

- (2) **MD5 Hash.** 6d63dc5cdb504f3365403c1296e696a0
- (3) **Malware APT Group.** Patchwork
- (4) **Vulnerability ID.** CVE-2017-0261
- (5) **Antivirus Detection Rate.** Low
- (6) **File Size.** 454 Kbs.
- (7) **File Extension.** Docx
- (8) **C&C Servers**

Ser	URL Address	IP Address	Country
(a)	-	176.107.181.213	Ukraine

(9) **Indicators of Compromise**

- (a) File locate at C:\ProgramData\Microsoft\DeviceSync\pri.d11.
- (b) Malware drop at C:\Users\\Appdata\Roaming\Microsoft\Windows\Start\Menu\Programs\Startup folder.
- (c) Persistence through registry key entry at **HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution1<filename>.exe.**

3. **Capabilities of Malwares**

- a. The malware is capable to access and edit Registry values of MS Word.
- b. The attacker can gain remote access of the system and execute additional payload from it and run Microsoft certified files to evade antivirus detection.
- c. The adversary maintains a database for data storage on local machine and creates temporary files for uploading on C&C server.
- d. Malware employs techniques of long-closed vulnerabilities and implanted EPS script.

4. **Recommendations**

- a. **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc and scan system regularly.
- b. Update all software including Windows OS, Microsoft Office etc on regular basis.
- c. Uninstall all not in use applications and software from system and personal phone.
- d. **Do not download attachments from emails unless you are sure about the source.**
- e. Window defender and firewall of system to be kept on recommended settings.

Subject: **Advisory - Prevention Against Cyber Espionage (Advisor No.6)**

1. Two sophisticated malwares have been found spreading through **spear phishing and social engineering** tactics. These malwares are specifically designed to target army / intelligence organizations as well as Defence attaches abroad in a well-planned manner. For compromising the target systems, two malicious MS-Word files have been crafted by the hackers that look like legitimate files. These documents are sent to the targets through emails either bearing subject "**China Cruise Missiles Capabilities**" or "**Chinese Pakistani War Games**". Downloading and clicking on these spurious documents result in execution of a malware in the background which compromises the victim's machine.

2. **Analysis of Malicious Email.** Summary of analysis of both the malware being spread through emails is as under: -

a. **Email's Subject.** China Cruise Missiles Capabilities.

(1) **Downloaded File Name.** China Cruise Missiles Capabilities-implication for Indian Army.docx

(2) **MD5 Hash.** 9f54962d644966cfad560cb606aeade2

(3) **Malware APT Group.** Confucius

(4) **Vulnerability ID.** CVE-2017-0199

(5) **Antivirus Detection Rate.** Low

(6) **File Size.** 476 Kbs

(7) **File Extension.** Docx

(8) **C&C Servers**

Ser	URL Address	IP Address	Country
(1)	Msoffice. User-assist.site	45.84.204.148	Lithuania

(9) **Indicators of Compromise**

a. Updates information is file C:\Users\tratable.accdb.

b. Temporary files at C:\Users\<random>.tmp.cvr

b. **Email's Subject.** Chinese War Games

(1) **Downloaded File.** Chinese_Pakistni_fighter_planes_play_war_games.docx