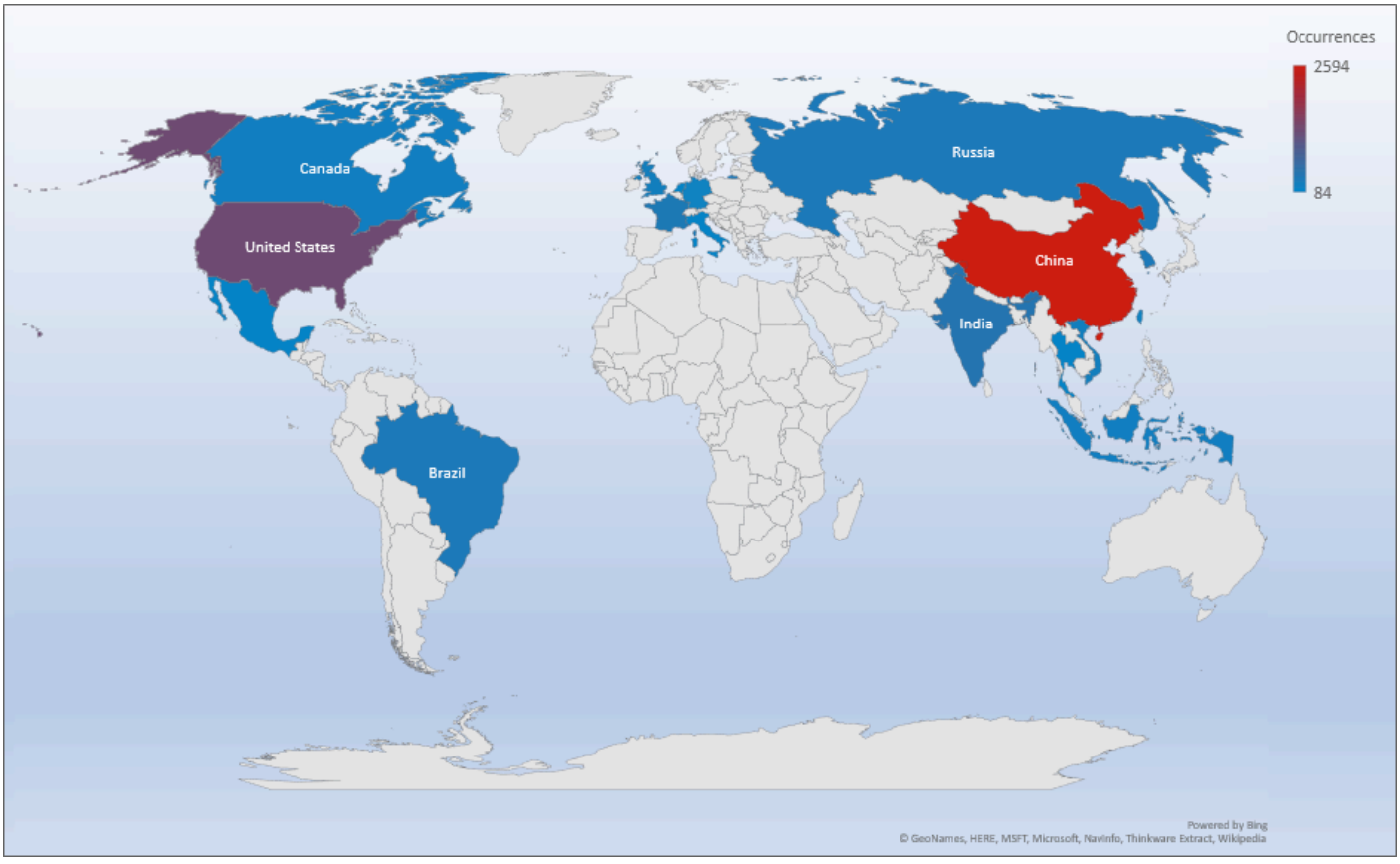
- **The top attacker country was China with 2594 unique attackers (36%).**
- **The top Exploit event was Authentication with 37% of occurrences.**
- **The top Trojan C&C server detected was Heodo with 26 instances detected.**
- **The most prevalent malware detected was Bitcoin Miner xme64-2141.exe, first seen 10th March 2019.**

