Security Newsletter

12 June 2017

This powerPoint file downloads malware when you hover a link, no macros required

A new social engineering attack has been discovered in the wild, which doesn't require users to enable macros; instead it executes malware on a targeted system using PowerShell commands embedded inside a PowerPoint (PPT) file. The malicious PowerShell code triggers as soon as the victim moves/hovers a mouse over a link, which downloads an additional payload on the compromised machine -- even without clicking it.

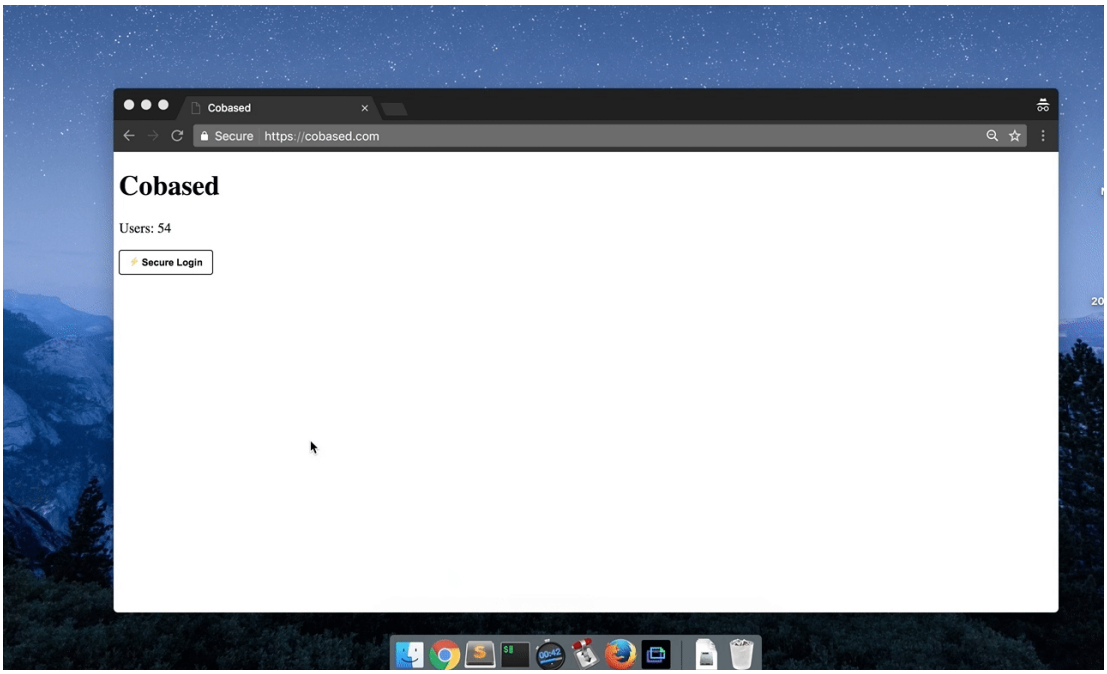
The PowerPoint files have been distributed through spam emails with subjects like "Purchase Order" and "Confirmation," which when opened, displays the text "Loading...Please Wait" as a hyperlink.

Fortunately the Protected View security feature that comes enabled by default in most supported versions of Office, including Office 2013 and Office 2010, displays a severe warning and prompts them to enable or disable the content. The security firm also said that the attack doesn't work if the malicious file is opened in PowerPoint Viewer, which refuses to execute the program. But the technique could still be efficient in some cases.

Read More

Original statement

SecureLogin — Forget About Passwords



SecureLogin is a decentralized authentication protocol for websites and apps. Classic passwords/2FA are poorly designed, hard to backup and inconvenient to use. SecureLogin is an all-in-one solution that creates a cryptographic private key from your email and master password to sign in everywhere and helps you to forget about passwords.

SecureLogin is not a new OAuth, not a password manager, not a new 2FA option. It's trying to be all three in one protocol. SecureLogin leverages deterministic password generation combined with a decentralized authentication scheme.

The author did his best to make the solution easy to use, login apps are available for all "major" client platforms (MacOs, iOS, Android, Windows 10). It will be interesting to see if this new concept will find its way to the market, between password managers, social connect buttons and other alternatives such as U2F.

