kindred

Security Newsletter

22 May 2017

Just by accessing a folder containing a malicious SCF file, a user will unwittingly share his computer's login credentials with an attacker via Google Chrome and the SMB protocol. SCF stands for Shell Command File and is a file format that supports a very limited set of Windows Explorer commands, such as opening a Windows Explorer window or showing the Desktop. The "Show Desktop" shortcut we all use on a daily basis is an SCF file.

Just like LNK files (shortcuts), SCF files, when stored on disk, will retrieve an icon file when the user loads the file in a Windows Explorer window. For many years, LNK files were allowed to store the location of their icon file inside a DLL or at an URL. After the Equation Group (cough, NSA, cough) used the ability to load malicious code via LNK files in the Stuxnet attacks, Microsoft patched LNK files to load their icons only from local resources. The same was not done for SCF files, which were not included in this patch, still being possible to load the icon of an SCF file from the Internet.

When the user has navigated to a folder containing a malicious SCF file, in milliseconds, the OS will read the SCF file and give away the user's credentials in the form of a NTLMv2, NTLMv1, or LM password hash. Many open-source tools that can crack these types of password hashes.

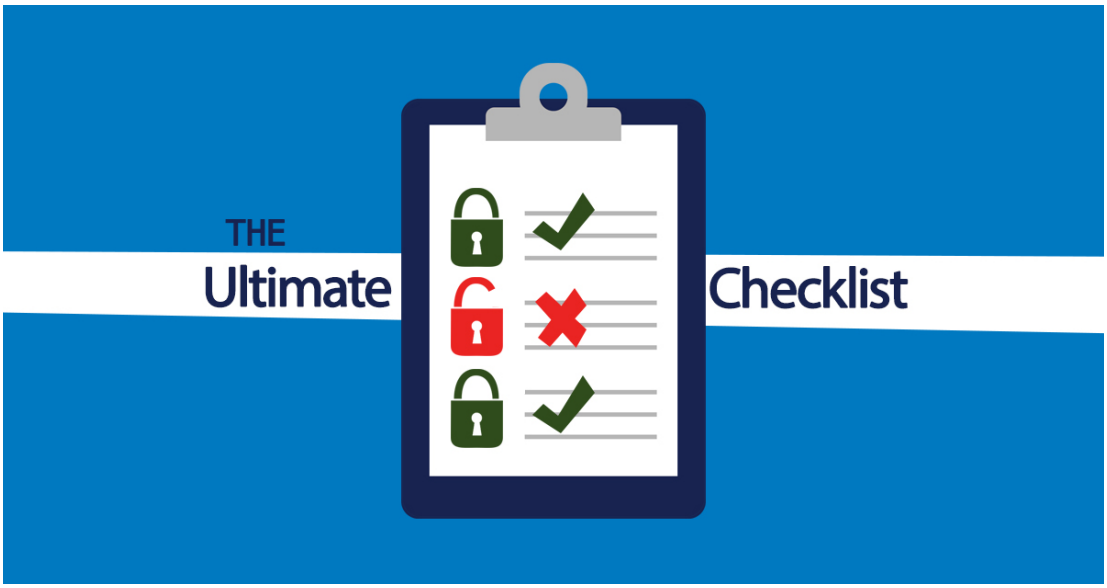
But this wouldn't be a problem if users wouldn't have malicious SCF files on their computers. Here is where Google Chrome comes in, in its default configuration, Chrome will automatically download files that it deems safe without prompting the user, this is the case for SCF files.

As a way to mitigate these types of attacks, you can change the default behaviour in *Settings -> Show advanced settings -> Ask where to save each file before downloading*. More advanced protection measures include blocking outbound SMB requests via firewalls, so local computers can't query remote SMB servers.

Read More

Tech Details

Web Developer Security Checklist



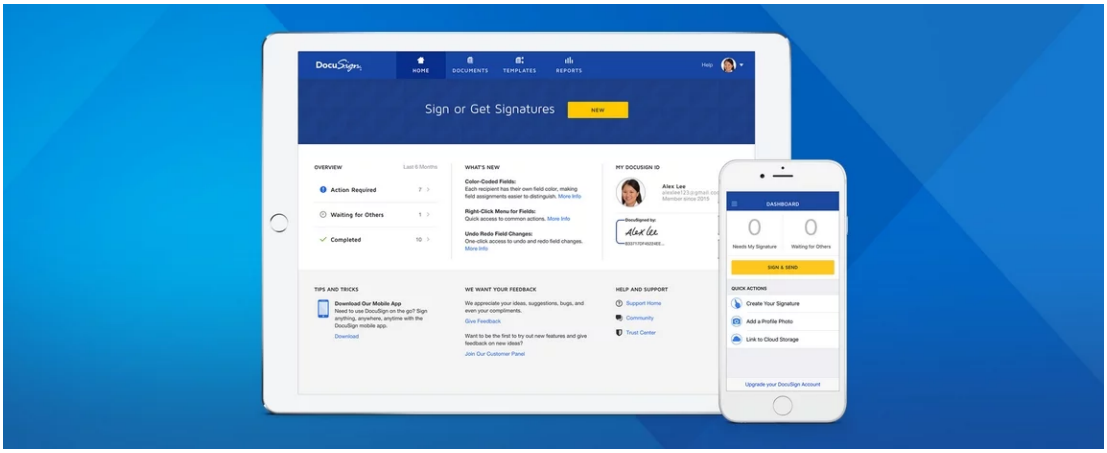
Developing secure, robust web applications in the cloud is hard. Michael O'Brien shares a security checklist for web developers so that you don't forget anything crucial in your next projects.