Top Attacker by Country

Country	Occurrences	Percentage
China	2594	34.55%
United States	1301	17.33%
India	433	5.77%
France	359	4.78%
Korea	327	4.35%
Brazil	325	4.33%
Russian Federation	310	4.13%
Vietnam	248	3.30%
United Kingdom	243	3.24%
Canada	195	2.60%
Indonesia	194	2.58%
Germany	173	2.30%
Taiwan	165	2.20%
Italy	128	1.70%
Hong Kong	126	1.68%
Netherlands	106	1.41%
Thailand	104	1.39%
Mexico	94	1.25%
Singapore	84	1.12%

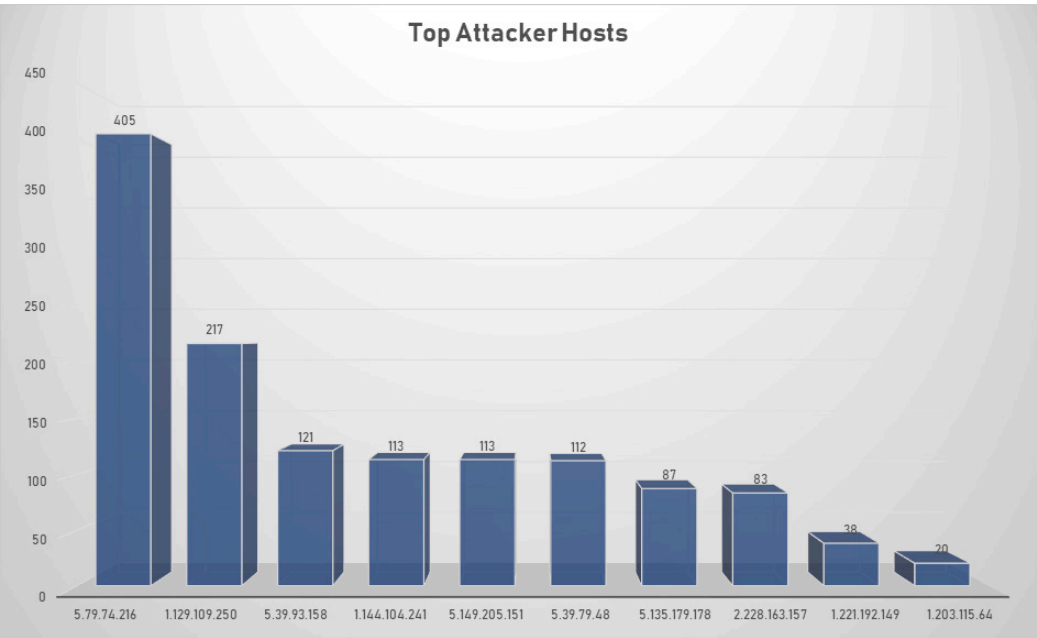


Threat Geo-location



Top Attacking Hosts

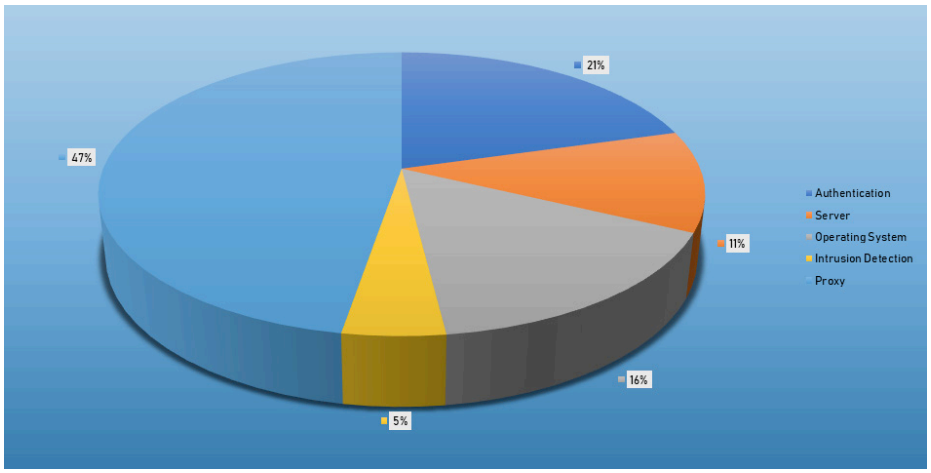
Host	Occurrences
5.79.74.216	405
1.129.109.250	217
5.39.93.158	121
1.144.104.241	113
5.149.205.151	113
5.39.79.48	112
5.135.179.178	87
2.228.163.157	83
1.221.192.149	38
1.203.115.64	20
5.189.176.250	17

