TZ-CERT HONEYPOTS WEEKLY REPORT
**Period : **13th of February – 19th of February, 2022
Report No.: TZ-CERT/WRHP/2022/8

1. NETWORK ATTACKS

A total **379,327** of attacks have been recorded compared to last week **599,377** 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.	116.105.212.31	admin	12345
2.	5.188.62.194	nproc	nproc
3.	185.246.130.20	111111	super
4.	116.110.3.253	guest	guest123
5.	116.105.216.128	test	querty
6.	220.74.113.235	user	000000
7.	5.188.62.196	ftpuser	password
8.	201.160.57.3	hadoop	123456qwerty
9.	195.3.147.76	support	0987654321
10.	189.217.193.9	MikroTik	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 **359,221** malicious software distributed compared to last week in which was **90,418**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	212.156.115.145	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	82.157.148.23	Trojan.SQLMap.Linux.2	844290834b6450425b146d4517cdf780
3.	47.108.222.53	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	61.19.254.107	Trojan.Agent.CZTF (B)	996c2b2ca30180129c69352a3a3515e4
5.	47.109.16.215	Trojan.Win32.Reconyc.fuzv	ab27f6c7634e9efc13fb2db29216a0a8

6.	47.108.206.67	Trojan-Ransom.Win32.Wanna.m	0ab2aeda90221832167e5127332dd702
7.	1.215.138.43	Ransom.Wannacry	414a3594e4a822cfb97a4326e185f620
8.	189.252.207.51	Gen:Trojan.Malware.pq0@a0R9t5ej	b1adcaff8310318296362f49154f9e41
9.	195.174.236.233	Win32/TrojanDownloader.Agent.DRI	70ccd9220cebb56eaa38b9f1bd1a1cd8
10.	134.195.196.23	Trojan-Ransom.Win32.Wanna.m	a55b9addb2447db1882a3ae995a70151

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **6,096** web attacks compared to last week which was **5,413**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 13th of February – 19th of February, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	20.186.176.159	/jenkins/login
2.	50.67.186.176	/login
3.	70.39.92.7	/manager/html
4.	188.215.235.107	/secure/ContactAdministrators!default.jspa
5.	104.254.247.159	/boaform/admin/formLogin?username=admin&psd=admin
6.	85.187.123.30	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	82.145.56.103	/config/getuser?index=0
8.	95.181.239.9	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	82.145.56.102	/hudson
10.	20.114.181.21	/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.