TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 25th of December – 31st of December, 2022
Report No.: TZ-CERT/WRHP/2022/51

1. NETWORK ATTACKS

A total of **93,087** attacks have been recorded compared to last week **352,404** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	5.235.221.156	root	admin
2.	5.235.223.237	admin	P@ssw0rd
3.	195.3.147.57	support	123456
4.	193.105.134.95	Administrator	123435
5.	170.64.153.105	guest	345gs5662d34
6.	137.184.39.84	administrator	3245gs5662d34
7.	41.78.73.121	supervisor	password
8.	179.60.147.157	default	1234
9.	221.234.230.12	admin1	PlcmSplp
10.	144.126.222.210	Admin	RIP000

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **55,955** malicious software distributed compared to last week in which was **277,603**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan Horse	698995585cb9ffdaedd9766216d141932733e4f964430d3b10c36e0e4cdfeedf
2.	197.57.106.66	Trojan.Generic.31654391	03cd785cc76ccb168997ee76b19b09bb6bf9a6c7e1ba5176355e887667cf5db9
3.	41.137.32.23	TrojWare.Script.TrojanDownloader.Agent.	1521ae629f701ea386738b5ad42c64e3c90a15adb8187d5e67d9671f7

			8716d54
4.	41.210.186.144	HEUR:Trojan-Downloader.Shell.Agent.p	e9e9f498039500e22875972412b4ccbaf0b6a47a54493a0ed874a1255e2024f9
5.	115.239.194.202	HEUR:Trojan-Downloader.Shell.Agent.bc	4644af4d238ffb50fb4a14ab5a1dbaea75a40163266267e5aa1c23fdb1ec4fa2
6.	182.70.125.131	Trojan.Linux.Generic.246192	17dcaa47b0b5981bfb77248c2e0c6670370e463e893b5f07d0152d57d758b69b
7.	202.142.174.182	Linux.MiraiTrojan.Linux.GenericKD.40003689	4d0e4b9c32063c3fa8ed17532637a62e32878238689b232b60ac855ed5ea5271
8.	94.25.179.75	Trojan.Linux.GenericKD.40003689	8536b4ebc530e81acce899611c92f66b944bc9bae57d5bf299719df66ab7bebf
9.	190.120.255.0	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
10.	110.39.129.38	Trojan.Win32.Eb.dqb	f4ac4f735b9ff260a275734d86610dccb8558d1a54c6d6a78a94c33b6aaf6e39

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,604** web attacks compared to last week which was **34,765**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 25th of December – 31st of December, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	20.86.0.91	in/config.php
2.	41.222.181.146	/
3.	20.90.112.171	/users/sign_in
4.	72.251.235.155	/favicon.ico
5.	41.78.169.54	/robots.txt

6.	65.74.177.179	/boaform/admin/formLogin
7.	185.224.128.2	/admin/config.php
8.	41.78.73.121	/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.png
9.	109.237.96.124	/assets/webpack/runtime.9fcb75d4.bundle.js
10.	152.89.196.211	/assets/webpack/main.a66b6c66.chunk.js

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

4.1 Note that most of malicious IP addresses captured are also listed as malicious IP addresses in other sources that are also observing security attacks; thus, security measures should be considered to counter act, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

4.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

4.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

4.4 Deploy Intrusion Detection System (IDS) and configure to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.