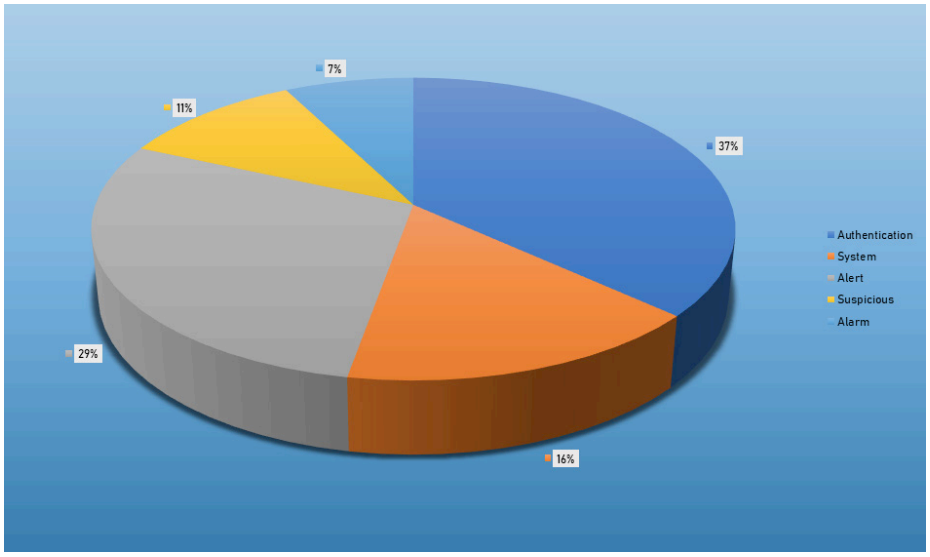


Top Network Attackers

Origin AS	Announcement	Description
AS60781	5.79.64.0/18	LeaseWeb Netherlands B.V.
AS1221	1.128.0.0/11	Telstra
AS16276	5.39.0.0/17	OVH SAS
AS50477	5.149.204.0/22	Svyaz-Energo Ltd.

