TZ-CERT HONEYPOT WEEKLY REPORT

Period: 2nd to 8th November 2026 | **Report No.:** TZ-CERT/WRHP/2026/45

01: WEEKLY ATTACK SUMMARY

1,304,051	1,595,393	34,374	1,662,460
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 41.4% vs last week	↑ 82.5% vs last week	↓ 47.8% vs last week	↓ 41.1% vs last week

A total of 1,304,051 network attacks were recorded across all sensors during the period 2nd to 8th November 2026, representing a decrease of 41.4% compared to last week's 2,224,859 attacks. Malware activity increased by 82.5%, web attacks decreased significantly by 47.8% and ICS attacks fell by 41.1%. This divergence indicates a shift in adversary focus toward malware distribution.

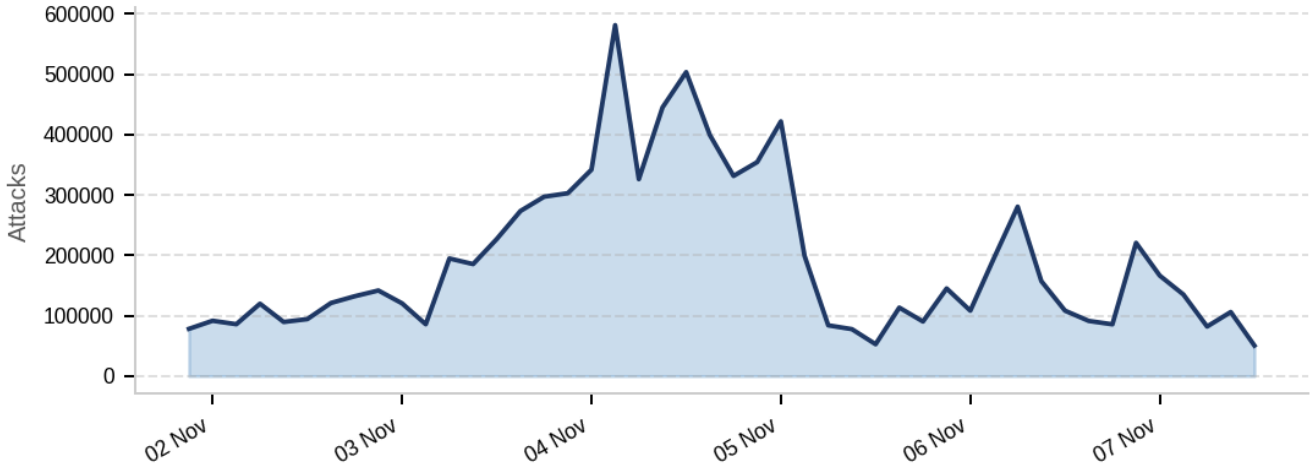


Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,304,051 attacks have been recorded, down from last week's 2,224,859 by 41.4%. The top 10 attacking IPs and the most frequently attempted usernames and passwords are listed below; each column is ranked independently by frequency. Most credentials used are default or weak, so enforcement of password policies is strongly advised.

SN	ATTACKING IP	TOP USERNAMES	TOP PASSWORDS

1.	179.43.133.154	root	123456
2.	109.160.32.36	admin	1234
3.	179.43.139.58	ubuntu	123
4.	62.99.5.57	0	0
5.	109.160.32.148	user	admin
6.	94.183.174.99	deploy	password
7.	109.160.32.161	administrator	12345678
8.	109.160.32.37	test	root
9.	109.160.32.177	eagle	1
10.	109.160.32.163	support	12345

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 1,595,393 malicious software samples were distributed during the week, an increase of 82.5% compared to last week's 874,348. The top ten attacking IPs and, ranked separately, the ten most frequently downloaded malware samples with their SHA256 hashes are listed below for threat hunting and IOC correlation.

SN	ATTACKING IP	MALICIOUS SOFTWARE	SHA256 HASH
1.	162.250.126.218	miner.malxmr/rootkit	a151d3f4f2422531f30a843ffb35479596c86722bb103bdf8591105687f9b125
2.	41.93.68.98	downloader.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
3.	102.208.164.221	trojan.mirai/usblk126	6a6839d06cad3a0a6e37ab8874aa7dfee5b5818b8f0586fd74d680c34d890e68
4.	41.59.203.60	trojan.abtrojan/njww	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
5.	202.69.36.104	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	41.59.196.23	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
7.	2.187.37.124	trojan.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
8.	41.90.13.170	trojan.sagnt/usblk426	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141

9.	41.59.211.41	trojan.sagent/abtrojan	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
10.	41.10.182.159	trojan.agent5/alien	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 34,374 web attacks were recorded, a decrease of 47.8% from last week's 65,903. The top 10 attacking IPs and the most requested URIs are detailed below, each ranked independently. Notable activity includes environment file (.env) enumeration.

SN	ATTACKING IP	TOP URI / REQUEST
1.	102.220.163.241	/
2.	213.209.159.175	/.aws/config
3.	217.60.76.167	/admin/config.php
4.	85.11.167.204	/favicon.ico
5.	185.177.72.64	/.env
6.	103.215.74.112	/robots.txt
7.	85.155.14.16	/login
8.	45.138.12.51	/.git/config
9.	129.213.151.234	/logon.htm
10.	194.50.16.198	/.env.production

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,662,460 ICS attacks were recorded, a decrease of 41.1% from last week's 2,822,022. The top 5 attacking IPs and, ranked separately, the most targeted industrial protocols with their ports are listed below. Exposed ICS services represent a high-risk vector requiring immediate attention from critical infrastructure operators.

SN	ATTACKING IP	PROTOCOL EXPLOITED	PORT
1.	46.128.202.246	snmp	161
2.	62.214.226.95	IEC104	2404
3.	62.214.224.59	guardian_ast	10001
4.	151.228.156.25	kamstrup_protocol	1025
5.	100.36.63.118	ipmi	623

Table 4: Top 5 ICS Attacking IPs with Protocols and Ports

06: RECOMMENDATIONS

Based on honeypot sensor data for this reporting period, the following actions are recommended for national ICT stakeholders:

1. Monitor all listed malicious IP addresses across internal networks. These IPs are also flagged by external threat intelligence sources and may be used in further attacks.

2. Enforce strong password policies and prohibit usage of the listed credentials (usernames and passwords). Deploy mechanisms to monitor and alert on excessive login attempts.

3. Scan all systems for files matching the SHA256 hashes listed in the Malware section (Table 2) and quarantine any matches immediately.

4. Deploy or update Intrusion Detection Systems (IDS) with rules to flag the IP addresses, web request patterns, and ICS protocols identified in this report.