TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 6th of November – 12th of November, 2022
Report No.: TZ-CERT/WRHP/2022/45

1. NETWORK ATTACKS

A total of **190,713** attacks have been recorded compared to last week **422,828** 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.	116.105.220.26	oracle	123456
2.	202.53.94.150	admin	admin
3.	179.60.147.101	user	7ujMko0admin
4.	116.110.3.13	root	root
5.	117.4.243.10	guest	abc@123
6.	193.105.134.95	ubuntu	ubuntu
7.	141.98.11.91	support	1234567890
8.	116.110.120.127	ftpuser	P@ssw0rd
9.	195.3.147.57	Administrator	support
10.	167.172.82.33	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 **734,371** malicious software distributed compared to last week in which was **1,631,722**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan Horse	4d8b0e13e06f626fd1902066d31651986d90f26fa7d2882042a29446ce205cf0
2.	41.78.173.77	A Variant Of Win32/TrojanDownloader.Small.AVZ	6a3e07572488ae5458e54eb5ecc1975b73e809eb608b646db16f72e0f0be46ef
3.	41.78.64.254	TrojWare.Win32.Ransom.WannaCry.AB@75g	8a972c7f6fcd9ebd02b695a0c49daa383538cf077ef182da3bf1f760212

			ca259
4.	178.204.248.195	HEUR:Trojan-Downloader.Win32.Generic	e03f2685cec2f85f8394d2d2b478416860fa5f093a56e326bc1076a7762fe679
5.	41.59.201.7	Trojan-Ransom.Win32.Wanna.m	71ef590b32ef90a021be7bafd074b7698ffefab7f935e371568bef5eb2543f19
6.	41.59.211.41	Trojan:Linux/Multiverze	67296512900d96d96fd7c01cb36a0beb6c4f0e420599306d76b545af14dce31b
7.	41.59.201.3	Linux.Mirai	2c34a1647db1663e54e771b7c86161e3946e5aee922750064d3a43cd0717adf9
8.	197.230.127.92	Gen:Trojan.Malware.eC5@a0JB20mi	0db4f8ea9c2fd15a3fa176534bacb8507660f7d0944fa1f11e889410e6585337
9.	117.4.80.165	Trojan.Agent.CZTF	cf24468309418e6cb31f2278583c374056206463ec1fd31b7409201a9e41fa27
10.	212.179.100.52	HEUR:Trojan.Win32.Miner.b.gen	f34467ae1bb6802a641095d5b4a179c80f2af7f05f73d97145b0a13866684920

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,949** web attacks compared to last week which was **3,302**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 6th of November – 12th of November, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URL
1.	35.204.82.246	/
2.	114.35.183.25	/users/sign_in
3.	45.95.147.40	/favicon.ico
4.	41.78.169.54	/robots.txt

5.	51.75.194.66	/.env
6.	13.76.252.159	/adcr.nhn
7.	121.173.126.140	/_asterisk/graph.php
8.	152.89.196.211	/boaform/admin/formLogin
9.	95.182.121.73	/actuator/gateway/routes
10.	183.136.225.32	/admin/config.php?password%5B0%5D=ZIZO&username=admin

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.