TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 16th of February to 22nd of February, 2025
Report No.: TZ-CERT/WRHP/2025/08

1. NETWORK ATTACKS

A total of **245,462** attacks have been recorded compared to last week's **235,422** 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.	103.80.117.250	root	(empty)
2.	58.239.58.227	Admin	qwerty123456
3.	131.161.22.242	tech	123456
4.	62.171.130.190	ubuntu	345gs5662d34
5.	45.249.8.86	vadmin	password
6.	87.98.138.86	debian	!@#$%^&*
7.	5.161.181.1	guest	P@ssw0rd!!!
8.	218.92.0.179	sa	telnet
9.	118.107.88.19	postgres	Welcome123
10.	80.178.219.114	ftpuser	root

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 **55,308** malicious software distributed, compared to last week in which was **118,637.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	BASH/Dloader.AAN!tr.dldr	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	113.53.43.162	Trojan:Linux/Multiverze	043675aa01acc869a78590befba137ba77e45a7509926739f7d13b75042d4119
3.	124.66.139.2	trojan.multiverze/vsntch24	2c950af8754cef68298d2e128d11045eed5018c35d30394f5ec087768dc9ae88

4.	39.57.36.136	trojan.r002c0dlc24	75a512a7acd86a80d2ff5c180c80d1a852e7391aeeacc1ebcfae9e344b5c940f
5.	41.230.10.221	ELF/Xorddos.D!tr	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
6.	41.175.24.90	trojan.xorddos/ddos	47eda32af60fe513d6edabf8ab322e18d45619663040a1c294a93b91d6386601
7.	185.250.29.61	ELF/Xorddos.AB!tr	2f42a42c6c2f48bce1a8c436362e3e43ec0c9cd0fb8c9bba4bf5f61f5415730d
8.	14.171.75.39	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	180.195.210.169	miner.qwxqh/r002c0dbf25	3ff682369764dc6e104fdc38a20c0b83f89e83925a664191a6d648d9e6a9cd04
10.	185.217.188.112	trojan.fcrcu/r002c0dbf25	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,391** web attacks compared to last week which was **5,934.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of February to 22nd of February, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.176	/
2.	204.76.203.18	/.env
3.	193.68.89.10	/admin/config.php
4.	162.217.96.20	/cgi-bin/luci/;stok=/locale
5.	185.93.89.118	/robots.txt
6.	193.68.89.51	/admin/config.php?password%5B0%5D=ZIZO&userna

		me=admin
7.	195.178.110.163	/favicon.ico
8.	78.153.140.224	/config/application.yml
9.	141.255.166.90	/libs/js/iframe.js
10.	36.189.253.253	/_profiler/phpinfo

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,566** ICS attacks compared to last week which was **2,354.**

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 16th of February to 22nd of February, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.41.47	kamstrup_protocol	1025
2.	152.32.206.38	IEC104	2404
3.	101.36.123.247	guardian_ast	50100
4.	207.90.244.10	kamstrup_management_protocol	10001
5.	118.193.33.155	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.