TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 23rd of February to 01st of March, 2025
Report No.: TZ-CERT/WRHP/2025/09

1. NETWORK ATTACKS

A total of **319,605** attacks have been recorded compared to last week's **245,462** 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.	62.171.130.190	root	(empty)
2.	117.232.115.59	admin	1234
3.	45.249.8.86	guest	anonymous@
4.	186.22.239.76	default	admin@123
5.	51.222.150.53	super	123456
6.	51.222.150.61	support	letmein
7.	177.11.49.133	administrator	SUPPORT
8.	185.233.247.245	telnet	Sa@1234
9.	194.0.234.107	ubnt	MonTelSys
10.	87.98.138.86	ONTUSER	123qwe!@#

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 **69,315** malicious software distributed, compared to last week in which was **55,308.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	HEUR:Trojan-Downloader.Shell.Agent.dh	229022b01619739c182d59433ae8ebe87d299175a938e344f569dfc060cab870
2.	196.115.84.19	CL.Downloader!gen277	3bb94afe8bd7fff0f5ee5673b42130d1c8c545bed9a20d10cbbd017046559898
3.	179.63.38.135	Trojan.GenericKDZ.109484	49edcdcb01745fc7111690cc81681d62178bcc5e262cc27c6829679af85f5846

4.	41.138.61.41	Backdoor:Linux/Hajime.A	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	144.123.166.146	Trojan:Linux/CoinMiner!MTB	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
6.	41.38.119.113	trojan.multiverze/r002c0dfu24	00deea7003eef2f30f2c84d1497a42c1f375d802ddd17bde455d5fde2a63631f
7.	79.133.190.160	trojan.r002c0dah25	0670da04a700a5e7ec0ca80de285d75985116b669dc02c61cebfc22b5b3edab3
8.	101.51.50.189	HEUR:Trojan.Linux.Miner.gen	2a4fd33c7f7af47b72f8ec6f55ae21ca998e110910f8b8b7b929b256069979a9
9.	197.232.90.83	Exploit.EXP/ELF.Coinminer.A	32c44efae5abbf335db74360d5cc58135005ebdcc41d9cf8b61258a2ef8cafb8
10.	113.53.43.162	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,771** web attacks compared to last week which was **4,391.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd of February to 01st of March, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.176	/
2.	195.177.95.251	/.env
3.	193.68.89.10	/cgi-bin/luci/;stok=/locale
4.	13.235.239.143	/admin/config.php
5.	181.214.167.234	/favicon.ico
6.	92.255.57.58	/robots.txt

7.	162.217.96.20	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	193.41.206.189	/login.rsp
9.	78.153.140.151	/admin/assets/js/views/login.js
10.	193.68.89.51	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,012** ICS attacks compared to last week which was **3,566.**

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 23rd of February to 01st of March, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.185.104	kamstrup_protocol	1025
2.	3.143.222.172	guardian_ast	10001
3.	118.26.36.130	kamstrup_management_protocol	50100
4.	152.32.188.177	IEC104	2404
5.	167.94.138.60	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.