Issued 5/18/17

Researcher Finds Way to Steal Windows Login Credentials via Chrome

A security researcher managed to perform an impressive attack that allowed him to gather computer login credentials via Google Chrome and the SMB protocol. While this type of exploits are not new, they're usually limited to local area networks. Another thing that makes this particular attack noteworthy is the fact that there have been no publicly demonstrated SMB authentication related attacks on browsers other than Internet Explorer and Edge in the past decade.

Serbian security researcher Bosko Stankovic of DefenseCode mixed together two different techniques - one taken from the Stuxnet operation, and another that was detailed back in 2015 at the Black Hat security conference. He put together the attack by focusing on SCF files, which stands for Shell Command File, a format that supports a limited set of Windows Explorer commands. These files are similar to LNK files, which when stored on disk will retrieve an icon file. Following the Stuxnet attacks, Microsoft forced LNK files to only load their icons from local resources so they would no longer be vulnerable to attack by making them load malicious code. SCF files, however, were left alone. Stankovic took this information and created a SCF file that loads its icon image from an URL. At the end of that URL stands an SMB server.

Once a computer tries to load that icon from this server, the server asks and receives the user's login credentials as it makes the user's computer think it needs to authenticate. "Due to the non-printable character %0B Chrome will download the response as iwantyourhash.scf file. The moment the download directory containing the file is opened Windows will try to authenticate to the remote SMB server, disclosing the victim's authentication hashes," he explains.

The security researcher advises people to disable automatic downloads n Google Chrome by going to Settings > Show advanced settings > and then check the "ask where to save each file before downloading." "Currently, the attacker just needs to entice the victim (using fully updated Google Chrome and Windows) to visit his web site to be able to proceed and reuse victim's authentication credentials.

Even if the victim is not a privileged user (for example, an administrator), such vulnerability could pose a significant threat to large organizations as it enables the attacker to impersonate members of the organization. Such an attacker could immediately reuse gained privileges to further escalate access and perform attacks on other users or gain access and control of IT resources.