2003 (NTISB-II)

Islamabad 25 May, 2021

26 MAY 2021

Subject: - **Advisory – Ransowmare Attacks (Advisory No.36)**

M(Admin/HR)

M(I.T)

A.S(Rev. Div.)

1. Recently, malicious cyber actors deployed **Dark Side ransomware** against a US pipeline company ICT network that heavily crippled country's gasoline supply. Consequently, a **state of emergency in 18x USA states** was declared. Cyber threat actors also **stole 100 GB of data** and leaked it online even after an amount of USD 5M was paid as ransom. In light of this devastating attack, an advisory is attached at **Annexure-A** to sensitize all concerned.

2. Forwarded for information and dissemination to all concerned, please.

Annex-A

Subject: **Advisory - Ransomware Attacks (Advisory No. 36)**

1 **Introduction.** Recently, malicious cyber actors deployed **Dark Side ransomware** against a US pipeline company ICT network that heavily crippled country's gasoline supply. Consequently, a **state of emergency in 18x USA states** was declared. Cyber threat actors also **stole 100 GB of data** and leaked it online even after an amount of USD 54 was paid as ransom. In light of this devastating attack, it is urged that network / system administrators of critical organizations must follow recommendations mentioned in **para 3** to prevent against the ransomware attacks.

2. **Technical Details**

a. **Attack Vectors.** Cyber threat actors used attack vectors such as Phishing Emails, Remote Desktop Protocol **(RDP)** and Known Vulnerability exploitation.

b. **Attack Tools, Tactics & Procedures (TTPs).** Following TTPs were used:-

(1) **PowerShell:** for **reconnaissance** and **persistence**

(2) **Metasploit Framework:** for reconnaissance

(3) **Mimikatz:** for reconnaissance

(4) **BloodHound:** for reconnaissance

(5) **Cobalt Strike:** for installation

(6) **7-Zip:** a utility used for **archiving files** for exfiltration

(7) **Rclone** and **Mega client: tools** used for exfiltrating files to cloud storage

(8) **PuTTy:** an application used for network file transfer.

c. **Mode of Operation**

(1) After gaining access; DarkSide actors deployed DarkSide ransomware to **encrypt** and **steal sensitive data.**

(2) The actors then threaten to publicly release 100GB of data if the ransom is not Paid.

(3) Even after ransom of 5 million dollars was paid, the attackers did not provide the decryption key and leaked the data.

3. **Recommendations**

a. **System / Network Administrators.** In order to prevent from ransomware attack, **application whitelisting** is the **key** and must be applied at all endpoints along with following additional measures:-

(1) Windows commands / utilities not required by end-users such as like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe,cipher.exe and syskey.exe **should be blacklisted for endpoint execution.**

(2) **Block execution of scripts** having extension .vbs, .vbe, .hta, tjs, .wsh, .wsf, com, .pif, .psi extensions.

(3) **Blacklist / block outbound network connections** from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, lmshta.exe, excel.exe and eqnedt32.exe.

(4) Block execution of powershell and command prompt, if explicitly not required by the endpoint.

(5) Centralized **monitoring of endpoint windows logs** must be performed to detect anomalous user behavior.

(6) Cyber threat actors may continue to innovate new techniques, launch new attacks and create new strains of crypto -malware. Therefore, it is essential to have **access to reputable threat intelligence feeds**.

(7) Always implement multi-factor authentication for remote network access via VPN service.

(8) Regularly **update antimalware solutions running on endpoints** in enterprise environment as well as standalone systems.

(9) Educate endusers regarding cyber security best practices and antimalware measures.

(10) Ensure that data backups are regularly taken and duly verified.

b **End-users**

(1) **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

(2) **Do not download attachments from emails or websites unless you are sure about the source.**

(3) Avoid downloading software from untrusted websites or torrents.

(4) Use Chrome / Firefox browsers for surfing internet instead of Internet Explorer.

(5) Make sure that web browser is up-to-date and no plugins other than adblock or adblock plus are enabled.

4. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

asntisb2@cabinet.gov.pk

5. Forwarded for information and dissemination to all concerned, please.

* * * * *

31 MAY 2021

M(IT)

AS(RD)

Subject: - **CRITICAL VULNERABILITIES AND BREACHES IN WEBSITES / IT INFRASTRUCTURES OF GOVERNMENT MINISTRY / DIVISION / ORGANIZATIONS / DEPARTMENTS.**

Of late, critical vulnerabilities have been identified in the websites / IT infrastructures of numerous Government Ministries / Divisions / Organizations / Departments. Cyber probe of these websites / networks revealed that no IT / cyber security measures were in place at the network / infrastructure level in these organizations / departments. In order to patch the vulnerabilities various advisories have been issued by NTISB on regular basis. Beside taking various active security measures to protect our IT security networks, a need was also felt to educate / sensitize senior government officers holding sensitive portfolios and dealing with the National Security matters on issues relating to Cyber Security. To this end, a presentation on Cyber Security issues was delivered to all **Federal Secretaries** by **Director Generai ISi** on **3rd Feb 2021** and on **11th Mar 2021**.

2. Recently a sharp rise in hostile cyber espionage operation is again observed. It is pertinent to highlight that several advisories and guidelines on the subject have already been issued to Government Ministries / Departments over the period of time, but the suggested cyber security measures are still not being observed by these Government Ministries / Departments which has resulted in leakage of sensitive information.

3. Keeping in view these cyber espionage operations by the Hostile Intelligence Agencies (HIAs), there is a need to take stringent measures at every Ministry / Division / Department level by the relevant stake holders to curb the tendency of frequent breaches / vulnerabilities. Therefore, following measures are required to be adopted by all concerned: -

68227-R

a. Every Ministry / Division / Department to nominate a **Cyber Security Officer (CSO)** (using existing IT resources) who will be responsible for

CSO

Cont'd.....P/2

ensuring Computer Network / Data System protection and implementation of Cyber Security best practices. Particulars of CSO be shared with NTISB, Cabinet Division by 15 June, 2021.

b. Every Ministry / Division / Department to formulate their own Cyber Security Policy and the same be shared with NTISB, Cabinet Division, for necessary vetting before implementation by 15 June, 2021. Necessary guidelines are attached at **Annexure - A**.

c. In the light of para-16 of Internet & E-mail Policy, approved by the Prime Minister of Pakistan, it is required that 1st party cyber security audit be carried out by respective Ministries / Divisions / Departments and audit report be shared with NTISB, Cabinet Division by 1 July, 2021.

d. Punitive actions be taken against the violators as per rules by all concerned.

4. Forwarded for compliance, please.

Annex-A

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

GENERAL GUIDELINES FOR PROTECTION AGAINST CYBER ATTACKS

1. **System / Network Administrators**

a. All the IT systems must be properly hardened at hardware, software and operating system level.

b. All those Windows commands / utilities not required by the end-users should be blocked for endpoint execution like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe.

c. Block execution of scripts with .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif, .ps1 extensions.

d. Blacklist / Block outbound network connections from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.

e. Centralized monitoring of end-point Windows logs must be performed to detect anomalous user behavior.

e. Regularly update anti-malware solutions running on endpoints in enterprise environment as well as stand-alone systems.

g. Educate end-users regarding cyber security best practices and antimalware measures.

h. All email attachments be opened on offline system instead of online systems.

i. Moreover, all attachments sent over email must be password protected and password be shard through an alternative medium.

j. Regularly monitor that aforesaid practices are being followed and conduct surprise checks to ensure that cyber security practices are being followed by the end-users.

2. **Internet Users**

a. Never store official email account's usernames and passwords in the browsers.

b. Do not open spoofed subject emails and mark these as spam.

c. Never click / login to unknown URLs received in the email.

Cont'd.....P/2

d. Install reputed and updated antivirus such as Kaspersky that can block known phishing sites.

e. Enable **Two Factor Authentication** on all personal / official email accounts including WhatsApp, Facebook, Instagram and Twitter accounts (especially those linked with social media sites and internet banking).

f. Use reputed browsers like Chrome, Firefox and do not install unnecessary browser plugins / addons except adblock / adblock plus.

g. Do not click on popups and ads displayed during web surfing.

