TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 29th of May – 04th of June, 2022
Report No.: TZ-CERT/WRHP/2022/22

1. NETWORK ATTACKS

A total of **295,040** attacks have been recorded compared to last week **253,611** 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.	178.62.96.205	admin	123456
2.	129.205.102.242	nproc	nproc
3.	5.188.62.194	user	1
4.	206.189.206.35	test	test
5.	116.98.162.249	111111	$passwo
6.	195.3.147.76	guest	guest
7.	116.98.166.170	ftpuser	ftpuser
8.	171.251.17.49	ftp	ftp
9.	5.188.62.250	support	support
10.	5.188.62.196	123321	111111

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 **18,685** malicious software distributed compared to last week in which was **63,898**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	89.248.165.57	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	41.59.199.207	Linux/SQLMap	283944e9dde24d58244006583be8420b
3.	41.59.217.115	TrojWare.Win32.Ransom.WannaCry.AB@75g	5265fc3146b7e3922c79ef463aaecd16
4.	104.200.131.248	Linux/SQLMap	63d99eb9dbb58306cbb3a9b7e2ecfb27
5.	41.59.4.53	Trojan.Win32.Reconyc.fuzv	683cb6978d059a237b3f679f6006e866
6.	41.59.192.77	Trojan-	6e72ad805b4322612b

		Ransom.Win32.Wanna.m	9c9c7673a45635
7.	45.143.203.15	Ransom.Wannacry	8d776bb95c43be7ffd5eadc85ee291a0
8.	119.152.240.47	Dropped:Generic.Malware.F!dld!.0204478	996c2b2ca30180129c69352a3a3515e4
9.	120.124.34.112	Trojan.Win32.Swisyn.fsyi	9ba5379aa41d707a4331d27a004baec1
10.	64.188.30.6	Trojan.Agent.CZTF	a1c2199d384764282210050b2975910e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **80,334** web attacks compared to last week which was **30,993**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 29th of May – 04th of June, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	5.188.211.72	/jenkins/login
2.	5.188.211.21	/login
3.	5.188.211.13	/manager/html
4.	5.188.211.16	/secure/ContactAdministrators!default.jspa
5.	5.188.211.10	/boaform/admin/formLogin?username=admin&psd=admin
6.	5.188.211.26	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	5.188.211.15	/config/getuser?index=0
8.	5.188.211.35	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	5.188.211.22	/hudson
10.	52.187.176.210	/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.