TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 28th May to 3rd of June, 2023
Report No.: TZ-CERT/WRHP/2023/22

1. NETWORK ATTACKS

A total of **75,189** attacks have been recorded compared to last week **85,414** 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	p@ssword
3.	171.251.23.53	sa	123456
4.	41.78.75.186	user	Win1doW$
5.	111.198.57.24	cron	666666
6.	41.78.174.77	support	root
7.	41.78.38.140	postgres	admin123
8.	104.248.243.11	www-data	1qaz@WSX
9.	67.205.183.226	telnet	ABCabc123
10.	180.142.128.168	postgres	ubnt

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 **156,132** malicious software distributed compared to last week in which was **147,125**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.86.254	Linux.Mirai!g2	818675ba09b4883e57790aff9a79669275dfe088d02dc5f5cf459b16375d17db
2.	41.59.211.41	Trojan.Linux.GenericKD.11272	7d93419e78647d3cdf2ff53941e8d5714afe09cb826fd2c4be335e83001bdabf
3.	41.59.194.240	Trojan:Linux/Multiverze	77a2c317ca9d43acc056cf8217a8c838d23af63965b33dc931877360d5919b8d

4.	41.59.201.7	trojan.linux/hajime	4b050a597507d3149b3f7709e8ae5e5b5ce0914c9c53064503b9d16052784998
5.	41.59.200.32	Trojan:Linux/Downldr.B!MTB	f8d6c87b8b4665dc7ee47c730aa9b895cc2263a15e4c44ef4b9fdffed87769c2
6.	41.59.41.28	trojan.linux	ab31ea17ea415efd30a19fdb7a68b92146692b76584007cbbb94f55b9761b8dc
7.	189.127.37.214	trojan.linux	9ec9a97605509da77411ab9b0267c25fb8074e36e2d96adb50a144d6dcf35620
8.	219.146.255.114	Riskware/CoinMiner	e dadd035cac52ae08767a9aea15761678f8a3ebad09f55d3a36e2205387a15bcd
9.	190.202.74.158	HEUR:Trojan-DDoS.Linux.Xarcen.d	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
10.	85.175.60.34	Trojan.Win32.Eb.dqb	4bf044ae7b903ca9edf19180b617abd363bf981d4a22d0b0de13fa72461be4fa

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,548** web attacks compared to last week which was **2,070**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 28th May to 3rd of June, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	83.97.73.89	/favicon.ico
3.	43.252.75.114	/users/sign_in
4.	41.78.169.54	/boaform/admin/formLogin

5.	41.78.174.77	/.env
6.	41.78.75.186	/robots.txt
7.	41.78.174.45	/1.php
8.	41.78.38.140	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	71.210.130.110	/recordings/
10.	109.237.96.124	/bundle.js

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.