TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 19th of January to 25th of January, 2025
Report No.: TZ-CERT/WRHP/2025/04

1. NETWORK ATTACKS

A total of **662,113** attacks have been recorded compared to last week's **416,474** 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.	194.163.150.130	root	Win1doW$
2.	218.92.0.178	admin	r00t
3.	208.109.235.47	postgres	123qwe!@#
4.	180.180.121.4	validator	abc123456
5.	194.0.234.107	superadmin	admin
6.	114.32.168.119	telnetadmin	proftpd
7.	114.35.66.183	sa	telnet
8.	75.97.22.17	ubuntu	P@ssw0rd
9.	125.229.222.137	supportadmin	adminpass
10.	125.231.226.185	oracle	validator

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 **74,363** malicious software distributed, compared to last week in which was **78,062.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan:Linux/Multiverze	72ce5b00ca4bfa0c18fcdf03a15e5391a85d81300783626598fe7e022e0ec538
2.	201.209.215.206	Trojan.Gen.NPE	0bf15aa87b7edf963533962273cd9c622b74dd1e47e770aa910fdf22ce0851df
3.	171.245.160.230	HEUR:Trojan.Linux.Miner.gen	16d20b9cf5bc20f04368d323cd4729649b1be1e0569ec263c3ddad0421c26d79

4.	202.179.76.76	Mal/Generic-S	1ef0eb60318495dd0cb100fc828f28237d487b800605c7cc54155cf34582598b
5.	122.187.213.38	Trojan:Linux/Multiverze	20e3f957446527a31ff3fd9d53b48c6046c9858d789ca043a6869cbea254bc20
6.	41.90.230.214	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	196.202.80.207	ELF/Xorddos.AB!tr	03dbf5ef3046a32f095b9ed6037a02c3b8421bdaf8d45cbe9b83e019e89ef2b7
8.	41.78.227.2	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	41.65.245.19	Trojan:Linux/CoinMiner	faf5a92e9a852b9e25c06a1885de55d50341a5b5dee4c5770eb382dee3891ef4
10.	59.48.243.18	Backdoor:Linux/Mirai!rfn	ab7bddd383d763c580e88786e6af080d72f909552e9feebc9e37e5a2ab545719

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,962** web attacks compared to last week which was **1,784.**

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

SN	ATTACKING IPS	TOP URI
1.	162.217.96.20	/
2.	193.41.206.24	/admin/config.php
3.	203.190.10.125	/favicon.ico
4.	106.13.112.250	/.env
5.	146.19.24.168	/robots.txt
6.	5.181.190.248	/logon.htm

7.	147.45.198.54	/admin/assets/js/views/login.js
8.	102.211.152.45	/1.php
9.	185.196.220.253	/admin/config.php?password%5B0%5D=ZIZO&username=admin
10.	41.78.73.146	/.well-known/security.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,071** ICS attacks compared to last week which was **2,739.**

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 January to 25th of January, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.135.161	kamstrup_protocol	1025
2.	147.182.133.8	IEC104	2404
3.	64.227.13.119	kamstrup_management_protocol	50100
4.	147.182.225.86	guardian_ast	10001
5.	207.90.244.10	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.