Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 28) Jun 18**

1. **Introduction.** Radware Threat Research Group has observed vulnerability in paint application "Relieve Stress Paint", through phishing emails and Facebook. This application holds the capability to collect Facebook users' credentials and payment methods. Downloading and running the file, executes malware in background, named as "Stresspaint", that compromises the device.

2. **Summary of Malicious Application**

a. **Classification.** Trojan/ Adware.

b. **Distribution.** Fake aol.net website (xn- -80a2a18a.net).

c. **Other Details.** Browser cookies and login data files are sent encrypted to the C2 server.

d. **Registry keys created/ modified**

(1) HKLMSOFTWAREMicrosoftMindows\\CurrentVersion\\ Run\\ Updata.

(2) HKCU\Software\ClassesWirtualStore\MACHINE\SOFTWA RE RelieveStressPaint\guid-<random HHMMSSYYYYMMDD>.

e. Botnet operators use an open source Chinese CMS called Layuicms2.0. Research group believes that next target will be Amazon.

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

a. Temp\\DX.exe —persistent dropper.

b. Tempupdata.d11—credential/cookie stealing purposes

c. Desktop\RelieveStressPaint.lnk.

d. AppData\Local\Google\Chrome\User Data\Default\Login Data11111

e. AppData\Local\GoogleChrome\User Data\Default\Cookies

4. **Malware Capabilities**

a. On large scale, mlware can be used for monetization, ransom, espionage, propaganda, identheft and malvertising.

b. Malware steals Login credentials, session cookies, network traffic; history,username, address, telephone number, etc.

5. **Recommendations**

a. **Install and update well reputed Antiviruses** Such as Kaspersky, Avira, Avast ete.

b. In case if indicators of ComproMise (para 3) are found in the System, please disconnect the c6mputer from intemet and reinstall windows.

c. Update all softwares including Windows OS, Microsoft Office and disable macros.
d. Don't download attachments from untrusted sources.