



TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 22nd October to 28th of October, 2023
Report No.: TZ-CERT/WRHP/2023/43

1. NETWORK ATTACKS

A total of **14,982** attacks have been recorded compared to last week **16,337** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	193.105.134.95	root	root
2.	185.246.128.133	admin	admin
3.	170.64.165.88	(empty)	123456
4.	1.28.227.146	supervisor	1234
5.	41.78.75.186	support	(empty)
6.	112.196.2.187	guest	password
7.	41.78.73.146	Admin	Win1doW\$
8.	182.48.80.230	factory	888888
9.	180.111.65.15	user	adminHW
10.	185.11.61.234	3comcso	1234admin

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **7,053** malicious software distributed compared to last week in which was **1,743**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.86.254	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	41.59.37.63	trojan.xorddos/ddos	831854b41065f7c3fa06fa2e6001457a65d2765a0e8a04bfdd65a5aa8cef ace4
3.	89.107.112.67	trojan.generica/xorddos	b2b661ba3eb22e95b829fb35fce38a0485ca4a3a198ec5c28e6945328c212f5b

4.	202.125.143.66	Adware/Miner	286a1eebeb4b65f34f70 597d798adf6245167a16 735d1e20b45db9dd5a6 d0b69
5.	197.39.70.117	trojan.hajime/genericrxic	b39633ff1928c7f548c6a 27ef4265cfd2c3802308 96b85f432ff15c7c81903 2c
6.	220.178.1.18	ELF/Xorddos.AB!tr	ba76ffe8c2f466442077c 70ed874b2459d677cec e7d36cc71e2a8542c27f 8c2b
7.	193.118.53.91	trojan.xorddos/ddos	0291de841b47fe19557c 2c999ae131cd571eb61 782a109b9ef5b4a4944b 6e76d
8.	59.44.37.155	trojan	d7f98e379c400c133407 81ccb65017c00033082 4ea26680866b9d3e43d 641721
9.	175.19.197.49	trojan.hajime/genericrxhy	a04ac6d98ad98931278 3d4fe3456c53730b212c 79a426fb215708b6c6da a3de3
10.	185.180.143.146	trojan	d92f51db8b2df9ebac3c 18e3691eddf473e80647 42d46987077d72e570e 74b6b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **328** web attacks compared to last week which was **280**.

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 22nd October to 28th of October, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	72.251.232.180	/
2.	41.78.169.54	/users/sign_in
3.	41.78.75.186	/admin/config.php
4.	41.78.73.146	/boaform/admin/formLogin
5.	109.237.96.124	/.env
6.	121.173.126.140	/admin/config.php?password%5B0%5D=ZI

7.	165.154.174.108	/favicon.ico
8.	109.237.96.251	/a2billing/admin/Public/index.php
9.	165.232.188.105	/adcr.nhn
10.	67.217.57.54	/recordings/index.php

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

- 4.1 Note that most of 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 counter act, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.
- 4.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.
- 4.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.
- 4.4 Deploy Intrusion Detection System (IDS) and configure to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.