No. 19-78/2019-SA
Government of India
Ministry of Communications
Department of Telecommunications
Sanchar Bhawan, 20, Ashok Road
New Delhi-110 001
(Security Assurance Wing)

Dated: 08.07.2020

Subject: **Best Practices – Cyber Security**

A cyber attack occurs if a threat successfully breaches security controls. Evidence shows that cyber attacks are growing in sophistication, frequency and gravity. Our ever-growing reliance upon Internet places our organisations and individual users at the risk. In most of the cyber-attacks, the cyber threat actors use spear-phishing emails to deliver the malware on to the victims' computers. Thus we need to understand the tactics of the cyber threat actors and urgently secure the internet connected systems (computers/tablets/smartphones) both at organization as well as the user end to prevent any breach.

2. Some of the very common tactics, techniques and procedures adopted by cyber threat actors to compromise the computers are as follows:

2.1 Spear phishing mail

Email from known contacts or sources (either by compromised accounts or through spoofed IDs) are sent to specific users on subject relevant to the recipient. These email usually contain malicious links or attachments. Once the recipient opens the link or attachment, Crimson RAT (Remote Access Trojan) malware embedded in MS Office documents install and steal information from the victim computers. Currently, these actors are using Covid-19 themed spear-phishing emails to deliver the malware on to the victims' computers.

2.2 Evading the traffic analysis

Backdoor, which is delivered via a weaponised document from spear phishing email, is being used to steal sensitive information from the victim's computer. To communicate with the Commaed& Control Server, the malware would exfiltrate data (using standard Windows component "Background Intelligent Transfer Services-BITS) utilising small network bandwidth to avoid detection from traffic bandwidth analysis.

2.3 Exploiting web application vulnerabilities

Cyber threat actors are exploiting the prevailing vulnerabilities in the websites of organizations to steal data, which are meant only for authorized and authenticated users. Further, such vulnerable websites are used for lateral entry for identifying sensitive systems and to carry out cyber-attacks.

2.4 Creation of dubious Apps

Dubious Apps developed by malicious actors on the theme of COVID-19 are being sent to targeted users through WhatsApp and other Social Media links.

2.5 DDoS attack

In order to disrupt the essential public services and utility services, attackers are employing Distributed Denial of Service (DDoS) attack wherein, a multitude of compromised systems (bots) attack a single target, thereby causing denial of service for users of the targeted system. Attackers are also using the compromised systems of organization to carryout DDoS attack on other entities.

3. To mitigate the cyber security threats it is essential to ensure that adequate protections on the ICT systems are put in place at the organizational level. Some of the best practices on organization security are enclosed at **Annexure-I**

4. Further, in view of the current situation of COVID-19, many organizations have adopted Work From Home (WFH) concept, where unsecured home computers are extensively used to connect to the organizational network. To mitigate the cyber security threats emanating from WFH, users may follow best practices as enclosed at **Annexure-II**

5. This is issued with the approval of Chief Information Security Officer(CISO) & DDG(SA), DoT.

Enclosure: As above

08/7/2020

(Vinai Kumar Kanaujia)
Director(Security Audit)
Telephone: 011-2303 6509

To,

1. All officers/officials of DoT Hq.
2. Heads of all Attached Offices/ Subordinate Offices/ Field Offices/ Autonomous bodies/ Statutory bodies/ Training Centres/ CPSEs of DoT

Copy to:

1. PSO to Secretary (T)
2. Sr. PPS/PPS to Member(S), Member(T), Member(F)
3. Sr. PPS/PPS to Additional Secretary
4. Sr. PPS/ PPS to Advisor(O), Advisor(T), Advisor(F)

ANNEXURE-I

Best practices – Cyber Security (Organization level)

- Implement **Application Whitelisting to ensure** only approved application can be executed on user machines. This will be able to prevent attackers from running malware and executing malicious code on a system. Ransomware attacks by sophisticated cyber threat actors and cyber fraud attacks can be prevented (or made difficult) with this solution
- Enforce **Multi-Factor Authentication** (MFA) to prevent phishing attacks that steal email credentials. In case MS Office 365 is being used, MFA should be enabled. MFA should also be enabled for Windows logins, which would be effective against brute force attacks particularly using Remote Desk Protocol (RDP)
- Enable **network segregation** (partitioning of a network to keep critical parts of the infrastructure away from the internet and from less secure internal networks) to contain malicious activity and prevent successful propagation of the malware. This can prevent direct attacks on system that should not be internet facing. Effective monitoring of log-ins and auditing of sensitive data can be put in place to ensure that the data is tracked.
- Install **anti-phishing software** that can run on the mail server and examine emails for any hyperlinks containing phishing websites/ malwares. This can prevent credential loss and malicious code execution through phishing.
- Ensure **Patch Management** (software running on the network is patched and up-to-date) is done on regular basis especially on servers where unpatched remote desktop software if present could lead to cyber-attacks. Else remove unused or unpatched software from computers, particularly remote desktop software. Close ports that need not be connected to the internet.
- Enforce **password policy** in the organization to ensure that a minimum strength of password is complied with across the network. This would help in preventing brute force attacks and from attackers taking advantage of default passwords.
- Periodical **audit of IT systems.**
- **Legacy computers** (particularly internet facing servers) **to be taken off** so as to reduce attack surface.
- **Educate staff** on phishing attacks and email compromise frauds.
- Use **Firewall Access Control Lists** to restrict direct network access to user machines so only approved devices are allowed to connect to them.
- Perform **regular backups** to allow quick restoration of impacted devices. Ensure backups are kept offline and make sure there is a recovery plan in place.
- To secure the web application, **regular Vulnerability Assessment and Penetration Testing** (VPAT) of the entire ICT systems from competent auditors and testers, may be carried out.

Remedial measures in case the system is compromised

- Disconnect the infect computers from LAN/ Internet immediately.
- Remove unused or unpatched software from computers, particularly remote desktop software, if any.
- Change passwords of all emails and online services from another secure computer.
- Hard disks of the infected computers may be formatted after taking backup of data files.
- Operating systems and applications should be re-installed from clean software.
- Backup data should be scanned for virus before restoring it.

ANNEXURE-II

Best practices – Cyber Security (User level)

- Always use **genuine software.** Install the latest updates/ patches for Operating System, Antivirus and Application software.
- **Limit user privileges** on the computer. Always access Internet as a standard user but not as Administrator.
- **Restrict remote access.** If file sharing is not required in your day-to-day work, disable file and print sharing.
- Be wary of **storing personal information** on various Social Media and other platforms.
- **Do not share financial details,** e-wallet details or banking details with anyone.
- Beware of **unsolicited contacts from individuals** in person, on the phone, or on the Internet who are seeking organizational or personal data
- **Do not share usernames,** passwords, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.
- **Do not provide information about yourself** that will allow others to answer your security questions- such as when using "I forgot my password" feature. Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends and co-workers on Social Media platforms.
- **Check and verify email** sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
- Be **cautious of tiny** URLs in Email contents.
- **Do not open attachment** having extension: VBS, U64, SHS, PIF, SCR.
- **Protect against social engineering attacks.** Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
- Regularly **check the last log-in details** of emails accounts.
- **Internet-connected computers should not be used for drafting storing classified official documents / correspondences.**

*****