TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 29th October to 4th of November, 2023
Report No.: TZ-CERT/WRHP/2023/44

1. NETWORK ATTACKS

A total of **91,928** attacks have been recorded compared to last week **14,982** 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.	89.183.39.92	root	root
2.	151.238.154.216	admin	admin
3.	193.105.134.95	PlcmSplp	123456
4.	185.246.128.133	(empty)	12345
5.	41.78.73.146	ubnt	PlcmSplp
6.	41.78.75.186	guest	(empty)
7.	165.227.47.17	cameras	password
8.	170.64.170.6	3Comsco	ubnt
9.	93.179.90.178	supervisor	adminHW
10.	143.110.188.140	factory	54321

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 the 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 **100,425** malicious software distributed compared to last week in which was **7,053.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	103.99.207.146	trojan.mirai/cryp	8127f8c730ffe7f767bec28b083dc7f1acd797399f712a201e991f39b9716b6f
2.	196.189.8.22	downloader.bash/miraib	1276e2b8c6b6eaa3b894dc0dc5d537c19b1d8a0e9a82943b364e1c2605e38ed8
3.	101.2.162.121	trojan.hajime/genericrxhu	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	112.135.208.161	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	113.109.196.6	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	113.161.184.10	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	196.202.72.23	trojan.xorddos/ddos	0291de841b47fe19557c2c999ae131cd571eb61782a109b9ef5b4a4944b6e76d
8.	196.221.206.182	trojan.	e91b36bc7495acbbeebfda1c6c3b17e8ea4bbcb42e85137f814377f482fa9fc6
9.	78.85.200.253	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
10.	91.98.58.52	trojan	57e224a416820d22ae95d577c1df71a043ad51c0d6204b80c0a68a8c9120d167

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,120** web attacks compared to last week which was **328.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 29th October to 4th of November, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	72.251.232.180	/
2.	41.78.75.186	/users/sign_in
3.	102.68.79.231	/admin/config.php
4.	109.237.96.124	/admin/config.php?password%5B0%5D=ZIZO&username=admin
5.	41.78.169.54	/adcr.nhn

6.	41.78.73.146	/favicon.ico
7.	117.132.188.204	/boaform/admin/formLogin
8.	121.173.126.140	/.env
9.	152.32.247.22	/a2billing/admin/Public/index.php
10.	60.217.75.70	/robots.txt

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.