TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 19th of October to 25th of October, 2025
Report No.: TZ-CERT/WRHP/2025/42

1. NETWORK ATTACKS

A total of **713,074** attacks have been recorded compared to last week's **956,132** 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.	194.50.16.73	root	123456
2.	112.26.45.228	admin	123
3.	103.99.206.83	odoo	admin
4.	206.81.107.154	dqi	password
5.	167.250.224.25	dspace	P@ssw0rd
6.	185.246.130.20	ftp	marek2025
7.	187.248.68.142	administrator	root123
8.	115.29.198.219	user01	adminHW
9.	196.251.88.103	tomcat	qwerty
10.	41.78.73.146	supervisor	welcome

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 **584,271** malicious software distributed, compared to last week in which was **544,800.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	Shell/ElfDownloader.S1	1ebf139fe8271dd0c5ee67ae22e4d4269115508c089fb2f31143c3778ae3b193
2.	41.59.211.41	Trojan.Linux.Multiverze.4!c	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
3.	196.41.60.214	Trojan.Linux.Generic.D64DBB	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

4.	41.59.201.132	Miner:Linux/CoinMiner.99dbe0da	079b5572f35d9de8cdfcdd1d0dbdc395753f1c9bcb474f18dac752842f745b07
5.	41.59.149.186	HEUR:Trojan.Linux.Miner.gen	20e3f957446527a31ff3fd9d53b48c6046c9858d789ca043a6869cbea254bc20
6.	111.223.126.92	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	156.204.178.16	HackTool/Linux.BitCoinMiner.a	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	200.105.177.62	Riskware.Linux.BitCoinMiner.1!c	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	85.185.30.130	Trojan.Linux.MALXMR.USBLHH25	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	176.65.31.129	HEUR:Trojan-Downloader.Shell.Agent.p	7a4515e7ea0674a1844fe0b38d5143e79b7c7bb174c6b5fe13d81bcb5981519f

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **57,469** web attacks compared to last week which was **21,363.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of October to 25th of October, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.110	/
2.	139.87.113.214	/login
3.	64.39.103.49	/manager/
4.	139.87.112.123	/robots.txt
5.	64.39.106.87	/sysmgmt/2015/bmc/info
6.	64.39.106.125	/CGI/Java/Serviceability?adapter=device.statistics.de

		vice
7.	64.39.106.5	/q79w_38jg__.shtml
8.	45.148.10.243	/favicon.ico
9.	79.110.49.8	/accounting/control/main
10.	34.174.171.71	/webacs/js/xmp/nls/xmp.js

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,018** ICS attacks compared to last week which was **3,279.**

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 October to 25th of October, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	3.130.96.91	kamstrup_protocol	1025
3.	45.140.17.97	IEC104	2404
4.	139.87.112.110	kamstrup_management_protocol	50100
5.	3.134.148.59	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.