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

No. 1-5/2003 (NTISB-II) Islamabad 10 August, 2018

Subject: **Prevention Against Cyber Espionage (Advisory No 148)**

1. **Introduction.** **Cyber Security** researchers have discovered **critical vulnerabilities** in **Microsoft Windows, Microsoft Office, internet explorer (1E), powershell, visual studio** and **adobe flash player .These vulnerabilities** facilitate a **remote attacker** to execute **malicious** code on **vulnerable system.**

2. **Technical Analysis**

a. **These critical** issues are observed due to **memory corruption flaws** in **internet explorer, edge browser** and **chakra scripting engine.**

b. **A critical flaw (CVE-2018-8327)** affects Powershell editor services that could allow a **remote attacker** to execute malicious code on **vulnerable system.**

c. Following the **most critical vulnerabilities** found in **Microsoft Windows** and other softwares:-

(1) Scripting Engine **Memory Corruption** Vulnerability **(CVE-2018-8242).**

(2) **Edge Memory** Corruption Vulnerability **(CVE-2018-8262).**

(3) **Chakra** Memory Corruption Vulnerability **(CVE-2018-8280).**

(4) Microsoft Edge Memory Corruption Vulnerability **(CVE-2018-8301).**

(5) Microsoft Edge **Information Disclosure** Vulnerability **(CVE-2018-8324).**

3. **Affected Products.** These vulnerabilities affect **Microsoft Windows** and following softwares:-

a. Internet Explorer IE
b. ChakraCore
c. Microsoft .NET Framework
d. PowerShell
e. Visual Studio
f. Microsoft Office
g. Adobe Flash Player
h. Microsoft Share Point
i. ASP .NET.

PS TO CHIEF SECRETARY SINDH 18
Diary No 24685
Inward Date 15/8/2018
Outward Date

NO. PS/SECY/I.T/166/ Dated: 16-08-2018

DG ISI TD Dairy No. 254 Dated 16-8-18.

4. **Recommendations**

a. **Security patches** have been **released** by all **vendors;** it is strongly advised to **update** against these vulnerabilities.

b. For updating **Microsoft Windows** go to **Setting**→ Update & Security→ Windows→Updates →**Check for updates.**

c. **Install** and **update** well reputed antivirus such as **Kaspersky,** Bitdefender, Nod32 and **Avast** etc.

d. Regularly update all software's including **Windows OS** and **Microsoft Office.**

e. Don't download **attachments** from, unknown emails source.

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

**Major**
**(Ch Usman Firdous)**
**Assistant Secretary-II (NTISB)**
**Ph# 051-9204560**

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**
**Copy to :-**

SPS to Cabinet Secretary, Cabinet Division , Islamabad

PS to AS-III, Cabinet Division, Islamabad

APS Secretary, NTISB

APS Deputy Secretary, NTISB

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

No. 1-5/2003 (NTISB-II)

Islamabad \0 August, 2018

PS TO CHIEF SECRETARY SINDH 18
Diary No 2468
Inward Date 15/8/2018
Outward Date

Subject: **Security Concerns on E- Filing - Government and NTC DATA Center / Network**

1. NTC has been providing Information and Communication Technology (ICT) infrastructure and services including telecom, internet, e-mail, web-hosting, VPN, video conferencing, DSL, etc. to all major government organizations. Defacement of government websites hosted at NTC on occasions of national importance prompted Ministry of IT to consult NTISB, Cabinet Division for carrying out detailed security assessment. Conduct of Information Security Audit of NTC's ICT infrastructure as well as websites developed by National IT Board (NITB) hosted at NTC and the e-Office application managed by NITB was initiated to identify vulnerabilities and recommend appropriate remedial measures for protection of sensitive government information.

2. Brief engagement details are as below:-

a. **Security Assessment of NTC In 2016.** After surfacing of Wikileaks regarding Green Line Telecom exchange, security assessment activity of NTC's ICT infrastructure and associated services was initiated in Sep 2016. A joint assessment team was formed and after consultation with NTC, following major components were identified for assessment. The activity continued for few days and had to be **stopped due to non-provision of required information and denial of required access to infrastructure elements:-**

C.S
Secy. (I.T) GNTC

(1) ISP, Data Network and Data Center
(2) Telecom Infrastructure
(3) Green Line Communication
(4) CPEC Web and Mail Servers

b. **Security Assessment NTC and NITB in 2018.** On 15 August 2017, a cyber-attack originating from India resulted in hacking of Ministry of Defence (MoD) website. **In backdrop of the attack,** NTISB initiated security posture assessment of NTC's ICT infrastructure and hosted websites/applications. The activity continued from 24 Apr to 24 Jun 2018. During partially conducted activity, certain security loopholes were identified and notified to NTC. In the same backdrop, assessment of NITB managed applications and websites was also carried out. No details of websites were shared during the activity, however, e-office applications was analyzed for security vulnerabilities. **The activity is currently suspended again after refusal of NTC to give access to auditing team and share evidences of lapses recorded during the partially carried out assessment**

2. **Critical Observations.** Based upon the partially carried out recent activity, following critical observations are relevant-

a. **NTC**

(1) Absence of network security devices at critical Internet and intranet service points for government organizations has been making it an attractive target even for trivial cyber-attacks.