After you review the checklist below, you may acknowledge that you are skipping many of these critical security issues. This checklist is simple, and by no means complete. It is a list of some of the more important issues you should consider when creating a web application.

Note from the curator: While I could nit-pick on some items – for example I would say that a password needs to be long and ***unique****, not necessarily "random", as a long passphrase you've made up yourself can do wonders and is way easier to remember – this checklist is a nice summary of important security steps to think about during development and deployment phase.*

Read More

DocuSign Admits Data Breach That Led to Recent Spam Campaigns



DocuSign, a major provider of electronic signature technology, acknowledged today that a series of recent malware phishing attacks targeting its customers and users was the result of a data breach at one of its computer systems.

The company stresses that the data stolen was limited to customer and user email addresses, but the incident is especially dangerous because it allows attackers to target users who may already be expecting to click on links in emails from DocuSign.

DocuSign was already a perennial target for phishers and malware writers, but this incident is likely to intensify attacks against its users and customers. DocuSign says it has more than 100 million users, and it seems all but certain that the criminals who stole the company's customer email list are going to be putting it to nefarious use for some time to come.

Read More

Even More

WannaCry is getting a lot of siblings: Meet Adylkuzz and Uiwix

On Friday, May 12, attackers spread a massive ransomware attack worldwide using the EternalBlue exploit to rapidly propagate the malware. his particular attack also appeared to use an NSA backdoor called DoublePulsar to actually install the ransomware known as WannaCry.

Over the subsequent weekend, however, Proofpoint discovered another very large-scale attack using both EternalBlue and DoublePulsar to install the cryptocurrency miner Adylkuzz. Initial statistics suggest that this attack may be larger in scale than WannaCry: because this attack shuts down SMB networking to prevent further infections with other malware via that same vulnerability. It should be noted that the Adylkuzz campaign significantly predates the WannaCry attack, beginning possibly as early as April 24. This attack is ongoing.

Uiwix is currently infecting victims using the EternalBlue exploit and looks more advanced. Rather than the ransomware being self-propagating like WannaCry, the developers of Uiwix are most likely scanning for and using a script that infects vulnerable computers. When a victim becomes infected with the ransomware, it will not be written to disk. Instead this ransomware will run directly from memory. This makes it difficult for most security programs to properly detect and block it.

This is why it is so important that everyone makes sure the MS17-010 security updates released by Microsoft for the EternalBlue vulnerability are installed. If you are no longer using a supported Windows version, Microsoft has released updates for Windows XP, Windows 8, and Windows Server 2003, which typically no longer receive security updates.

Read More about Adylkuzz

Read more about Uiwix

Vault 7: CIA Co-Developed Athena Malware with US Cyber-Security Company

WikiLeaks' newest Vault 7 release, titled Marble Framework, discusses a host of tools used to hide the CIA's tracks.

It does this in a very unique way, however, by replacing the code for a given malware program with another language AND its encoding equivalent, including such languages as Chinese, Russian, Korean, Arabic and Farsi. This then gives CIA malware the appearance of having originated from one of these language groups as a means to throw off forensic investigators.

In addition, Marble Framework may have provided support for sending encrypted communications as well. This release is unique for WikiLeaks in that it is not an actual set of Wiki pages or emails. Rather, this is a .zip file containing literal source code to components of Marble Framework.

Next time you see an article stating that an attack comes from Russia because they've found comments in Cyrillic or something similar, think twice.

Read More

Previous Vault7 releases

WannaCry Ransomware Decryption Tool Released; There is hope...if you did not reboot.

If your PC has been infected by WannaCry – the ransomware that wreaked havoc across the world last Friday – you might be lucky to get your locked files back without paying the ransom of $300 to the cyber criminals. French security researcher from Quarkslab, has discovered a way to retrieve the secret encryption keys used by the WannaCry ransomware for free, which works on Windows XP, Windows 7, Windows Vista, Windows Server 2003 and 2008 operating systems.

There is a catch though: if you have restarted you're computer since the attack, you're out of luck. To prevent the victim from accessing the private key and decrypting locked files himself, WannaCry erases the key from the system, leaving no choice for the victims to retrieve the decryption key except paying the ransom to the attacker. However, it does not erase the does not erase the prime numbers used to create the key from memory.

Based on this finding, Guinet released a WannaCry ransomware decryption tool, named WannaKey, that basically tries to retrieve the two prime numbers, used in the formula to generate encryption keys from memory. Although the tool won't work for every user due to its dependencies, still it gives some hope to WannaCry's victims.

Read More

Penetration testing AWS storage: Kicking the S3 bucket

In this instalment, we'll look at an Amazon Web Service (AWS) instance from a no-credential situation and specifically, potential security vulnerabilities in AWS S3 "Simple Storage" buckets.

After walking through the AWS S3 methodology, we'll apply that to the Alexa top 10,000 sites to identify the most popular AWS users for these vulnerabilities. Each site with open S3 permissions has been contacted by Rhino Security Labs in advance for remediation.

If you like to know more about common AWS security flaws and misconfiguration, have a look at flaws.cloud, this website will lead you to better practice through funny security challenges.

Read More

Learn AWS security with challenges

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.