Subject: - **Cyber Security Advisory - Malware Analysis - Installation of Smart - S RADAR Onboard OV2600T (Advisory No. 01)**

Context. Indian state sponsored Cyber Threat Actors and APT groups have been targeting Pakistan's civil and military setups for espionage. DO NOT (also known as APT-C-35 & Sector E02) is a threat actor (APT group) operating since 2016. The threat actor is known for targeting organizations and individuals in South Asia with sophisticated windows and Android malware.

2. **Objective**. Do Not threat actor mainly collects and exfiltrates data to Indian intelligence agencies for cyber espionage.

3. **Current Status**. Recently, the threat actor has improvised cyberattack toolkits thus causing concerns for potential victims. The threat actor has emerged in various cyber threat intelligence watchdogs alerts. Modus operandi and preventive measures against DO NOT threat actor are mentioned in ensuing paras.

4. **Targets Countries**

   a. South Asia-Bangladesh, Sri Lanka, Pakistan and Nepal (including embassies abroad).
   b. International – Emerging powers.

5. **Interested Areas**

   a. Government and military organizations
   b. Ministries of Foreign Affairs
   c. Embassies

6. **Modus Operandi**. DO NOT APT has been consistently targeting critical entities with waves of spear phishing emails and malicious attachments. It has been repeating attack patterns on same victims with advanced techniques. Few techniques are mentioned below: -

   a. Macros in MS-Word, Excel, PowerPoint etc. leading to remote access.
   b. Windows Framework RTF files with .doc extensions further containing links to download malware and gain shell access. This is the latest attack technique used by APT - C-35.
   c. YTY Malware-Indigenously developed by DO NOT APT consists of a chain of downloaders that ultimately download a backdoor with minimal functionality, used to download and execute further components of DO NOT Team's toolset

7. Indicators of Compromise (IoCs) and Famous Attacks and Toolkits. Details are provided at **Appendix-I** and **Appendix-II**.

8. **Preventive Measures**. Few preventive measure (but not limited to) to defend against DO NOT APT attacks are as follows: -

a. Utilizing system hardening be ensured at all endpoints.

b. Active directory domain networks be hardened to ensure protection against Kerberos based attacks (Golden, Silver and Skeleton Key Attacks)

c. Execution of signed executable like PsExec.exe, Netcat.exe, Socat.exe and netcat.exe be blocked and monitored.

d. Execution of unsigned executables from %temp% directory and AppData directory be blocked and monitored.

e. Malware focused audit of all endpoints be conducted periodically.

f. Always use reputed anti-malware/anti-virus.

g. Establish SOC for network/host visibility at organizational level be ensured by utilizing open source XDR, EDR and SIEM solutions.

Appendix I

INDICATORS OF COMPROMISE (IoCs)

Ser	SHA-1	Filename	ESET detection name
a.	78E82F632856F293BDA86D77D02DF97EDBCDE918	cdc dll	Win32/TrojanDownloader.Donot.C
b.	D9F439E7D9EE9450CD504D5791FC73DA7C3F7E2E	wbiosr.exe	Win32/TrojanDownloader.Donot.D
c.	CF7A56FD0613F63418B9DF3E2D7852FBB687BE3F	vdsc.exe	Win32/TrojanDownloader.Donot.E
d.	B2263A6688E512D90629A3A621B2EE003B1B959E	wuaupdt.exe	Win32/ReverseShell.J
e.	13B785493145C85B005E96D5029C20ACCFFE50F2	gedit.exe	Win32/Spy.Donot.A
f	E2A11F28F95117536983A5CDBAA70E8141C9DFC3	wscs.exe	Win32/Spy.Donot.B
g.	F67ABC483EE2114D96A90FA0A39496C42EF050B5	gedit.exe	Win32/Spy.Donot.B

Appendix II

FAMOUS ATTACKS AND TOOL KITS

Ser	Name	Malicious Files	Timeline
a.	DarkMusical	Excel - Monthly Action Plan.xls	Jun 2021
b.	Henos	RTF file - ProtocolUpdate.doc	Feb 2021
c.	Gedit	RTF file - Quality Assurance Programme.doc	2020 - 2021
d.	Jaca	PPT - Approved Plan.pptx	2020 - 2021