TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 20th of November – 26th of November, 2022
Report No.: TZ-CERT/WRHP/2022/47

1. NETWORK ATTACKS

A total of **189,131** attacks have been recorded compared to last week **218,397** 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.	27.19.192.181	oracle	123456
2.	171.225.184.215	admin	admin
3.	193.105.134.95	user	7ujMko0admin
4.	171.225.184.110	root	888888
5.	171.225.184.81	guest	abc@123
6.	195.3.147.57	ubuntu	ubuntu
7.	171.225.184.237	support	1234567890
8.	61.177.172.143	ftpuser	P@ssw0rd
9.	171.225.184.137	Administrator	support
10.	171.225.184.240	test	Win1doW$

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 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 205,828 malicious software distributed compared to last week in which was 597,788.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan Horse	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	41.59.211.41	A Variant Of Win32/TrojanDownloader.Small.AVZ	57f315b6e95f9525295b4c8e3e16718411936aeec32a3cbabb9af1817074ca70
3.	41.59.201.3	TrojWare.Win32.Ransom.WannaCry.AB@75g	c2d709eb1b8e00ececb5a0057b0b70177892ddfc297d03b2d0339671

			6505ba5e
4.	41.59.201.7	HEUR:Trojan-Downloader.Win32.Generic	0792ff784d6edc721ab513f2b4d0db5e8f8750b066419537e359b1b2ec17a1cc
5.	160.242.84.252	Trojan-Ransom.Win32.Wanna.m	4813d4e041f3d07b6b29ee77de4cba101c3e38ea9f164f2ca52f6be0ed0999f5
6.	41.59.203.192	Trojan:Linux/Multiverze	afe67c83ecb43d41edc0f321d490325c7aad4c870683c9d022109a187c2478d6
7.	41.93.47.66	Linux.Mirai	c5a75f119ab776d85abf51efca7c882d5eb911501a0e011c0218da229e79bc3e
8.	125.231.75.77	Gen:Trojan.Malware.eC5@a0JB20mi	f4ac4f735b9ff260a275734d86610dccb8558d1a54c6d6a78a94c33b6aaf6e39
9.	41.210.155.45	Trojan.Agent.CZTF	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
10.	41.41.241.22	HEUR:Trojan.Win32.Miner.b.gen	1952de4348d659fccb42e2fabfdf37874dd3f79eb8a3efa47aab69cb4c754a15

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of 4,127 web attacks compared to last week which was 2,443.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th of November – 26th of November, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	20.203.214.174	//admin/config.php
2.	72.251.235.155	/
3.	104.28.221.46	/users/sign_in
4.	141.255.166.2	/boaform/admin/formLogin

5.	41.78.169.54	/favicon.ico
6.	152.89.196.211	/.env
7.	109.237.97.141	/recordings/
8.	51.79.163.63	/admin/config.php
9.	149.56.27.16	//ajax.php?yokyok=ls
10.	196.216.92.69	/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.