SECRET

E-28149

II/21021/40/2014-IS-II/M Pt.
Government of India
Ministry of Home Affairs
(IS-I Division/ Monitoring Unit)

North Block, New Delhi
Dated: 23rd May, 2017

Office Memorandum

Subject: Phishing campaign to gather user credentials (Username/Password) and targeted attacks to compromise computers used by officials of Govt. of India – regarding

The undersigned is directed to state that it has been observed that a new wave of Phishing campaign, to gather user credentials and targeted attacks to compromise computers, is on the rise. Another, alarming trend is to use spoofed/compromised mail IDs of NIC domains (@gov.in, @nic.in, @mea.nic.in, etc.) with intended recipients. Based on our analysis, the attacks can be categorized into following types: -

i) Phishing Emails to gather user credentials (username/password)

ii) Emails with malicious web links / file attachments to compromise computers

iii) Seemingly novice Emails to establish association with the recipient for further malicious activities.

2. It is increasingly noticed that, malicious codes embedded in document files like doc, xls, pdf, and zip etc. are sent as mail attachments to compromise computers. Opening of these files would result in compromise, which in turn may lead to pilferage of computer configuration details, keystrokes, documents stored in computer etc, besides gaining remote access to the compromised computers.

3. Occasionally mails without any malicious components are also sent to prospective targets to establish association for further malicious activities.

4. A copy of conventional Email/cyber security norms & best practices for smart phone users is attached. It is requested to take necessary action and sensitize all offices under your authority.

JS(RKC)
24/5

D.Adm S.

Pl. circulate
24/5/17

23/5

(Shailendra Vikram Singh)
DGM (IS.I)
Tel: 23093753

Encl: As above.

30/5/17

To,
All Ministries/Departments of the Govt. of India

US (Adm)

30/5/17

SO/Adm

31/5

Annexure

Conventional Cyber Security Norms and Best Practices

A) Do's and Don'ts to minimize Malware (Virus, Trojan, and Worms etc.) infections while using Internet-connected or standalone Computers.

Do's

1. Always use genuine software.
2. Install the latest updates/patches for Operating System, Antivirus and Application software.
3. Enable a firewall. Operating Systems have an inbuilt firewall which can be used to stop unwanted Internet connections.
4. Limit user privileges on the computer. Always access Internet as a standard user but not as Administrator.
5. Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
6. Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
7. Regularly check the last logging details of email accounts.
8. Use strong passwords that include a combination of letters, numbers, and symbols.
9. Use only officially supplied USB storage media. USB storage media should be regularly formatted after use to erase any malicious files hidden from normal view.
10. Regularly take backup of document files to avoid lose of files in case of emergencies like malware infections, hard disk crash, corrupted applications and other unforeseen incidents.
11. Users should be periodically briefed about Cyber Security measures.

Don'ts

1. Avoid downloading and installing pirated software.
2. Internet-connected computers should not be used for drafting / storing sensitive official documents / correspondences.
3. Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.
4. Don't download and open file attachments that originated from unknown sources.
5. Auto storage of user name and password in browser /web page should be disabled in shared computers used for Internet activities.
6. Avoid using personal USB storage devices / Smart Devices on office computers. Don't put unknown USB storage device into your Computer.
7. Don't share passwords with anyone. Don't use the same password on all websites and services.

/asic secure practices for Email usage:

1. Do not open/reply to any suspicious mail and never click any hyperlinks/web links/URLs mentioned in the body of such mails.
2. Scan mail attachments before downloading / opening.
3. Do not enable VBS Macro when asked for while opening Microsoft documents (doc/docx, xls/xlsx, ppt/pptx and mdb/mdbx). By default, Microsoft products come with VBS Macro disabled.
4. In Adobe Acrobat Reader for PDF files, do not enable Java Scripts or similar scripting functions.
5. In case of noticing any suspicious activities, change passwords of all online accounts (emails and others) from other secure computer.

C) A few indicators of a Generic Malware infected computer:

1. Computer runs slowly than normal, stops responding or freezes often. Computer crashes and restarts every few minutes.
2. Unusual error messages pop up constantly.
3. New toolbars, links, or favorites added to your web browser.
4. Home page, mouse pointer, or search program changes unexpectedly.
5. Unusual network traffic and connectivity from the computer even without doing any Internet activity.

(These are common signs of malware infection, but they may also be indicative of mere hardware or software problems.)

s to check and protect from malware infections in Windows computer.

1. Always set automatic updates for Operating System, Anti-Virus and Applications. For Windows OS auto update can be done as follows:-

   Control Panel -> Windows Updates ->Change Settings -> Install updates automatically.

   (For other software follow the steps as given in the respective software.)

2. Checking for unusual network traffic with Windows "netstat -na" command.

   Type "cmd" in "run" and type "netstat –na". Checkout foreign Established connection and IP addresses. Check the IP address for its ownership

3. Check for any unusual executable running automatically at Windows startup.

   Type "msconfig" in "run" and check for any unusual executable running automatically.

   (Disable, delete or uninstall any unnecessary /unknown executable/ program.)

