SECRET

Subject: **Advisory - Prevention Against Cyber Espionage (Advisory - No 32)**

1. **Introduction.** A malicious email named as **"Appointment with Maj General Asif Ghafoor"** is being sent to officers and staff of defense/ intelligence organizations. The email contains a link to download a malicious file. Downloading and opening the file executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Emails**

   a. **Subjects.** Appointment with Maj General Asif Ghafoor

   b. **Name of Attachments.** Invite.doc

   c. **Antivirus Detection Rate.** 9/67 **(13.4% Very Low).**

   d. **Malware Type.** Trojan based Keylogger / File stealer

   e. **CVE (Common Vulnerabilities and Exposures).** CVE-2017-0199

   f. **Exploit Type.** RTF (Rich Text Format)

   g. **C&C Servers**

Ser	URL	IP	Hosting Country	Registrant Country
	217.182.54.211/Project1. exe	217.182.54.211	France	-
	pcupdate.ddns.net/mercury/A85473F9FABE64BBF703F968BC5CEA/syspba.exe	217.182.38.178	USA	USA
	pcupdate.ddns.net/mercury/heliocentric.php	217.182.38.178	USA	USA
	invite.ispr.press			Panama
	tracking.ispr.press	-	USA	Panama

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

   a. C:\Temp\csvt.exe.

   b. C\Users\<Admin>\\AppData\Local\Microsoft\Windows\. TemporaryInternetFiles\ Content.lE5\5DCYMFOC**syspba.exe.**

   c. C\Users\<Admin>\AppData\Local\Microsoft\Windows\ TemporaryInternet Files\Content.IEMJFK3770**Program1.exe**

   d. CAUsers\\<Admin>\AppData\Roaming\Microsoft\Windows\Start Menu\ProgramS\Startup**Network Interna.link.**

4. **Capabilities of Malware.**

   a. 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.

b. The malware has the ability to act as a key logger and a file stealer. Malware can steal the usernames and passwords along with sensitive user data.

c. The malware can copy' itself into registry and it can automatically execute itself on windows boot.

5. **Recommendations.**

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

b. Block C&C Servers at para 2g in firewalls of own networks.

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

d. Update all softwares including Windows OS, Microsoft Office and all other softwares.

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