TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 11th February 2024 to 17th of February, 2024
Report No.: TZ-CERT/WRHP/2024/7

1. NETWORK ATTACKS

A total of **75,958** attacks have been recorded compared to last week's **329,255** 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.	185.246.128.133	root	admin
2.	193.105.134.95	user	user
3.	41.78.73.146	admin	root
4.	89.208.103.89	default	123456
5.	170.64.144.83	(empty)	(empty)
6.	162.14.111.169	guest	!Q2w3e4r
7.	110.7.52.148	ubnt	qwertyuiop123
8.	161.132.38.128	support	12345
9.	8.242.72.116	Admin	password
10.	42.180.209.74	test	1234

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 **25,995** malicious software distributed, compared to last week in which was **495,403.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	52.81.102.75	trojan.billgates/ganiw	b43f51ff2d22190de75067 15402aa89521a55d2a24f 15044103dfe6fb2cb860c
2.	103.230.152.162	trojan.hajime/genericrxic	d5601202dff3017db23814 5ff21857415f663031aca9 b3d534bec8991b12179a
3.	41.78.64.250	trojan.hajime/genericrxic	d5601202dff3017db238 145ff21857415f663031a ca9b3d534bec8991b12 179a
4.	59.93.195.107	trojan.hajime/genericrxic	d5601202dff3017db238 145ff21857415f663031a ca9b3d534bec8991b12

			179a
5.	155.138.245.246	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	103.111.233.114	Trojan.Linux.Generic.208033	50d49c223d41d5e906853cf1b3db9349520e831cfbfe87cbc66d8728f1f9052f
7.	103.138.5.47	Trojan.Linux.Generic.208033	d3b18c52712d3e7a5fc75c027745bff51ddaf90275191341a1eff48270710a48
8.	111.59.11.164	trojan.	1c847d3bd3ef4bf7e21a7091f1479e0e2ca432585ebea996653845b9adfb150e
9.	13.38.26.129	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 **1,456** web attacks compared to last week which was **7,293.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 11th February 2024 to 17th of February, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	185.203.122.137	/
2.	146.19.24.28	/users/sign_in
3.	41.78.73.146	/favicon.ico
4.	185.224.128.55	/manager/html
5.	63.251.106.21	/robots.txt
6.	43.156.49.134	/.env
7.	121.41.37.98	/admin/config.php
8.	20.150.216.72	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	31.220.3.140	/HNAP1/
10.	207.46.13.125	/?XDEBUG_SESSION_START=phpstorm

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.