Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.: 154 **01-08-2022**

Name: Early Warning & High Alert – Prevention against Hacking attempts on National Days (14th Aug, 6th Sep 2022)

Threat Classification: Phishing Emails, Hacking, Defacement, Denial of Service (DoS)

Context:

This cyber threat advisory is being shared in light of the security intelligence collected from the evidence available from private and public sources. All Telecom licensees are notified through an early warning to take the necessary steps to prevent and minimize the impact of cyber-attacks, espionage, and sabotage. Various hostile elements, launch offensive operations to cripple the critical services and infrastructure of Pakistan. 2017-2021 Trend analysis shows a high frequency of reported hacking and defacement activity on official websites including government and ministries allegedly by Indian hackers.

Implications of Cyber-Attacks on National Day:

Hackers perform malicious activities on National Days i.e. Independence Day, Defense day, and similar national events, having serious consequences.

Details are as under:

1. Display of anti-state content on national websites (Website hacking, defacement)
2. Unavailability of online services (Denial of Service attack).
3. Breach and loss of critical or sensitive national data (Exfiltration)

Applicability of Advisory:

This advisory is applicable to all PTA licensees which are managing the following:

1. Website(s) hosted commercially or self-managed company's own website(s)
2. Publicly exposed Portal(s)
3. Publicly exposed APIs / Webservices
4. Or any other publicly exposed IT Services

Remedial Measures:

For Immediate Actions:

Sr. No	Actions
1	Whitelist IP addresses where the admin panel is accessible
2	Implement secure login sessions.
3	Do not save configuration files in public folders. Store in an encrypted format
4	Avoid tempting or threatening content in the email
5	Be careful with attachments especially with executable extensions like .exe, .msi, .vb, .bat etc
6	Don't click on unknown links in emails. These can be malicious

7	Disable unnecessary services, ports, protocols, modules, and anonymous accounts
8	Disable remote access to Database Servers
9	Enable fraud warning features where available
10	Input sanitization on public-facing/internet-exposed websites and services
11	Disable server-info and signatures
12	Do not run web servers as 'root'
13	Inspect passphrases for use of any weak or default log-in credentials
14	Assign minimal privileges on administrator accounts, multifactor authentication, and defined authorization procedures
15	Install, enable, and update Web Application Firewall (WAF) and Anti-DDoS protection; ensure control properly functioning for on-time and automated detection and prevention.
16	Inspect the contents and latest back-ups of the public-facing/internet-exposed site and services for hidden malware and vulnerabilities. Remove all critical vulnerabilities.
17	Ensure 24/7 security monitoring of critical infrastructure, services, and websites for proactive remediation and response to any detected/observed abnormal activity.
18	Update CMS, and webservers with the latest plugins, releases, and security patches
19	Identify the point of contact (and a backup) for incident response.
20	Contact the vendor/third party/service provider, to ensure appropriate security measures and report any abnormal activities if you have hosted a website on their platforms.

For Best Practices:

Sr. No	Actions
1	Follow secure code development and maintenance practices for public exposed websites and services.
2	Properly harden all public exposed websites and services.
3	Properly harden all Firewalls, routers, switches, and network nodes.
4	Properly harden DNS and Email services.
5	Train employees on phishing, social engineering and incident response procedures
6	Update Plug-ins to fix bugs, patch security issues, and install updates on web servers.
7	Schedule regular back-ups of database
8	If any malicious activity is found immediately inform PTA through the CERT portal.

In case of an Incident:

Sr. No	Actions
1	Replace the website with a maintenance page immediately
2	Inform relevant parties of the incident (e.g. regulator, management, customers etc.)
3	Make a statement to the public to preserve your organization's reputation.
4	Restore your website with backups to ensure a quick recovery.
5	Report the incident to law enforcement authorities.
6	Have technical support and RCA (root cause analysis) of the incident to analyze how the website was defaced and evaluate the process of response (e.g. to improve for any future complications).

Recommendations:

1	Strictly follow all mitigation measures mentioned above.
2	Perform vulnerability assessment and penetration testing of websites and exposed services and remediate the identified vulnerabilities and weaknesses at the earliest.
3	Employ trained and dedicated resources for critical services and data protection.
4	Report suspicious email addresses to your respective organizations
5	If any malicious activity is found immediately inform PTA through the CERT portal or email at cert@pta.gov.pk