PowerShell y RickyBobby en la filtración de WikiLeaks (Vault 7: CIA Hacking Tools Revealed)

About RickyBobby v4.x.x

(S) RickyBobby 4.x is developed by IOC/EDG/AED/Operational Support Branch (OSB) as a lightweight implant for target computers running newer versions of Microsoft Windows and Windows Server. The RickyBobby implant enables COG operators to upload and download files and execute commands and executables on the target computer without detection as malicious software by personal security products (PSPs). RickyBobby 4.x improves upon previous versions of RickyBobby by being easier to install, task using the Listening Post (LP), and manage multiple implant installations.

(S) RickyBobby 4.x is comprised of several .NET DLLs and a Windows PowerShell script. RickyBobby uses Windows PowerShell to download and dynamically execute the .NET DLLs in memory. OSB chose Windows PowerShell as the execution vector because it is installed by default on all Microsoft's operating systems since Windows Vista and it runs as trusted, Microsoft-signed process. RickyBobby 4.x can be installed remotely or with physical access to the target computers using batch files.