# TZ-CERT HONEYPOT WEEKLY REPORT

**Period:** 9th to 15th November 2026 | **Report No.:** TZ-CERT/WRHP/2026/46

## 01: WEEKLY ATTACK SUMMARY

| 1,739,117 | 3,505,959 | 26,912 | 1,152,417 |
|---|---|---|---|
| NETWORK ATTACKS | MALWARE SAMPLES | WEB ATTACKS | ICS ATTACKS |
| ↑ 33.4% vs last week | ↑ 119.8% vs last week | ↓ 21.7% vs last week | ↓ 30.7% vs last week |

A total of 1,739,117 network attacks were recorded across all sensors during the period 9th to 15th November 2026, representing an increase of 33.4% compared to last week's 1,304,051 attacks. Malware activity increased by 119.8%, web attacks decreased by 21.7% and ICS attacks fell by 30.7%. This divergence indicates a shift in adversary focus toward network services and malware distribution.




*Figure 1: Daily trend of Honeypot attacks*

## 02: NETWORK ATTACKS

A total of 1,739,117 attacks have been recorded, up from last week's 1,304,051 by 33.4%. 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.** | 103.163.215.105 | root | 123456 |
| **2.** | 31.129.22.45 | admin | 1234 |
| **3.** | 195.178.110.78 | ubuntu | admin |
| **4.** | 179.43.133.154 | user | 123 |
| **5.** | 109.160.32.130 | test | root |
| **6.** | 109.160.32.160 | deploy | 12345 |
| **7.** | 109.160.32.120 | Administrator | 12345678 |
| **8.** | 60.255.74.197 | enable | password |
| **9.** | 109.160.32.39 | system | linuxshell |
| **10.** | 109.160.32.125 | support | 1 |

*Table 1: Top 10 Network Attacking IPs*

## 03: MALICIOUS SOFTWARE (MALWARE)

A total of 3,505,959 malicious software samples were distributed during the week, an increase of 119.8% compared to last week's 1,595,393. 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 | downloader.bash/miraia | 39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96 |
| **2.** | 41.93.68.98 | miner.malxmr/rootkit | a151d3f4f2422531f30a843ffb35479596c86722bb103bdf8591105687f9b125 |
| **3.** | 41.59.196.23 | downloader.shell | 742ff862dd55f92409cad918738c80a3452a0b787d142e0283999a65b060c573 |
| **4.** | 41.59.203.60 | trojan.malxmr/usblhf26 | d7f98e379c400c13340781ccb65017c000330824ea26680866b9d3e43d641721 |
| **5.** | 41.93.63.66 | trojan.mirai/ddos | 26a130b4d98c369ac5654549e475d57d17317b59a270d22582e03b1dad44deb7 |
| **6.** | 41.90.13.170 | trojan.mirai/ddos | ad2093e45299f0e977c1781287996bb171b901e1515608b2ce0327b38ebbc651 |
| **7.** | 41.59.212.4 | Unidentified | b90fbe43ac36f9acb7dca057539362bcdf311211f5db0d976ad4eaf93a36c054 |

| | | | |
|---|---|---|---|
| **8.** | 102.208.164.221 | trojan.mirai/ddos | 039910009130c76f55f7fb165f52227c1d3d3905c5abdc32b0978eaaa0ce71b6 |
| **9.** | 41.10.182.159 | trojan.abtrojan/multiverze | 062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a |
| **10.** | 93.123.109.6 | trojan.mirai/ddos | 0c77a7ed5c5dcc7828bdffada959bf0ac1180ecfd43713f203ee9d5bf429283a |

*Table 2: Top 10 Malware Samples with SHA256 Hashes*

## 04: WEB ATTACKS

A total of 26,912 web attacks were recorded, a decrease of 21.7% from last week's 34,374. 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.** | 45.148.10.238 | / |
| **2.** | 94.26.106.224 | /admin/config.php |
| **3.** | 45.138.12.51 | /favicon.ico |
| **4.** | 194.180.49.41 | /robots.txt |
| **5.** | 144.31.25.99 | /.env |
| **6.** | 144.31.25.88 | /SDK/webLanguage |
| **7.** | 213.209.159.175 | /.aws/config |
| **8.** | 77.90.185.244 | /102.207.206.92/.env |
| **9.** | 217.60.76.167 | /boaform/adminformLogout//boaform/admin/login.asp |
| **10.** | 195.178.110.48 | /.git/config |

*Table 3: Top 10 Web Attacking IPs and URI Targets*

## 05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,152,417 ICS attacks were recorded, a decrease of 30.7% from last week's 1,662,460. 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.** | 174.48.2.137 | snmp | 161 |
| **2.** | 74.109.179.39 | ipmi | 623 |
| **3.** | 71.30.240.98 | IEC104 | 2404 |
| **4.** | 76.33.215.139 | guardian_ast | 10001 |
| **5.** | 35.146.149.43 | kamstrup_protocol | 1025 |

*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.