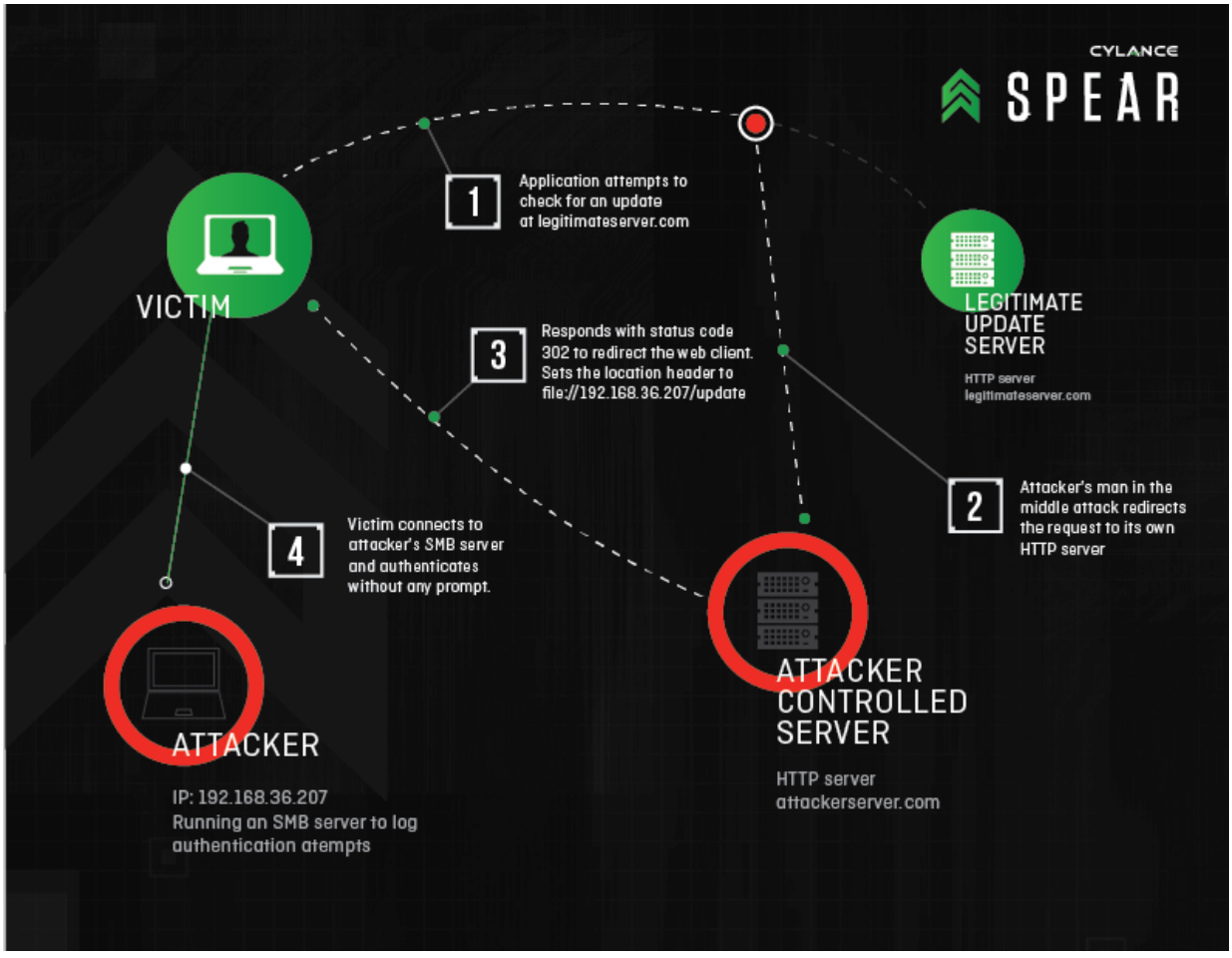
Redirect to SMB vulnerability in Windows discovered

April 14 2015, by Nancy Owano



Credit: Cylance

News stories on tech spots on Monday reported that the Irvine,

California, security company Cylance's SPEAR research team discovered a vulnerability relating to all versions of Windows including the Windows 10 Preview. The vulnerability is called "Redirect to SMB". The technique can be exploited to steal login credentials. "Redirect to SMB" works by "hijacking communications with legitimate web servers via man-in-the-middle attacks, then sending them to malicious SMB (server message block) servers that force them to spit out the victim's username, domain and hashed password," said Cylance.

After testing dozens of applications, Cylance identified 31 vulnerable software packages that can be abused to leak login credentials using this vulnerability. They included popular applications such as Adobe Reader, Apple QuickTime and Windows Media Player, as well as several antivirus, security, team and developer tools. They disclosed this to CERT at Carnegie Mellon University in late February.

The CERT unit of the Software Engineering Institute at Carnegie Mellon University, which tracks computer bugs and internet security issues, issued information about this on Monday. According to a Cylance blog posting by Brian Wallace on Monday, "Carnegie Mellon University CERT disclosed the vulnerability to the public today (#VU672268), following six weeks of working with vendors to help them mitigate the issue."

The CERT information, headlined "Vulnerability Note VU#672268, Microsoft Windows NTLM automatically authenticates via SMB when following a file:// URL," spelled out the problem:

"Software running on Microsoft Windows that utilizes HTTP requests can be forwarded to a file:// protocol on a malicious server, which causes Windows to automatically attempt authentication via SMB to the malicious server in some circumstances. The encrypted form of the user's credentials are then logged on the malicious server. This

vulnerability is alternatively known as 'Redirect to SMB'."

The Cylance team uncovered Redirect to SMB while hunting for ways to abuse a chat client feature providing image previews.

Wallace said that the "Redirect to SMB" is most likely to be used in targeted attacks by advanced actors—attackers must have control over some component of a victim's network traffic.

Bill Rigby of Reuters further explained that if a hacker can get a Windows user to click on a bad link in an email or on a website, "it can essentially hijack communications and steal sensitive information once the user's computer has logged on to the controlled server." Rigby said, though, that in the latest variation of the technique, Cylance said users could be "hacked without even clicking on a link." That could happen if attackers intercepted "automated requests to log on to a remote server issued by applications running in the background of a typical Windows machine, for example, to check for software updates."

Wallace said, "We hope that our research will compel Microsoft to reconsider the vulnerabilities and disable authentication with untrusted SMB servers."

But wait. Microsoft said the threat posed by the purported weakness was not as great as Cylance supposed. Reuters quoted an emailed statement from Microsoft, "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. There are also features in Windows, such as Extended Protection for Authentication, which enhances existing defenses for handling network connection credentials."

Chris Paoli in *GCN*, a site for public-sector IT professionals, pointed out

that "While the Cylance team has been able to provide proof of concept for the flaw, it said that there have been no known attacks using Redirect to SMB."

What does the CERT think of all this? Under the "Solution" heading, the announcement said "The CERT/CC is currently unaware of a full solution to this problem." They said that affected users may consider a number of workarounds: Consider blocking outbound SMB connections (TCP ports 139 and 445) from the local network to the WAN; update NTLM group policy; do not use NTLM for authentication by default in applications; use a strong password and change passwords frequently.

The CERT note thanked Brian Wallace of Cylance for reporting the vulnerability.

More information: blog.cylance.com/redirect-to-smb