TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 25th of September – 1st of October, 2022
Report No.: TZ-CERT/WRHP/2022/39

1. NETWORK ATTACKS

A total of **252,076** attacks have been recorded compared to last week **126,427** 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.	78.47.166.111	nproc	nproc
2.	116.105.213.130	admin	admin
3.	78.46.46.131	user	54321
4.	116.98.167.113	root	root
5.	116.105.215.71	Administrator	12345
6.	116.110.105.4	ubuntu	ubuntu
7.	92.255.85.113	support	1234567890
8.	41.78.174.77	supervisor	password
9.	116.110.94.190	ftpuser	support
10.	171.251.30.144	guest	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 **1,131,916** malicious software distributed compared to last week in which was **39,428**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.173.77	Trojan Horse	7107326e81d955aff29f49487aa3da23
2.	41.78.64.254	A Variant Of Win32/TrojanDownloader.Small.AVZ	685bc2af410d86a742b59b96d116a7d9
3.	41.78.76.190	TrojWare.Win32.Ransom.WannaCry.AB@75g	235e9af4c6f5b5de7d30d0589bbcff14
4.	41.78.102.150	HEUR:Trojan-Downloader.Win32.Generic	ae12bb54af31227017feffd9598a6f5e

5.	74.116.0.114	Trojan-Ransom.Win32.Wanna.m	02c5f1515bf42798728fac17bfe1e4c1
6.	104.152.52.183	Trojan-Ransom.Win32.Wanna.m	2ef7aaa6d2d73813b0b509a9c1abca66
7.	118.100.11.31	Trojan-Ransom.Win32.Wanna.m	996c2b2ca30180129c69352a3a3515e4
8.	41.59.217.115	Gen:Trojan.Malware.eC5@a0JB20mi	c2b8b099bb55f52e094d22266b6d7b34
9.	41.59.192.77	Trojan.Agent.CZTF	0129086ae5fa2269d1037ff0ac0fca48
10.	41.59.89.218	HEUR:Trojan.Win32.Miner.b.gen	3062df26ec61ca773e8c7cd487322562

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,761** web attacks compared to last week which was **10**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 25th of September – 1st of October, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	20.39.250.47	/jenkins/login
2.	117.187.173.3	/login
3.	41.78.174.124	/manager/html
4.	41.78.174.77	/secure/ContactAdministrators!default.jspa
5.	41.78.73.121	/boaform/admin/formLogin?username=admin&psd=admin
6.	95.182.123.66	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	183.136.225.35	/config/getuser?index=0
8.	92.118.39.44	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	41.78.169.54	/hudson
10.	109.237.96.124	/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.