



## TZ-CERT HONEYPOTS WEEKLY REPORT

Period : 21<sup>st</sup> of August – 27<sup>th</sup> of August, 2022

Report No.: TZ-CERT/WRHP/2022/34

### 1. NETWORK ATTACKS

A total of **166,911** attacks have been recorded compared to last week **145,976** 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.	161.97.118.100	nproc	nproc
2.	150.230.253.138	admin	admin
3.	111.225.217.34	user	P@ssword1
4.	185.240.246.114	root	root
5.	116.98.168.66	test	Test1234
6.	78.46.46.131	ubuntu	ubuntu
7.	116.98.171.250	support	123456
8.	78.47.166.111	admin1234	password
9.	179.60.147.161	Postgres	abc123
10.	95.214.24.192	oracle	oracle

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 **1,310,483** malicious software distributed compared to last week in which was **1,556,674**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	64.95.101.10	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	197.250.198.6	A Variant Of Win32/TrojanDownloader.Small.AVZ	ae12bb54af31227017feffd9598a6f5e
3.	119.93.116.253	TrojWare.Win32.Ransom.WannaCry.AB@75g	7107326e81d955aff29f49487aa3da23
4.	190.23.219.68	HEUR:Trojan-Downloader.Win32.Generic	0ab2aeda90221832167e5127332dd702

5.	41.59.89.218	Trojan-Ransom.Win32.Wanna.m	414a3594e4a822cfb97a4326e185f620
6.	121.122.97.187	Trojan-Ransom.Win32.Wanna.m	996c2b2ca30180129c69352a3a3515e4
7.	83.69.141.105	Trojan-Ransom.Win32.Wanna.m	a55b9addb2447db1882a3ae995a70151
8.	46.100.60.176	Gen:Trojan.Malware.eC5@a0JB20mi	e9d1ba0ee54fcdf37cf458cd3209c9f3
9.	212.220.45.5	Trojan.Agent.CZTF	beb68e9c7ef18f421df8230c032fe02a
10.	42.157.129.157	HEUR:Trojan.Win32.Miner.b.gen	cd99e5e4f44621978faf8df0e01d2d2b

Table2: Top 10 Malicious attacking IP

### 3. WEB ATTACKS

During the week the sensors recorded a total of **81** web attacks compared to last week which was **1,285**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 21<sup>st</sup> of August – 27<sup>th</sup> of August, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	13.244.117.62	/jenkins/login
2.	13.245.14.40	/login
3.	51.83.75.133	/manager/html
4.	135.125.239.88	/secure/ContactAdministrators!default.jspa
5.	188.68.61.6	/boaform/admin/formLogin?username=admin&psd=admin
6.	159.223.26.31	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	106.75.2.164	/config/getuser?index=0
8.	106.75.4.49	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	121.123.25.106	/hudson
10.	139.87.71.160	/favicon.ico

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.