



## TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 10<sup>th</sup> of November, 2024 to 16<sup>th</sup> of November, 2024

Report No.: TZ-CERT/WRHP/2024/46

### 1. NETWORK ATTACKS

A total of **213,737** attacks have been recorded compared to last week's **91,894** 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.	210.245.119.111	kafka	proftpd
2.	178.162.215.169	admin	admin
3.	109.68.191.194	proftpd	qwerty
4.	149.28.62.29	ftpuser	123456
5.	104.248.120.216	mysql	p@55w0rd
6.	103.200.88.34	tech	r00t
7.	202.159.60.204	root	8888888
8.	104.238.179.4	Administrator	(empty)
9.	134.209.118.247	ubnt	1q2w3e4r
10.	155.138.205.242	centos	Win1doW\$

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 **24,748** malicious software distributed, compared to last week in which was **27,145**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.203.231.205	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	156.196.226.225	Trojan.Gen.NPE	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
3.	200.188.149.147	Adware/Miner	992cb5a753697ee2642aa390f09326fdb7fd59119053d6b1bdd35d47e62f472

4.	105.108.206.35	Application.Linux.Generic.27209	69dc9dd8065692ea262850b617c621e6c1361e9095a90b653b26e3901597f586
5.	197.2.124.210	Application.Linux.Generic.27213	29f8524562c2436f42019e0fc473bd88584234c57979c7375c1ace3648784e4b
6.	45.148.10.154	Adware/Miner	992cb5a753697ee2642aa390f09326fcd7fd59119053d6b1bdd35d47e62f472
7.	171.7.8.32	Trojan:Linux/CoinMiner	69dc9dd8065692ea262850b617c621e6c1361e9095a90b653b26e3901597f586
8.	42.114.249.76	Mal/Generic-S	6a4af8a73c08a4006dc17a7965263bb54090ac50c9a4a0bd568b80a996e8d42f
9.	177.138.241.62	Trojan:Linux/Hajime!MSR	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
10.	203.92.41.34	Backdoor:Win32/Berbew	be2942f620524ff0841a90f1e1b5dcfffb8d1875e7fb059ad914a36990195b3e

Table2: Top 10 Malicious attacking IP

### 3. WEB ATTACKS

During the week the sensors recorded a total of **4,672** web attacks compared to last week which was **4,239**.

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 10<sup>th</sup> of November to 16<sup>th</sup> of November, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	162.217.96.20	/
2.	179.43.168.146	/admin/config.php
3.	162.217.96.21	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	194.50.16.198	/login.asp
5.	158.220.120.139	/login.rsp

6.	192.99.152.209	/logon.htm
7.	91.66.164.82	/admin/assets/js/views/login.js
8.	203.190.10.118	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
9.	203.190.10.114	/recordings/index.php
10.	66.249.64.106	/cgi-bin/index.html

Table3: Top 10 web attacking IP

#### 4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,683** ICS attacks compared to last week which was **1,794**.

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 10<sup>th</sup> of November, 2024 to 16<sup>th</sup> of November, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	194.32.120.162	IEC104	2404
2.	143.244.167.115	guardian_ast	10001
3.	45.79.167.197	kamstrup_protocol	1025
4.	141.98.7.248	kamstrup_management_protocol	50100
5.	13.58.97.162	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.