Subject: - **Advisory – UPAS Malware (Advisory No. 23)**

General Information. UPAS malware was first spotted/ observed in mid of 2012. It was allegedly created by **WannaCry Killswitch developer (Marcus Hutchins).** Since 2012, various strains of malware are available and it is still active.

2. **Major Contours**

a. **Infection Mechanism**. USB, Social Engineering, Phishing and Email.

b. **Target Platform**. Microsoft Windows.

c. **Persistence Mechanism**. %APPDATA%, %TEMP%, Windows Registry Hive HKLM/ HKCU run key with name of Microsoft (fake entry).

d. **Malware Functionality**

(1) Process Injection (Injection into legitimate process memory).

(2) FTP/ Browser Credential Stealer.

(3) Maintains Persistence.

(4) Sandbox Evasion.

(5) Lateral Movement.

(6) Keylogging.

(7) Additional Payload of Solaris (For Botnet based DDoS attack).

e. **Level of Sophistication**. Ordinary.

f. **C2 Infrastructure**. HTTP based C2 infrastructure.

3. **Remedial Measure**

a. UPAS malware can be removed by deleting the persistence locations present at %APPDATA% and then deleting the corresponding registry at HKLM/ HKCU.

b. Deployment of indigenously developed SIEM / XDR solutions at sensitive locations / offices to safeguard against such attacks.