Subject: **Prevention against New Word Exploit (Advisory No. 20)**

1. **Introduction.** A new attack vector capable of sending non malicious word document has been discovered by the researchers for targeted infection; document becomes malicious when accessed over the internet These malicious Word files are delivered through intelligently crafted spoofed / phishing emails to the target. Downloading and opening such attachment form email executes malware in the background, resulting in hacking of data from the computer.

2. **Summary of malicious Emails.** Following are the few of identified / reported emails: -

| Ser | Email Subjects | Attachment Name |
|---|---|---|
| a. | IHD – FWO Projs in 10 Corps AOR | SCAN006.docx |
| b. | Kashmir: how Modi's aggressive 'Hindutva' project has brought India and Pakistan to the brink – again | Urgent Action.docx |
| c. | COPY OF LETTER – AMENDMENT IN HWS CONTRACT NO 1262/107/DMP (NAVY) | IHD – FWO Projs in HQ 10 Corps AOR. dock |
| d. | Required Data | Modis Hindutava Policy.docx |

e. **Vulnerability Information.** Customized CVE-2018-0802

f. **Antivirus Detection Rate.** 15/56 **(Low)**

g. **C&C Server.** Following C&C servers have been identified in this malware campaign: -

| Ser | Command and Control (C&C) URL | IP Address | IP Location |
|---|---|---|---|
| (1) | upgrading-office-content.esy.es | 185.224.138.58 | Netherlands |
| (2) | oppak.com | 203.124.44.31 | Pakistan |
| (3) | onlinejohnline99.org/Ms2u1p.php | 93.123.73.198 | Bulgaria |
| (4) | http://en-content.com | 178.62.188.63 | Netherlands |
| (5) | https://sites.google.com/view/fwo-prois-in-10-corps-aor/home (Legitimate Hosting website) | 172.217.17.78 | USA |
| (6) | https://mail-g-live-in-0-inbox-u.herokuapp.com/com/2cp20.php (Legitimate Hosting Website) | 50.19.85.156 | USA |
| (7) | http://support.worldupdate.live/ | 172.105.67.165 | USA |
| (8) | http://maq.com.pk | 203.124.43.227 | Pakistan |

h. **Indicators of Compromise**

(1) C:\Users\Blah\AppData\Roaming\Microsoft\Windows\StartMenu\ Programs/Startup\ **PINS.lnk**

(2) C:\Windows\Tasks**pinfile.exe** (Size = 523 KB)

(3) C:\Users\Blah\AppData\Roaming\Microsoft\Office\Recent**DFILE**

3. **Capabilities of Malware.** Exploited word document is delivered through a spoofed email, which redirects the user to a **legitimate white-listed hosting domain** like **(sites.google.com)**:

a. Malware collects information about computer name, IP address, network adopter settings, time zone settings and drops a payload from its C&C server.

b. It can extract stored usernames, passwords and enable itself to automatically execute on windows restart.

c. Subsequently, malware grants remote access to the hacker to execute various commands.

4. **Recommendations**

a. Don't open attachments from untrusted e-mails and **immediately report suspicious e-mail** to iCSIRT.

b. **Network administrator must check traffic flow** from endpoints to domains mentioned at Para 2(g).

c. System administrators must **keep up-to-date Antivirus / Anti-spyware signatures** on all endpoints along with **host / network-based firewall**.

d. **Application Whitelisting / Software Restriction Policies (SRP)** must be enabled to block binaries running from %APPDATA% and %TEMP% paths; malware generally executes from these location.