Top Event NIDS and Exploits



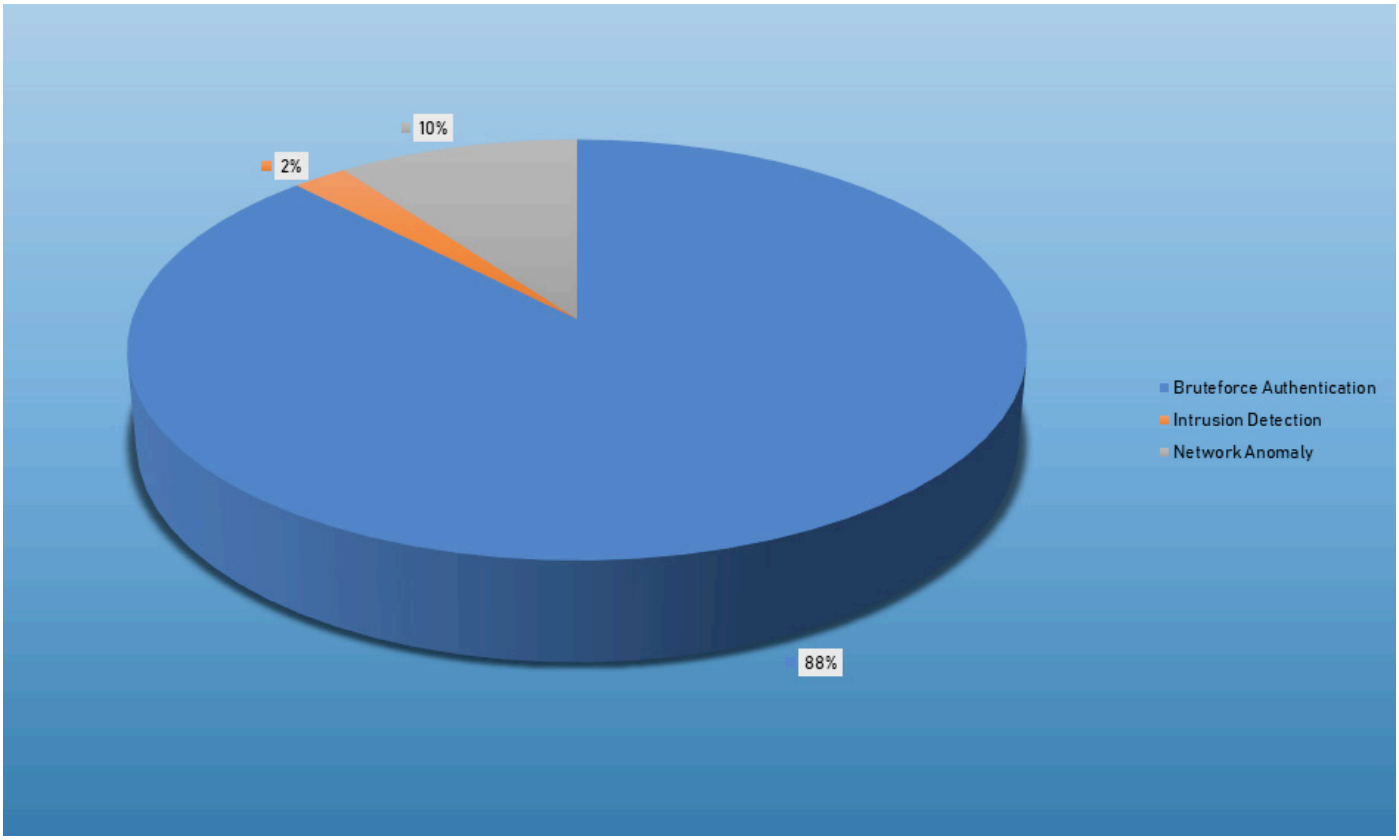


Top Alarms

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

Comparison from last week

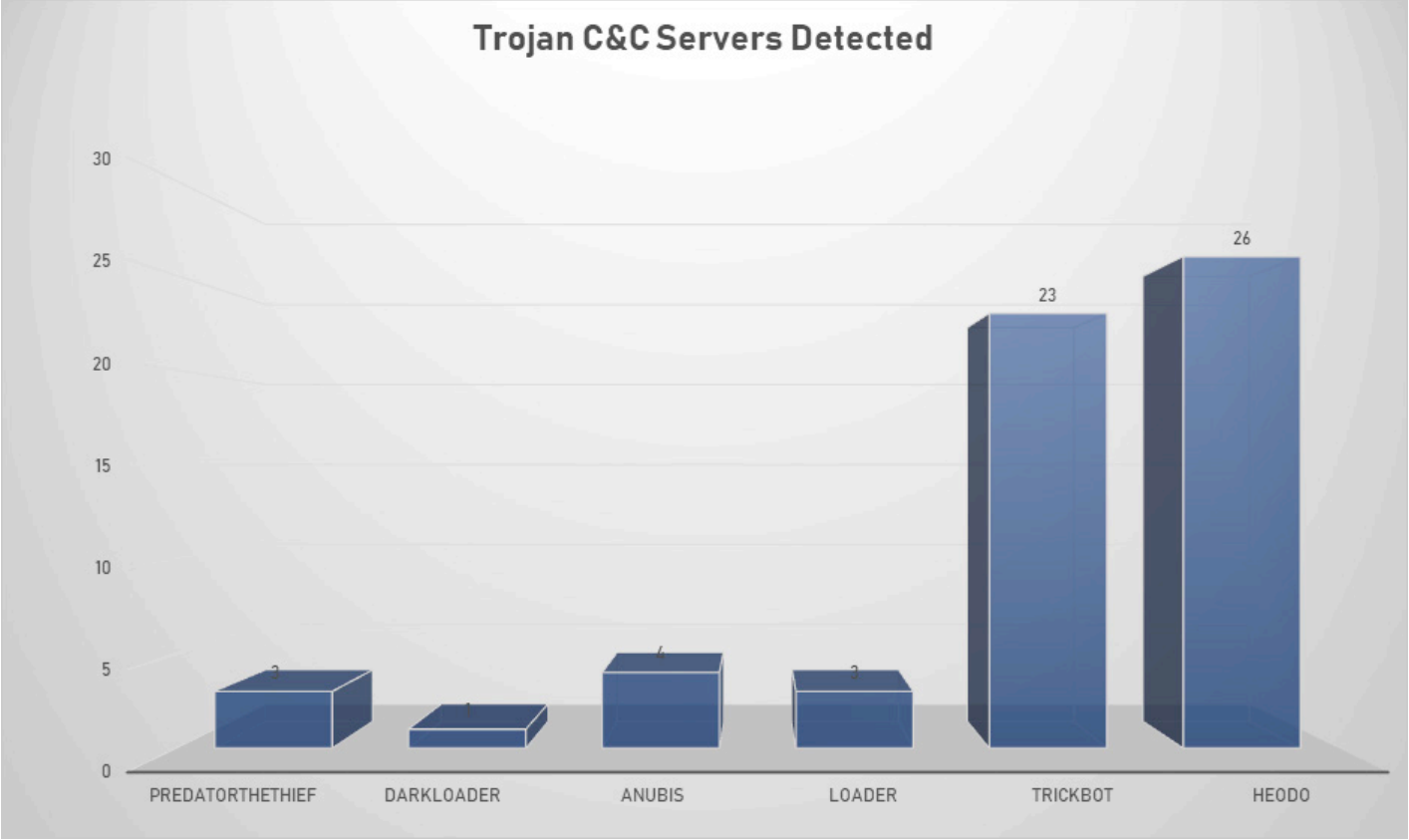
Type of Alarm	Occurrences
Bruteforce Authentication	3173
Intrusion Detection	83
Network Discovery	361



