Subject:- **Cyber Security Advisory - Analysis of Malicious Email (Imran Nazir "ntisb @cabinet.gov.pk & ad.it@cabinet.gov.pk") (Advisory No. 54)**

A targeted malware attack is spreading through an **email (Imran Nazir** ntisb@cabinet.gov.ok & ad.it@cabinet.gov.pk) among civil, defense and intelligence organizations for information gathering and system control. The malicious email contains multiple **.xlsx** files as attachment. These files look legitimate, but contain objects with malicious links leading to malware execution in the background using **Google Update triggers** and **Equation Editor Vulnerability.** Therefore, an advisory is attached at **Annexure-A** for onward sharing and compliance by Director IT, Cabinet Division.

2. Forwarded for information/ dissemination to concerned, please.

Annexure-A

Cyber Security Advisory - Analysis of Malicious Email (Imran Nazir "ntisb @cabinet.gov.pk & ad.it@cabinet.gov.pk") (Advisory No. 54)

1. A targeted malware attack is spreading through an **email (Imran Nazir** ntisb@cabinet.gov.pk & ad.it@cahinet.dov.pk) among civil, defense and intelligence organizations for information gathering and system control. The malicious email contains multiple **.xlsx** files as attachment. These files look legitimate, but contain objects with malicious links leading to malware execution in the background using **Google Update triggers** and **Equation Editor Vulnerability.** Therefore, recommendations at **Para 4** must be followed to avoid being victim of such emails.

2. **Summary of Malicious Email**

a. **Vulnerability ID.** CVE-2017-11882

b. **APT Group** SideWinder APT

c. **File Name** Process status.xlsx, Evaluation Repot.xlsx & Requirement. doc

d. **File Extension** .xlsx & .doc

e. **Antivirus Detection Rate.** Low

f. **Indicators of Compromise**

(1) Files created on suspicious locations C:\Users\Public\Documents\sihost.exe.

(2) Persistence keys used and Task scheduler was set at \Windows \Wininet**Ctf** and \Windows\Wininet\Ctfmon which gets triggered after every **15-20 minutes.**

g. **C&C Servers**

Ser	URL address	IP Address	Country
(1)	sambatvnewsupdate.com	198.54.126.118	USA
(2)	Helpdesk.autodefagapp.com	198.187.31.255	USA

3. **Capabilities of Malware**

a. The malware is specially designed for targeted attacks and can steal files / stored passwords from windows system and browsers.

b. The attack involved **Task schedualer** alterations to reside for persistence.

c. The malware employs sleep function as **defensive technique** and multiple copies of scripts are made for **persistence** and checks for **presence of debugger.**

d. The attacker can gain remote access of the system and can execute additional payload.

e. The malware uses **Equation Editor** to exploit based on **fileless technique.**

4 Recommendations

a. Cabinet Division email administrators and user accounts passwords must be changed immediately.

b. Be vigilant against email IDs; **(Imran Nazir** ntisb@cabinet.gov.pk & ad.it@cabinet.gov.pk). In case, the email IDs are legitimate and compromised, immediately change the passwords (as per **Para 4a).** In case the email IDs are not legitimate, block them at email server.

c. The IT department should disable Microsoft Equation Editor in Office from registry to avoid further attacks.

d. Microsoft executables including Verclsid, Rundll32, Regsvr32, Regsvcs / Regasm, odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, Control Panel, Compiled HTML File to be monitored as major malware executables and be blocked.

e. Do not download attachments from emails unless you are sure about the source.

f. Window defender and Firewall of system to be on recommended settings.

g. Be vigilant regarding redirected links and typing sensitive information online.

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

"ntisb @cabinet.gov.pk and **ad.it@cabinet.gov.pk"**

6. Forwarded for perusal and dissemination of information to all concerned and under command, please.