Issued 8/23/17

Flaw in LinkedIn Messenger Could Harbour Malware

The researchers found four exploits in the LinkedIn security systems. First, an attacker could create a malicious Power Shell script. The script is saved as a .pdf file and this is uploaded to LinkedIn's CDN server. If downloaded it would remain undetected.

The second flaw allowed a hacker to create a Windows registry file which contains a malicious PowerShell script and disguise it as a .pdf file. When the victim opens the file received via LinkedIn, the crafted REG containing the malicious payload runs, giving attacker control over the user's machine. From now on, the script will run each time the user logs in to his computer.

The third flaw sees a hacker creating a malicious XLSM file, embedded with Macro, disguised as an XLSX file. The Macro is a scrambled VB script shell code. The masqueraded file passes the anti-virus check and then it is uploaded successfully to LinkedIn's CDN and sent to the victim. When the victim opens the malicious XLSM file, Excel runs the VB scripts and the victim gets infected.

The last flaw is where a hacker creates a malicious DOCX file containing an external object. This object is linked to an HTA file on the attacker's server. The DOCX file is then uploaded successfully to LinkedIn's CDN, passing the virus check and sent to the victim. When the victim opens the malicious DOCX file, WINWORD automatically downloads the HTA file

through the object link, and then runs it. Once the HTA file is executed, the victim is infected.