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
PredatorTheThief	3	45.139.236.64, 93.189.47.184, 92.63.197.173
DarkLoader	1	104.27.174.139
Anubis	4	193.32.161.89, 193.32.161.87, 193.32.161.89, 45.141.84.36
Loader	3	83.166.246.53, 45.128.187.231, 193.187.175.176
TrickBot	23	194.5.250.162, 103.219.213.102, 195.123.238.214, 195.123.220.151, 95.181.198.94, 185.177.59.41, 5.2.77.5, 51.89.115.98, 66.55.71.129, 190.142.200.108, 170.84.78.224, 91.108.150.213, 181.113.28.162, 194.5.250.136, 189.28.185.50, 184.95.51.5, 192.3.247.117, 185.252.144.145, 195.133.145.141, 185.99.2.181, 85.204.116.74, 193.26.217.24, 185.117.75.112

Name	Number Discovered	Location
Heodo	26	181.57.193.14, 190.4.50.26, 190.128.222.14, 189.252.102.40, 74.208.125.192, 189.173.113.67, 193.34.144.138, 179.12.170.148, 190.79.228.89, 170.130.31.177, 104.239.175.211, 165.227.156.155, 211.110.229.161, 171.101.153.86, 67.225.179.64, 105.228.98.115, 188.220.235.237, 187.147.152.244, 189.189.56.216, 74.208.173.91, 186.18.224.149, 201.190.133.235, 190.210.184.138, 51.255.165.160, 217.160.19.232, 111.119.233.65



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.Generic KD:Attribute. 22lk.1201	74f4e2 2e5be9 0d1525 21125e af4da6 35	jsonMerge.exe
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

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-2114
Title: NFC Beaming Android Security Control Bypass Vulnerability
Vendor: Google

Description: NFC beaming of applications between devices using Android OS bypasses some security controls (the "install unknown application" prompt). This could lead to local escalation of privilege by installing an application with no additional execution privileges needed. This means, that an Android phone that has NFC and Android Beam enabled, then touching a malicious phone or a malicious NFC payment terminal to the device may allow malware to be installed by bypassing the "install unknown apps" prompt.

CVSS v2 Base Score: 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

ID: CVE-2019-11932
Title: Whatsapp Remote Code Execution Vulnerability
Vendor: Whatsapp
Description: A double free vulnerability exists in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif as used in WhatsApp for Android before 2.19.244. Successful exploitation 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-2019-11043
Title: PHP 7 Remote Code Execution Vulnerability
Vendor: Multi-Vendor
Description: A vulnerability exists in PHP where insufficient validation in the path handling code of FPM module could result in the execution of arbitrary code and to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution. This vulnerability could be exploited to gain partial access to sensitive information. Malicious users could also use this vulnerability to change partial contents or configuration on the system.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

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-2019-1414
Title: Visual Studio Code Elevation of Privilege Vulnerability
Vendor: Microsoft
Description: An elevation of privilege vulnerability exists in Visual Studio Code when it exposes a debug listener to users of a local computer. A local attacker who successfully exploited the vulnerability could inject arbitrary code to run in the context of the current user. If the current user is logged on with administrative user rights, an attacker could take control of the affected system.
CVSS v2 Base Score: 6.3 (AV:L/AC:M/Au:N/C:C/I:C/A:N)

ID: CVE-2019-2888
Title: Oracle WebLogic Server EJBTaglibDescriptor XXE Vulnerability
Vendor: Oracle
Description: A vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)