TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 25th of April– 02nd of May, 2020
Report No. : TZ-CERT/WRHP/2020/17

1. NETWORK ATTACKS

A total of **51,254** attacks have been recorded compared to last week **85,356** 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.	5.188.62.13	nproc	nproc
2.	45.227.255.207	admin	123456
3.	5.188.86.178	odoo	123
4.	5.188.86.212	git	password
5.	5.188.86.206	guest	123123
6.	5.188.87.58	hadoop	pass
7.	45.227.255.206	test	passw0rd
8.	5.188.87.60	user	p@ssw0rd
9.	5.188.86.165	oracle	P@ssw0rd
10.	5.188.86.164	ubuntu	123456789

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 **123,144** malicious software distributed compared to last week in which was **945,748**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	49.88.112.69	BehavesLike.Win32.RansomWannaCry.th	996c2b2ca30180129c69352a3a3515e4
2.	222.186.180.130	Trojan-Ransom.Win32.Wanna.m	37a3ca268f5d7379fcb5268296336771
3.	222.186.175.23	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a
4.	103.116.248.121	HEUR:Trojan.Win32.Miner.b.gen	685bc2af410d86a742b59b96d116a7d9
5.	206.189.218.172	HEUR:Trojan-	d3d550e38c82dc47192363dc3cf

		Downloader.Win32.Generic	7e9da
6.	167.99.194.147	Trojan Horse	dede6d1500af444a9f4d67bf9fcc6088
7.	202.78.227.164	HEUR:Trojan-Downloader.Win32.Genome.	64f62894e7b8f7574cb8ccea414d768f
8.	190.37.10.36	TrojanDownloader:Win32/Small.gen!B	235e9af4c6f5b5de7d30d0589bbcff14
9.	118.201.196.75	HEUR:Trojan-Downloader.Win32.Generic	02c5f1515bf42798728fac17bfe1e4c1
10.	212.142.154.71	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,472** web attacks compared to last week which was **1,329**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 25th of April and 02nd of May, 2020 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	140.238.42.16	/servlet/gs/explorer.cfm
2.	66.249.64.113	/perl/control/click.php
3.	66.249.66.131	/axis-cgi/editor/campas
4.	106.13.133.229	/perl/ovcgi/wais.pl
5.	189.151.203.204	/admin-manager/admin.jsp
6.	185.84.174.225	scripts/iisadmin/mailto.cgi
7.	66.249.66.129	/perl/control/john.pot
8.	185.176.27.114	/perl/ovcgi/global.cgi
9.	139.162.79.87	/servlet/suse/AT-admin.cgi
10.	121.201.34.11	/scripts/iisadmin/webgais

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.