



TZ-CERT HONEYPOTS WEEKLY REPORT

Period : 11th to 17th of June, 2023

Report No.: TZ-CERT/WRHP/2023/24

1. NETWORK ATTACKS

A total of **137,560** attacks have been recorded compared to last week **102,505** 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.	47.52.157.45	root	tomcat
2.	62.171.148.184	admin	P@ssw0rd
3.	193.105.134.95	guest	123456
4.	195.3.147.52	supervisor	qwerty123456
5.	159.223.99.140	git	abc123456
6.	41.78.75.186	ftpuuser	(empty)
7.	170.64.142.109	centos	Win1doW\$
8.	121.40.246.228	oracle	oelinux123
9.	185.224.128.141	sa	cameras
10.	41.78.174.77	mysql	realtek

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 **154,067** malicious software distributed compared to last week in which was **159,962**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	trojan.linux/mirai	98b1a3901d9143ee034 140c0555e18b620c29f4 9d0b566bb5bbd289f890 33339
2.	41.59.194.240	Linux/Agent.SHS!tr.dldr	65df44523c379b9cf7f33 4056642e51305af7a8c8 b4af7b084b4432632e85 098
3.	41.59.201.7	trojan.hajime/linux	77a2c317ca9d43acc05 6cf8217a8c838d23af63 965b33dc931877360d5 919b8d

4.	41.59.201.132	HEUR:Backdoor.Linux.Mir ai.fk	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.59.41.28	trojan.linux/hajime	f8d6c87b8b4665dc7ee47c730aa9b895cc2263a15e4c44ef4b9fdffed87769c2
6.	41.59.200.32	trojan.linux/xorddos	f8d6c87b8b4665dc7ee47c730aa9b895cc2263a15e4c44ef4b9fdffed87769c2
7.	41.111.178.34	ELF/Agent.MKVM!tr	0aa4b85087c0bb27544d908682f7df7ba5d6987206cf317263b7b018f6bcda2e
8.	41.59.114.90	trojan.linux	d86437b589214d732eace62cfcdf52121751508157564c74cbbea27d0e5a3119
9.	41.59.203.192	trojan.linux/uselvk422	c29dc96f96e7d23e18b4cb242dc404a22b5bfc39dd4489a24c30b942ef52742a
10.	41.137.137.90	Trojan.Win32.Eb.dqb	4bf044ae7b903ca9edf19180b617abd363bf981d4a22d0b0de13fa72461be4fa

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,455** web attacks compared to last week which was **2,551**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 11th to 17th of June, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	83.97.73.89	/
2.	43.134.103.90	/users/sign_in
3.	41.78.169.54	/favicon.ico
4.	109.237.96.251	/boaform/admin/formLogin
5.	41.78.38.141	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

6.	41.78.75.186	/.env
7.	109.237.96.124	/1.php
8.	196.189.124.200	/admin/config.php
9.	84.252.140.133	/bundle.js
10.	60.217.75.70	/files/

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.