Announce

Official webpage

Github Page

Researchers Port NSA EternalBlue Exploit to Windows 10

Experts at RiskSense have ported the leaked NSA exploit named ETERNALBLUE for the Windows 10 platform. This is the same exploit that was used by the WannaCry ransomware as part of its SMB self-spreading worm in the mid-May WannaCry outbreak that affected over millions of computers across the world.

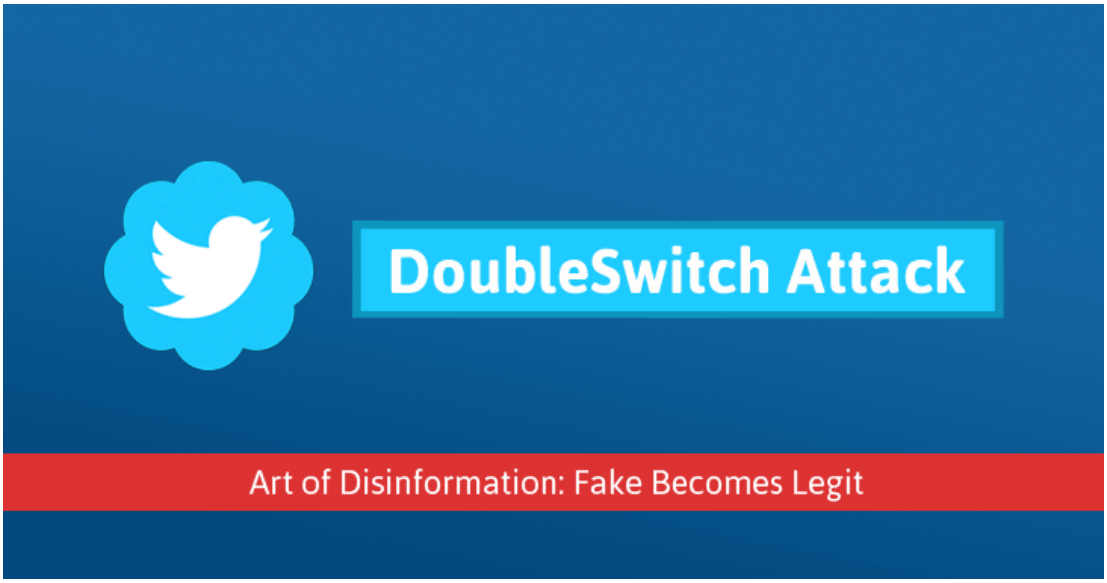
This ETERNALBLUE port only works against Windows 10 versions before the Redstone 1 release (April 2016). Furthermore, these older versions must have not received the MS17-010 security patch, which Microsoft released in March 2017. While this prevents the Windows 10 port of ETERNALBLUE to work on cutting-edge Windows 10 versions, there are still many older versions that are vulnerable to attacks.

Besides porting ETERNALBLUE to target Windows 10, the RiskSense crew also managed to remove DOUBLEPULSAR from the ETERNALBLUE exploitation chain. All Windows users should make sure they've installed the updates included in Microsoft's MS17-010 security bulletin.

Read More

MS17-010 Security Bulletin

Hackers Are Using An Effective Way to Spread Fake News From Verified Accounts



Now, researchers have uncovered a new, cunning attack technique currently being used by hackers to take over verified Twitter accounts and rename them to influential people in order to spread fake news. Dubbed DoubleSwitch, the attack begins with a simple account takeover, but then the hackers change the username and display name with the one having a large influence on social media.

