TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 18th February 2024 to 24th of February, 2024
Report No.: TZ-CERT/WRHP/2024/8

1. NETWORK ATTACKS

A total of **78,186** attacks have been recorded compared to last week's **75,958** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	218.92.0.93	root	Anonymous
2.	185.246.128.133	user	Pass1234
3.	193.105.134.95	admin	r00t
4.	170.64.135.58	default	123456
5.	170.64.222.19	(empty)	(empty)
6.	91.238.181.247	guest	!Q2w3e4r
7.	41.78.73.146	telnet	qwertyuiop123
8.	170.64.209.173	support	Win1d0W$
9.	170.64.209.139	sa	password
10.	170.64.201.115	test	p@ssw0rd!

Table1: Top 10 Network attacking IP

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

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **96,384** malicious software distributed, compared to last week in which was **25,995.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.250	trojan.billgates/ganiw	b43f51ff2d22190de7506715402aa89521a55d2a24f15044103dfe6fb2cb860c
2.	103.230.152.162	GenericRXIC-BY!B8ED2CB3E9FE	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	103.97.100.243	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

4.	202.83.28.53	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	1.10.250.30	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	12.158.40.82	Trojan.Linux.Generic.208033	50d49c223d41d5e906853cf1b3db9349520e831cfbfe87cbc66d8728f1f9052f
7.	113.172.186.110	Trojan.Linux.Generic.208033	d3b18c52712d3e7a5fc75c027745bff51ddaf90275191341a1eff48270710a48
8.	49.43.161.194	trojan.	1c847d3bd3ef4bf7e21a7091f1479e0e2ca432585ebea996653845b9adfb150e
9.	219.71.243.12	CoinMiner/Linux.Agent.30304472	62ae36274d9e33b704ce1485952cb76dea26dd84a6bf18c870db21ae1c3b7528
10.	60.217.69.70	CoinMiner/Linux.Agent.30304472	9cd71443cf6a3b601e0f9514ba1caa2f58a8fe7ea691d48f3813827525a5139b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,097** web attacks compared to last week which was **1,456.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 18th February 2024 to 24th of February, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	204.12.218.9	/
2.	163.53.246.31	/users/sign_in
3.	190.93.152.243	/admin/config.php
4.	63.251.106.21	/admin/config.php?password%5B0%5D=ZIZO&username=admin
5.	14.103.41.33	/favicon.ico

6.	185.224.128.55	/.env
7.	117.132.188.205	/robots.txt
8.	137.184.114.150	/a2billing/admin/Public/index.php
9.	36.139.63.59	/1.php
10.	41.78.73.146	/admin/assets/js/views/login.js

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the 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 the 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 counteract, 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 it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.