TZ-CERT HONEYPOTS WEEKLY REPORT
**Period : **16th to 22nd of April, 2023
Report No.: TZ-CERT/WRHP/2023/16

1. NETWORK ATTACKS

A total of **184,195** attacks have been recorded compared to last week **221,144** 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.	193.105.134.95	root	admin
2.	195.3.147.52	admin	123456
3.	116.110.75.174	support	support
4.	116.110.15.136	PlcmSplp	password
5.	116.110.72.248	user	PlcmSplp
6.	41.78.174.77	test	12345
7.	171.251.17.184	guest	1234
8.	116.105.217.16	345gs5662d34	(empty)
9.	116.110.114.142	ubuntu	345gs5662d34
10.	116.110.24.210	ubnt	user

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 **229,283** malicious software distributed compared to last week in which was **171,123.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan.Gen.NPE	f6ebea5a89985bbd86ceadac5d72f9f660be979c254c189a7301ec7dd7769d3c
2.	41.78.64.252	downloader.linux/medusa	80ad3c4b6686c680178b1f2cf87321c7a8cd61d28d16d88b7baf1be505b57f7a
3.	41.59.201.7	downloader.linux/medusa	4dd617076871d2b5c8204ed7787777f7162888b9a0123dc3b840b4ce0b62b589

4.	41.59.194.240	downloader.linux/medusa	e8b22de7eab7d0256480ac154cd2af8301b2ab6384df9a59f409091193554eae
5.	41.59.203.31	trojan.linux/mirai	36bc49ede8e0f4a54449602ca2bc681f96b14869841a243ddfb7d94fb6f28749
6.	173.214.80.202	trojan.linux/xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.211.101.78	trojan.linux	61313b582ba8fa8ba6a819fd4a960d51e7c92324efe8c0f5294c651f26223753
8.	41.78.64.254	Trojan.Linux.Generic.246192	e6ce9937266d30a22c6aa5c48d818dba86491b1becf1fe0ca07b3de85d2d88ab
9.	41.59.201.132	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946
10.	41.101.115.112	rojan.linux/xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,936** web attacks compared to last week which was **4,078.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th to 22nd of April, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	121.173.126.140	/
2.	122.168.198.123	/get
3.	4.236.146.128	//admin/config.php
4.	104.248.18.207	/adcr.nhn
5.	193.32.162.159	/users/sign_in
6.	175.198.181.204	/boaform/admin/formLogin

7.	109.237.96.124	/.env
8.	109.237.96.251	/favicon.ico
9.	41.78.174.77	/recordings/
10.	152.89.196.54	/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.