3. **Online Video Conferences.** In COVID Pandemic, office work has become dependent on the use of video conferencing / online collaboration tools such as Zoom, Zoho, Slack and Google Meet etc. Hackers are exploiting this lucrative opportunity to target government departments to extract sensitive data. In this regard, following best practices are recommended: -

a. Do not use online meeting / video conferencing tools for sharing classified information.

b. Use multi-layered and potentially multi-vendor solution as this approach makes it harder for an attacker to penetrate the network.

c. Keep the video conferencing systems and operational systems updated with latest versions of all relevant service packs and security updates.

d. Disable non-essential operating system services / ports.

e. Use a firewall to prevent an unauthorized network traffic.

f. Disable auto-answer to calls in virtual meeting rooms (video conferencing system). Configure call control system to reject unauthorized calls.

g. Enable strong authentication / encryption at audio and video clients.

h. Enable PIN code protection on Virtual Meeting Rooms by using distinct lengthy, unique and randomly generated PIN for each Virtual Meeting Room. Regularly change PIN code of each Virtual Meeting Room.

i. Enable **"Waiting Room"** feature so that host can exercise better control over participants. All participants to join virtual "Waiting Room", after permission by the host.

j. Restrict / disable file transfer, call record feature and limit screen sharing.

4. **Website Management**

a. Upgrade OS and webserver to latest version.

b. Website admin panel should only be accessible via white-listed IPs.

Cont'd.....P/3

c. Defend your website against DQL injection attacks by using input validation technique.

d. Complete analysis arid penetration testing of application be carried out to identify potential threats.

e. Complete website be deployed on inland servers including database and web infrastructure.

f. HTTPS protocol be used for communication between client and web server.

g. Application and database be installed on different machines with proper security hardening.

h. Sensitive data be stored in encrypted from with no direct public access.

i. DB users privileges be minimized and limited access be granted inside programming code.

j. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.

k. Updated Antivirus tools / Firewalls be used on both endpoints and servers to safeguard from potential threats.

l. Enforce a strong password usage policy.

m. Remote management services like RDP and SSH must be disabled in production environment.

n. Deploy web application firewalls for protection against web attacks.

o. Employ secure coding practices such as parameterized queries and proper input sanitization and validation to remove malicious scripts.

p. Avoid using insecure methods like print stack trace in production environment which can disclose important information.

q. Keep system and network devices up to date.

r. Log retention policy, must be devised for at least 3x months on separate device, for attacker's reconnaissance.

*****

Network Security Audit

16. For Network Security audit purposes a three-layered Network Security Audit approach will be adopted.

a. First Layer. Mainly consisting of System Administrators/Network Administrators and Coordinator at Ministries/Divisions and System /Network Administrators and security specialists at Data Centre, will be responsible to ensure correct and secure handling of systems as well as correct implementation of guidelines/instructions on the subject.

b. Second Layer. A technical audit of the System/Network Infrastructure of each Government Organization will be carried out periodically by a technical committee constituted by Cabinet Division having members as under as a second Network Security Audit layer:

Cabinet Division (NTISB)	- Permanent
IT & T Division (EGD)	- Permanent
Agency Concerned	- (Depending upon the concerned Organization)

The committee will carry out the implementation of above mentioned policy guidelines with respect to following: -

i. Systems/Networks Architecture.
ii. Vulnerabilities of licensed and customized applications.
iii. Implementation of instruction issued from time to time.

c. Third Layer. IT&T Division will establish a specialized/certified *Federal Network Security Audit Cell* in consultation with Cabinet Division (NTISB) comprising experts from Government officials and hired local experts (as and when required). This cell will carry out the detailed Network Security Audit (when instituted) in accordance with the guidelines/standards developed for the purpose and act as a third layer for Network Security Audit.

Violation of these instructions can lead to withdrawal or suspension of right to use systems / networks privileges, and necessary disciplinary action will be taken against defaulter as per laws and regulations in vogue.