4. Enable hidden files, folders and system files view to find any unusual or hidden files, especially useful while using USB storage devises.

   Control Panel -> Folder Options -> View -> select the "Show hidden files and folders" option and unselect "Hide protected operating system files"

Make sure there is no hidden file and folders present in the USB Storage device. Format the device if any unusual files (files having extensions exe, com, dat, scr and ini etc) are present besides the data files (doc, ppt, xls and pdf etc).

5. Delete the contents of Windows "Temp" and "Temporary Internet files" regularly.

   (a) Type %temp% in "run" and delete all the contents of temporary folder.
   (b) For deleting Temporary Internet Files follow steps as given by different browsers like Windows Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari.

Best Practices for Smart Phones / Tabs

Most of the smart phones and tablets (Tabs) are having equal computing power of a normal desktop / laptop systems. These gadgets are capable of delivering many services on video, voice, picture, GPS and other computational apps like any other computer. Therefore, all cyber security guidelines and best practices related to computers are also applicable to these devices.

Following are some of the security concerns of Smart devices:

- These are equally vulnerable to Malware attacks and data leakages as ordinary Internet connected computers.
- More applications, features and service are available on smart device for exploits than basic phones.
- These gadgets are known to be used for bugging (audio and video), monitoring call details, contents, SMS monitoring, sending malicious SMS, Emails, spoofing and other malicious activities without the knowledge of the user.
- Smart Phones and Tabs are known to have multiple vulnerabilities, which are being widely exploited by the attackers and adversaries.

Best Practices for users

- Do not store any classified / sensitive data (text / video / photograph) in the device.
- Before downloading any App, same should be checked for its reputation / review. Read vendor privacy policies before downloading apps and app permission should be reviewed closely
- Remember most apps collect and some times publishes user data on Internet, or they share data with others for revenue generation purpose.
- Auto start, data usage for each App and App permission should be controlled through the security features available (depends on OS and make of the phone)
- Review the default privacy settings of smart phone apps or services and, if needed, change the settings; e.g. settings about whether or not to attach location data to images, to social network posts, etc.
- Regularly check the outbound data usage of various apps.
- Relevant anti-virus software should be installed in the smart device and same be updated regularly.

- If the Smart device gets de-activated for any reason for few hours / one day, the service provider should be contacted immediately to ascertain the reason for deactivation.
- Turn off GPS location services to avoid getting tracked in real time.
- Turn off / remove the apps which are not needed.
- Many users tend to save their passwords to online services and sites on their device. Avoid having all important passwords saved in your device particularly when it comes to banking or payment apps. Therefore, do not auto-login or store passwords in the smart phone.
- When device is idle, it should get locked and require a password / pin or swipe pattern. Set the device to lock in relatively short time.
- During repairs, do not leave device unattended to deny the possibility of installation of Malware or copying of data.
- Take back-up of data (contacts, personal photos, etc.) on external media
- Do not reply or click on link on SMS or messages or photos sent by strangers.
- Do not jail-break device as jail-breaking removes the restrictions on which apps can be installed or not installed. This removes the protection set by the manufacturer.
- Be cautious with public Wi-Fi. Many Smartphone users use free Wi-Fi hotspots to access data (and keep their phone plan costs down). There are numerous threats associated with Wi-Fi hotspots. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks.
- Enable encryption. Enabling encryption on your Smartphone is one of the ways to safeguard information stored on the device, thwarting unauthorized access.
- Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile. The operator can block a phone using the IMEI code.
- It is necessary to lock your apps, especially the ones holding private information that you wish nobody but you could see. This is a second layer of security to prevent anyone from using your lost device particularly if they have managed to bypass your locked smart phones
- Remote wipe means that if your phone is lost or stolen, you can remotely clear all of your data--including e-mail, contacts, texts, and documents--off of the handset, thus keeping that information out of the wrong hands. Explore / subscribe to this feature.

Best practices for WiFi connectivity for users

Always remember WiFi signals are susceptible to monitoring without any indication of being monitored. Therefore, the security of the WiFi communication depends on the attacker's ability to break the encryption in a specified time rather than various best practices.

- Limiting coverage of access points: Evaluate physical perimeter to define positioning of wireless device thereby limiting radio transmission and coverage, inside the physical premises or intended coverage area
- Device configuration: Systems with ability to connect wireless network should be preconfigured with relevant and appropriate configuration. Restrict systems from which management access is permitted.
- Wireless encryption: Communication between user system and wireless Access Points (AP) are secured using highest graded encryption (WPA-2 or higher) for data confidentiality and integrity. Never use WEP encryption. Under no circumstances, should open APs be used.
- In order to allow authorized users to connect to the access point, wireless clients should be provided access based on MAC address.
- Do not auto-Connect to open Wi-Fi Networks.
- Change default Service Set Identifier (SSID a wireless network name) name and turn off SSID broadcast
- Change the default passwords of AP to a strong password. Ensure AP is configured with restricted access for its configuration.
- Disable Dynamic Host Configuration Protocol (DHCP)
- Update the firmware of access point. It can reduce the number of security loop holes in the access point.