TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 14th of November – 21st of November, 2021
Report No.: TZ-CERT/WRHP/2021/47

1. NETWORK ATTACKS

A total of **99,417** attacks have been recorded compared to last week **457,394** 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.	5.188.62.194	admin	Admin1
2.	5.188.62.196	guest	guest123
3.	116.110.121.105	nproc	nproc
4.	116.110.148.32	ftp	password
5.	41.74.113.50	test	test123456
6.	200.52.80.34	user	damn123$%adsa#%aFasaaaaaa
7.	116.98.171.28	ftpuser	password
8.	116.110.84.208	hadoop	1234qwer
9.	116.110.252.176	support	1qaz2wsx
10.	117.7.122.163	knockknockwhosthere	knockknockwhosthere

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 **631,440** malicious software distributed compared to last week in which was **470,045**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	185.53.90.111	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	146.0.42.94	A Variant Of Win32/TrojanDownloader.Sm	02c5f1515bf42798728fac17bfe1e4c1
3.	62.210.178.249	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	60.177.17.240	HEUR:Backdoor.Win32.Agent.gen	0ab2aeda90221832167e5127332dd702

5.	47.107.60.190	Trojan.Agent.CZTF	414a3594e4a822cfb97a4326e185f620
6.	103.234.54.92	Win32.Worm.Downadup.Gen	7bb455ea4a77b24478fba4de145115eb
7.	39.98.148.224	Ransom.Wannacry	02c5f1515bf42798728fac17bfe1e4c1
8.	213.202.233.100	Win32/Exploit.CVE-2017-0147.A	8c3ac09b90b14e6ab2ecce1bb4e475b0
9.	41.78.108.162	TrojWare.Win32.Ransom.WannaCry.AB@75g	a55b9addb2447db1882a3ae995a70151
10.	200.69.227.153	TrojWare.Win32.Cloxer.DRI@7nqo1u	beb68e9c7ef18f421df8230c032fe02a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,636** web attacks compared to last week which was **16,626**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 14th November and 21st of November, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	188.143.232.14	/jenkins/login
2.	194.26.74.7	/login
3.	20.119.67.74	/manager/html
4.	20.85.233.192	/secure/ContactAdministrators!default.jspa
5.	104.156.239.114	/boaform/admin/formLogin?username=admin&psd=admin
6.	173.245.209.106	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	20.120.115.3	/config/getuser?index=0
8.	40.85.101.152	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	154.3.251.102	/hudson
10.	52.232.70.110	/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.