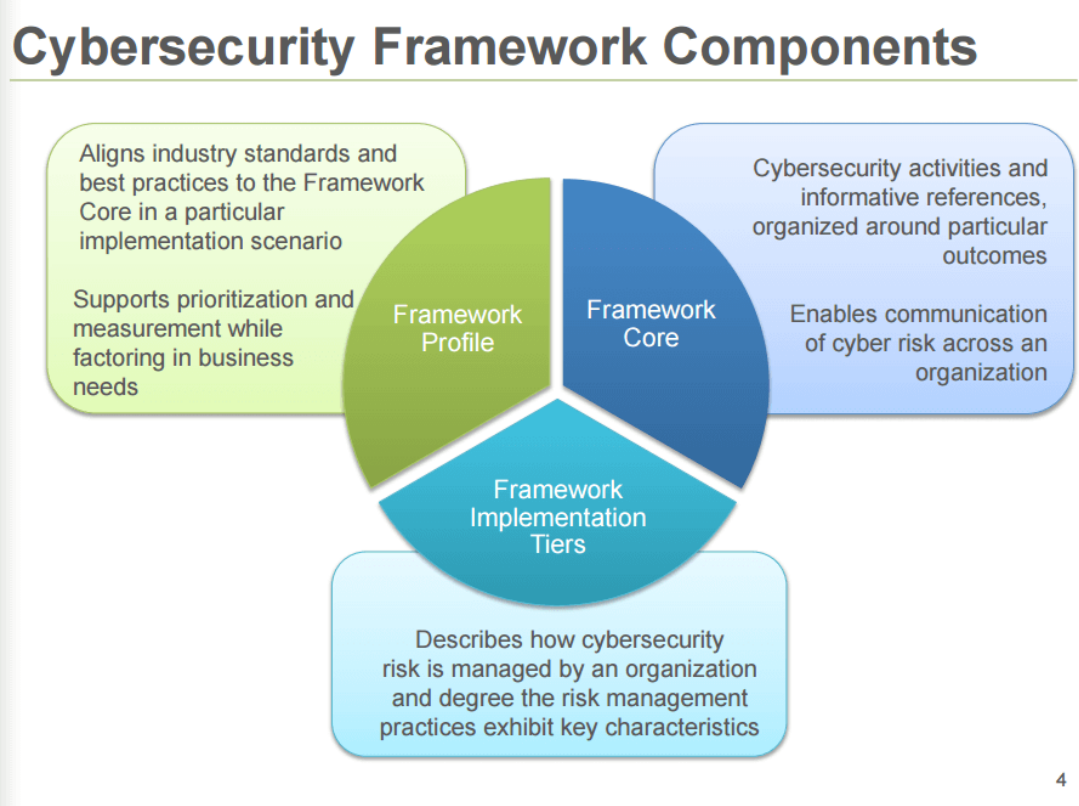
This attack was discovered when two journalists — Milagros Socorro and Miguel Pizarro, a member of Venezuela's parliament — were hacked and then renamed. The hacker then registered a new account, resembling with their original profiles, under the original usernames (Twitter handles), but using the attacker's controlled email addresses.

This means, every time victims try to recover their accounts using regular password reset option, the confirmation emails will be sent to the hijacker, who pretends that the issue has been resolved, making it almost impossible for the victims to recover their account.

Hackers then use hijacked verified accounts, but renamed to another influence, to feed fake news to the millions of followers of the original accounts. While it's unclear how the hackers managed to hijack the verified users at the first place, it is believed that the attack begins with malware or phishing attacks.

Read More

Your Essential Guide to Cyber Liability Insurance



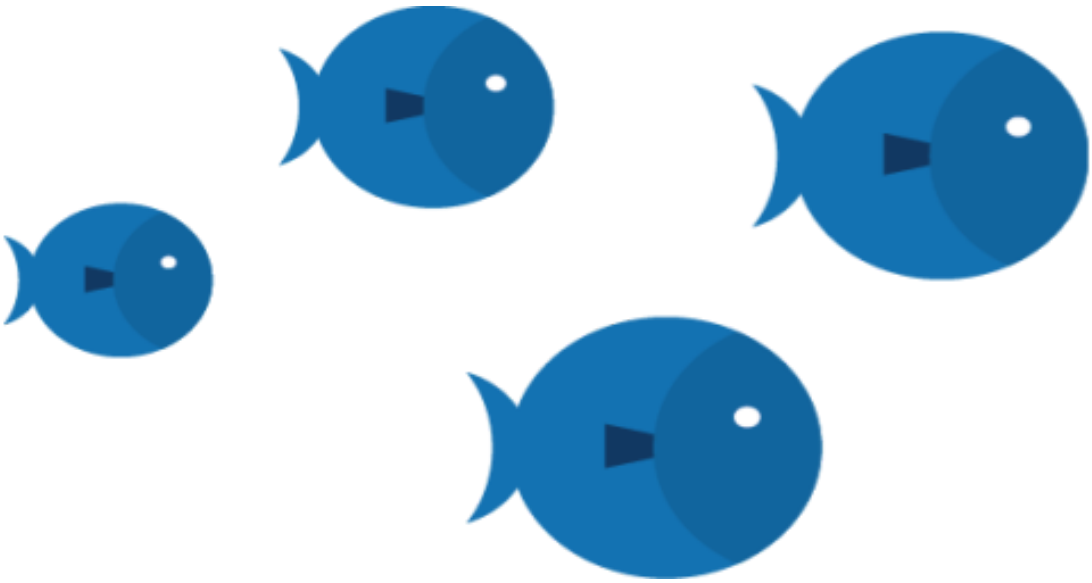
Small and medium companies get broken into just as frequently as big ones, they're just not important enough to generate the news. For these fledgling businesses, a severe hacking can eat up a year's worth of profit or even bankrupt them altogether.