(2) ICT infrastructure of NTC is found with insecure configurations with extensive use of public IP addresses even for critical network components e.g. **public IP addresses are directly terminating on firewalls, core switch and important routers.**

(3) **Critical administrative systems have been found with direct Internet connectivity** without any IT Security controls.

(4) Presence of easily exploitable vulnerabilities in NTC's ICT infrastructure and services can become launch pad for ingress into **logically isolated but physically connected** government networks.

b. **NITB**

(1) **Government communication and information sharing via e-Office interface is not secure.** The communication is being done on NTC's insecure telecom and communication network in plaintext where public IP addresses are terminating at core network devices.

(2) The prevailing trend of using e-Office application and internet on same system without using appropriate security measures puts sensitive data at risk of exposure to public network (i.e. Internet).

(3) **Administrator of e-Office at NITB** has **full visibility to activities and data of e-Office users.** Furthermore, copies of all e-Office user credentials and digital certificates are being stored at administrator's system. Resultantly, administrator can remotely log-in to the application as any legitimate user of e-Office.

3. **Conclusions**

a. Possibility of website defacement on **14 August 2018** is highly likely due to failure of NTC in implementing remedial measures despite identification as well as refusal to solicit assistance being offered by NTISB.

b. Telecom and network services provided by NTC are **NOT** secure and pose risk to IT security of government networks, data, websites and applications.

Government communications and information sharing done via e-Office is not holistically secured under information security umbrella and the information shared is at the risk of exposure on internet.

d. Non-cooperation in conduct of Information Security audit, repeated refusals for evidence sharing and failure in rectification of identified security loopholes call for suitable way forward.

4. Forwarded for further necessary action, please.

**Major**
**(Ch Usman Firdous)**
**Assistant Secretary-II (NTISB)**
**Ph# 051-9204560**

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

No. 1-5/2003 (NTISB-II)

Islamabad 10 August, 2018

Subject: **Prevention Against Cyber Espionage (Advisory No 147)**

PS TO CHIEF SECRETARY SINDH
Diary No 2463
Inward Date 15/8/2018
Outward Date

1. **Introduction.** A malicious email **"GE 2018 final checklist-personal postal ballot assignment"** is being sent to officers and staff of defense/ intelligence organizations. Email contains a malware hidden in **ZIP file,** containing malicious executables. Downloading and running the file, executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Emails**

a. **Subjects.** GE 2018 final checklist-personal postal ballot assignment

b. **Name of Attachments.** ECP 2018 checklist.zip

c. **Antivirus Detection Rate of Extracted Files**

| Ser | Files extracted | Detection Rate | Percentage % |
|---|---|---|---|
| (1) | ECP emergency and complaint.xls | 20/64 | 31.2 |
| (2) | List ECP Alerts.xls | 20/67 | 29.9 |
| (3) | OFFICIALS SMS SERVICES.xls | 33/67 | 49.2 |
| (4) | ieflash.exe | 20/67 | 29.9 |
| (5) | fileman.exe | 47/66 | 71.2 |

C.S
Dy. (I.T) GIAC

d. **Malware Type.** Trojan based Keylogger

e. **C&C Servers**

| Ser | C&C URL | IP Address | Hosting Country |
|---|---|---|---|
| (1) | h88-150-138-77.host.redstation.co.uk | 88.150.138.77 | UK |

3. **Technical Analysis.**

a. **Indicators of Compromise.** The malware makes following files on the infected system:-

(1) C:\Windows\Temp**fileman.exe**. (Original name is **services.exe)**

(2) C:\Users\admin\AppData\Roaming\MicrosoftWindows\Start Menu\Programs\Startup\ieflash64.exe. Original name is **native.exe**

(3) Registry key at Path and having Key: "TSUSERENABLED" "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMI ALSERVER

(4) The malware is being spread through Google drive link

https://drive.gbogle.com/file/d/1pNVigMzFM337dP9u41cD6BjnXgmRZmM

b. **Capabilities of Malware.**

(1) The malware is capable of getting system **IP, user, location, network configuration details,** computer configurations and it can upload these details on its **C&C server** mentioned at **para 2(e).**

(2) The malware has the ability to act as a **key logger** and steal the **usernames** and **passwords** of infected systems.

(3) The malware pan Copy itself into registry and it can **automatically execute** itself on windows boot.

(4) This trojan establishes and maintains continuous communication with its C&C server.

4. **Recommendations.**

a. **Install and update licensed and well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

b. Block C&C Servers at para 2(e) in **firewalls** of own networks.

c. In case if **indicators of compromise (para 3a)** are found in the system,please disconnect the computer from internet and **reinstall windows.**

d. **Update** all softwares including **Windows OS,** Microsoft Office.

e. **Don't download** attachments from **emails unless** you are sure about the source.

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

**Major**
**(Ch Usman Firdous)**
**Assistant Secretary-II (NTISB)**
**Ph# 051-9204560**

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments**

**Copy to :-**

SPS to Cabinet Secretary, Cabinet Division , Islamabad
PS to AS-III, Cabinet Division, Islamabad
APS Secretary, NTISB
APS Deputy Secretary, NTISB