Subject: **Prevention Against Cyber Espionage (Advisory No. 04) May 2017**

1. **Introduction.** A malware having different names **"WannaCry",** "**WannaCrypt**", **"WannaDecryptor","WannaCryptor2.0"** or **"WCry"** is infecting Windows PCs in around 150 countries. The malware is a ransomware attack and it targets the vulnerability in unpatched windows operating system to infect and spread itself automatically. It encrypts the files in victim's PC and asks for 300 to 600 USD for accessing the files again within limited time. The analysis is underway as new forms of malware are originating daily. Further information will be shared.

2. **Summary of Malware**

a. **Malware Type.** Exploit based Ransomware

b. **Antivirus Detection Rate.** 12/55 (21.81%)

c. **CVE (Command Vulnerability and Exposure) Index.** CVE-2017-0143

d. **Affected Operating Systems.** Windows XP, Windows Vista, Windows Serve 2008, Windows Server 2012, Windows 7, Windows 8, Windows 8.1, Windows 10

e. **C&C Servers.** Following C&C servers have been detected so far till 16 May 2017

Ser	**URL**	**IP**	**Hosted Country**	**Registrant**
(1)	tor-proxy9.mull-binde.de	163.172.13.165	France	-
(2)	dannenberg.torauth.de	193.23.244.244	Germany	-
(3)	nycbugO.nycbug.org	66.111.2.20	USA	-
(4)	www.electrobsd.org	95.211.138.51	Netherland	German
(5)	freedom.ip-eend.nl	192.42.113.102	-	-
(6)	-	205.186.153.200	USA	-
(7)	-	96.127.190.2	USA	-
(8)	-	184.154.48.172	USA	
(9)	-	108.163.228.172	USA	-
(10)	-	200.58.103.166	USA	-
(11)	-	216.145.112.183	USA	-
(12)	-	162.220.58.39	USA	-
(13)	-	192.237.153.208	USA	-
(14)	-	75.126.5.21	USA	-

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

a. C:\Users\<admin>\Desktop\@**WanaDecryptor@.exe**

b. C:\Users\<admin>Desktop\TaskData\Tor\taskhsvc.exe

c. C:\Users\<admin>Desktop**taskse.exe**

d. C:\Users\<admin>\Desktop\taskdl:exe

4. Capabilities of Malware

a. The malware has the capability to encrypt all user's files and upload the decryption key onto its C&C server and ask the user 300 USD for decryption.

b. The ransomware has the capability to give remote access to the hacker.

C. The malware can automatically spread to all the systems within the network

5. Recommendations

a. Update Windows 10, 8.1, 8, 7, XP, Vista. 2003, 2008 and 2012 through "Windows update" to stop the malware from infecting PCs and Servers.

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

c. In case if indicator's of compromise (pare 3) are found in the system, please disconnect the computer from internet, reinstall Windows and update it.

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