To protect against these unpredictable situations, your company should consider a cyber security liability insurance policy. A well negotiated one can cover most, if not all, of the damage caused by a cyber attack.

This article will go through the basics of setting up a cyber liability insurance for your company.

Read More

Domain Shadowing: Some of your subdomains may be taken over by somebody else



Do you know that it's possible that some of your subdomains maybe taken over by somebody else? This is due to the fact, that for some of your DNS records (mainly CNAME) you enabled zone delegation.

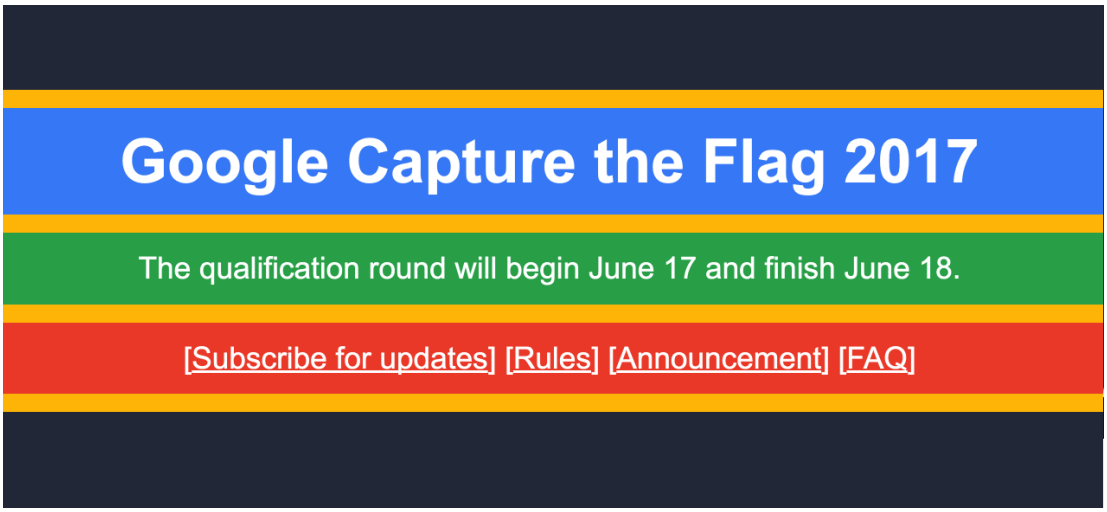
A subdomain takeover is considered a high severity threat and boils down to the registration of a domain by somebody else (with bad intentions) in order to gain control over one or more (sub)domains.

This presents an interesting attack vector, which can even lead to several high severity risks, like this authentication bypass explained in a bug bounty report by Arne Swinnen.

Read More

Even More

Announcing Google Capture the Flag 2017



On 00:00:01 UTC of June 17th and 18th, 2017 Google will be hosting the online qualification round of their second annual Capture The Flag (CTF) competition. Top 10 finalist teams will be invited to Google offices to compete onsite for a prize pool of over USD$31,337

In a 'Capture the Flag' competition we create security challenges and puzzles in which contestants can earn points for solving them.

At the Google CTF last year the winning team, 'Pasten' from Israel, earned over 4,700 points competing against 2,400 teams out of which 900 were able to solve at least one of our challenges.

Read More

CTF Page

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.