TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 16th of October – 22nd of October, 2022
Report No.: TZ-CERT/WRHP/2022/42

1. NETWORK ATTACKS

A total of **345,376** attacks have been recorded compared to last week **504,033** 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.	116.110.89.182	nproc	12345678
2.	185.216.71.81	admin	admin
3.	171.251.17.13	user	7ujMko0admin
4.	116.98.171.58	root	root
5.	116.110.102.229	guest	123456
6.	167.99.201.100	ubuntu	ubuntu
7.	179.60.147.99	support	1234567890
8.	61.177.173.21	supervisor	password
9.	171.251.22.81	User-Agent: python-requests/2.27.1	support
10.	193.105.134.95	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 **1,307,701** malicious software distributed compared to last week in which was **2,103,621**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan Horse	71ef590b32ef90a021be7bafd074b7698ffefab7f935e371568bef5eb2543f19
2.	41.78.173.77	A Variant Of Win32/TrojanDownloader.Small.AVZ	ae6d308fae42abc06ec22ba816c3b8e1edf59be08d454362416effc726b31cee
3.	41.78.76.190	TrojWare.Win32.Ransom.WannaCry.AB@75g	3b0285d601232ddee79a28f3923462f3e4f8c6

			cedb809377ed0da07ba06b651e
4.	41.93.47.66	HEUR:Trojan-Downloader.Win32.Generic	0db4f8ea9c2fd15a3fa176534bacb8507660f7d0944fa1f11e889410e6585337
5.	41.78.109.1	Trojan-Ransom.Win32.Wanna.m	b4e5e3e5ea11e333b57d97cbcef17847efd122443c8f7bc1c9aec0c84044bc4d
6.	41.59.87.166	Trojan:Linux/Multiverze	9a252ddabf3920295bb1db2a17085a58a8fd647793424167d6cd04318acc7bf6
7.	41.59.211.41	Linux.Mirai	c2d709eb1b8e00ececb5a0057b0b70177892ddfc297d03b2d03396716505ba5e
8.	81.171.20.43	Gen:Trojan.Malware.eC5@a0JB20mi	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
9.	196.41.222.5	Trojan.Agent.CZTF	0129086ae5fa2269d1037ff0ac0fca48
10.	41.175.24.90	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 **5,468** web attacks compared to last week which was **8,000**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of October – 22nd of October, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	51.103.219.37	/jenkins/login
2.	45.95.147.40	/login
3.	103.165.36.238	/manager/html
4.	69.247.251.32	/secure/ContactAdministrators!default.jspa
5.	89.247.41.175	/boaform/admin/formLogin?username=admin&psd=admin
6.	31.49.232.33	/boaform/admin/formLogin?username=adminisp&psd=adminisp

7.	102.113.233.23	/config/getuser?index=0
8.	109.15.243.214	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	190.5.136.170	/hudson
10.	75.112.188.210	/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.