Fecha: 26 de junio de 2014
Alejandro Asenjo

Herramienta: Kali Linux (Armitage, Social Engineer Toolkit)
Objetivo: buscar la vulnerabilidad y explotarla en Windows 7, y realizar una conexión remota.

Se localizó una vulnerabilidad en "Foxit Reader" que permite crear un "backdoor" en Windows 7, utilizando SET, PAYLOADS, se crea un documento de PDF que contiene un código malicioso para abrir un puerto en Windows y poder acceder sin autorización al equipo destino.

A través de SET se intentó el envío por correo electrónico pero fue detectado por GMAIL, pudiendo tener uno de los siguientes antivirus:

ClamAV	Exploit.Unicode_Mixed	20140626
Jiangmin	heur:Exploit.ShellCode.Gen	20140626
Microsoft	Exploit:Win32/Pidief.gen!D	20140626
Norman	Exploit.ADO	20140626
Qihoo-360	foxit_title_bof	20140626
Symantec	Trojan Horse	20140626

El archivo fue testeado por "virustotal", para detectar cuales antivirus pueden detectarlo.

El envío se realizó por el USB, y se ejecutó en la máquina destino. Volviendo al SET, se intentó realizar la escucha por "SET", "Create a Payload and Listener".

No pudiendo concluir con la prueba. Pero a la vista de los resultados, concluimos que se deben actualizar los programas instalados.