Subject: **Advisory – Prevention against Cyber Espionage (Advisory No. 8)**

1. **Introduction.** Recently, a malware has been found spreading through spoofed emails that is targeting defense / intelligence as well as government organizations. The email asks user to download a masqueraded document from **Ministry of Interior (MoI),** with subject **"MOI Amendment to Public and Optional holidays Year 2019"**. It contains a malicious link that redirects the user to download a document file. Downloading and opening the file executes a malware in background, which compromises victim's machine.

2. **Summary of Malicious Email.**

   a. **Email Subject. "MOI Amendment to Public and Optional holidays Year 2019".**

   b. **Document Name. MoI – Calendar 2019.doc.**

   c. **Spoodfed Email address. newsletter.public@nadra-moi.mail-a.cn.**

   d. **CVE ID.** CVE-2018-11183.

   e. **Antivirus Detection Rate.** Nil / 55 (No detection at the time of analysis).

   f. **File Size** 978 Kb.

   g. **File Extension.** Doc (Word Document Extension).

   h. **Exploit Technique.** DLL Injection into legitimate file.

   i. **File Hash**. 5b1f9145f850e11c26fc90bba916e38c.

   j. **C & C Servers**

Ser	URL address	IP Address	Hosting Location
(1)	https://narda-moi.cdn-dl.cn	185.45.193.195	Netherlands
(2)	Cdn-re.net	185.244.249.6	Romania

3. **Indicators of Compromise.** The system is infected if following files are found in the system: -

   a. C:\ProgramData\Dat\serv2**credwiz.exe (Digital Signature Protected File)**.

   b. C:\ProgramData\Dat\srv2**duser.dll (Malicious DLL)**.

   c. HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion.
   \Run**credw1 (Autostart Registry Key).**

4. **Capabilities of Malware**

   a. The malware has a **valid digital signature** and hence it has a very low detection rate.

b. The malware is specially designed for **targeted attacks** and **can steal files and keystrokes from windows system**.

c. The **attacker** can gain **remote access of the system** and can **execute additional payload** from it.

5. **Recommendations**

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

b. In case, if indicators of compromise (para 3) are found in the system, please **disconnect the computer form internet and reinstall Windows.**

c. **Update all softwares** including Windows OS, Microsoft Office and all other softwares on regular basis.

d. Uninstall all unwanted softwares from your system and android phone.

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

f. **Enable 2 factor authentication on all your email accounts (Gmail, Yahoo, Hotmail etc), social media accounts (facebook, whatsapp etc) especially internet banking to prevent any sort of unauthorized access** and financial loss.

g. **Never forward your OTP (One Time Password)** to anyone as it can easily hack your accounts.

h. Make sure that **host based firewall is enabled and configured** to block all incoming connections except whitelisted / allowed applications.