Written by Marco Attard
17 April 2015

Security researcher Cylance uncovers a variation of an old Windows weakness, Reuters reports-- "Redirect to SMB," a potential means for hackers to steal login detains from "hundred of millions" of PCs.

Redirect to SMB is similar to a 1997 vulnerability taking advantage of a Windows and Internet Explorer weakness allowing attackers to trick users into logging into a hacker-controlled server. However, while the previous vulnerability required clicking on a malicious link (from either email or website), the new variant does not even need that, as uses automated login requests sent by applications running in the background.

To do so it takes advantage of Windows Server Message Block (SMB) and 31 different applications, including Adobe Reader, Apple Quick Time, Apple Software Update for ITunes, Box Sync client, Microsoft's Internet Explorer 11, Excel 2010 and Windows Media Player and Symantec Norton Security Scan.

In good news, Cylance says it has only recreated Redirect to SMB in the lab, and it hasn't seen it in the wild, at least so far. On the other hand Microsoft says it already has precautions against the vulnerability.

"Several factors would need to converge for a 'man-in-the-middle' cyberattack to occur. Our guidance was updated in a Security Research and Defense blog in 2009, to help address potential threats of this nature," a Microsoft statement to Reuters reads. "There are also features in Windows, such as Extended Protection for Authentication, which enhances existing defenses for handling network connection credentials."

Go [Security Researchers Claim New Windows Security Weakness (Reuters)]