TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 4th to 10th of June, 2023
Report No.: TZ-CERT/WRHP/2023/23

1. NETWORK ATTACKS

A total of **102,505** attacks have been recorded compared to last week **75,189** 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.	139.9.73.181	root	admin
2.	193.105.134.95	admin	p@ssword
3.	195.3.147.52	(empty)	123456
4.	185.224.128.141	supervisor	1234
5.	111.198.57.24	tech	12345
6.	41.78.75.186	ubuntu	(empty)
7.	170.64.142.109	admin1	ubnt
8.	41.78.174.77	pi	user
9.	41.78.38.140	ubnt	root
10.	206.189.59.169	user	pass

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 **159,962** malicious software distributed compared to last week in which was **156,132**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	197.250.7.167	trojan.linux/mirai	65df44523c379b9cf7f334056642e51305af7a8c8b4af7b084b4432632e85098
2.	41.59.194.240	trojan.hajime/linux	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	41.59.200.32	trojan.hajime/linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

4.	194.65.120.40	trojan.hajime/linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.59.86.254	trojan.linux/hajime	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
6.	41.59.201.132	trojan.linux/xorddos	f8d6c87b8b4665dc7ee47c730aa9b895cc2263a15e4c44ef4b9fdffed87769c2
7.	41.111.178.34	trojan.linux	0aa4b85087c0bb27544d908682f7df7ba5d6987206cf317263b7b018f6bcda2e
8.	41.59.201.7	trojan.linux	d86437b589214d732eace62cfcdf52121751508157564c74cbbea27d0e5a3119
9.	41.59.211.41	trojan.linux/uselvk422	c29dc96f96e7d23e18b4cb242dc404a22b5bfc39dd4489a24c30b942ef52742a
10.	138.122.92.14	Trojan.Win32.Eb.dqb	4bf044ae7b903ca9edf19180b617abd363bf981d4a22d0b0de13fa72461be4fa

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,551** web attacks compared to last week which was **1,548.**

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

SN	ATTACKING IPS	TOP URI
1.	20.0.210.205	/
2.	18.136.27.8	//admin/config.php
3.	83.97.73.89	/users/sign_in
4.	190.101.154.30	/boaform/admin/formLogin
5.	98.214.9.84	/.env

6.	52.38.40.201	/favicon.ico
7.	109.237.96.124	/1.php
8.	41.78.174.77	/bundle.js
9.	109.237.96.251	/Autodiscover/Autodiscover.xml
10.	41.78.169.54	/_ignition/execute-solution

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.