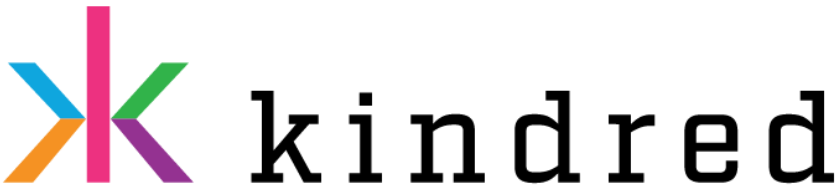
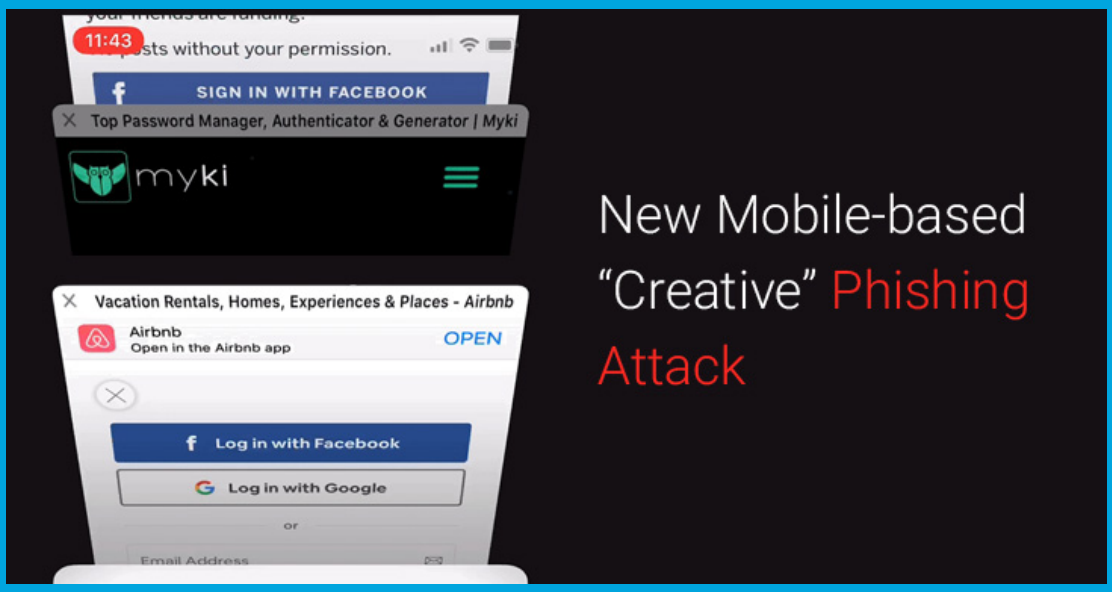


Security Newsletter

18 March 2019

Subscribe to this newsletter

New 'Creative' Phishing Attack You Really Should Pay Attention To



A cybersecurity researcher who last month warned of a creative phishing campaign has now shared details of a new but similar attack campaign with The Hacker News that has specifically been designed to target mobile users. Just like the previous campaign, the new phishing attack is also based on the idea that a malicious web page could mimic look and feel of the browser window to trick even the most vigilant users into giving away their login credentials to attackers.

As you can see in the video, a malicious website that looks like Airbnb prompts users to authenticate using Facebook login, but upon clicking, the page displays a fake tab switching animation video aimed to trick users into thinking that their browsers are behaving normally. If users are not very attentive to details and fail to spot minor differences, they would eventually end up filling the username and password fields on the phishing page, resulting in giving away their social media credentials to the attackers.

It should be noted that such advanced phishing attacks are not limited to Facebook, Safari browser or just to iOS mobile users only, but could very easily be adapted to target Android devices or any other social media site as well.

Since there are no clear guidelines to spot such creative phishing attacks, users are highly recommended to 1/ Use password managers that only auto-fill credentials on legit domains, helping you avoid giving away credentials to fake websites. 2/ Enable two-factor authentication, wherever available, preventing hackers from accessing your online accounts even if they somehow manage to steal your credentials. 3/ Ssk themselves "Why am I asked to log in?" Or "Am I not already logged in to this?"

Read More on TheHackerNews

Even More on Myki's Blog

New WordPress Flaw Lets Unauthenticated Remote Attackers Hack Sites

If for some reason your WordPress-based website has not yet been automatically updated to the latest version 5.1.1, it's highly recommended to immediately upgrade it before hackers could take advantage of a newly disclosed vulnerability to hack your website.

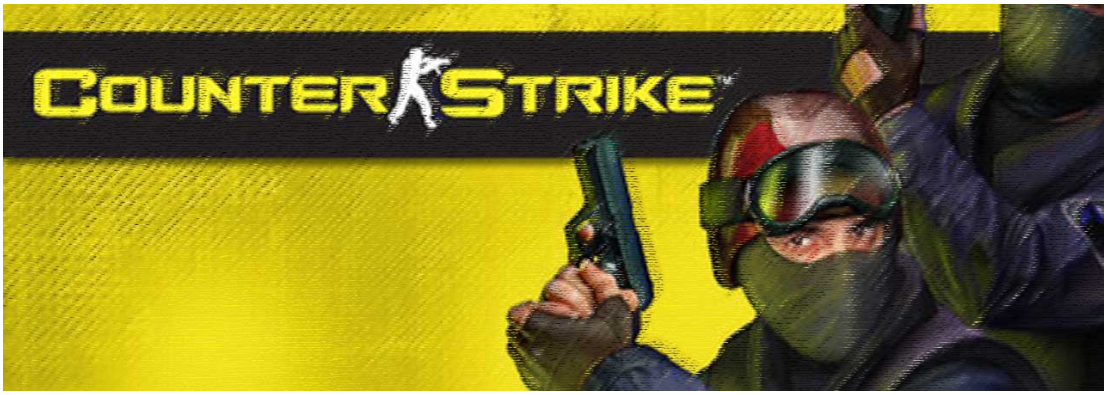
The flaw stems from a cross-site request forgery (CSRF) issue in the Wordpress' comment section, one of its core components that comes enabled by default and affects all WordPress installations prior to version 5.1.1. Unlike most of the previous attacks documented against WordPress, this new exploit allows even an "unauthenticated, remote attacker" to compromise and gain remote code execution on the vulnerable WordPress websites.

According to the researcher, the attacker can then even take complete control over the target WordPress websites remotely by injecting an XSS payload that can modify the WordPress template directly to include a malicious PHP backdoor—all in a single step without the administrator noticing. Since WordPress automatically installs security updates by default, you should already be running the latest version of the content management software. However, if the automatic updating of your CMS has been turned off, you are advised to temporarily disable comments and log out of your administrator session until the security patch is installed.

Read More on TheHackerNews

Even More on BleepingComputer

39% of All Counter-Strike 1.6 Servers Used to Infect Players



When playing a video game, most people do not worry about getting infected by the their game client. New research, though, shows that's exactly what is happening when 39% of all existing Counter-Strike 1.6 game servers were trying to infect players through vulnerabilities in the game client.

Security researchers have discovered a network of malicious Counter-Strike 1.6 multiplayer servers that exploited remote code execution (RCE) vulnerabilities in users' gaming clients to infect them with a new malware strain named Belonard. The network has been shut down.

The person behind the botnet would then use the Belonard malware to make modifications to users' CS1.6 clients and show ads inside users' games. But above all, the trojan was primarily used to promote legitimate CS1.6 multiplayer servers by adding them to the users' available server list, which the Belonard developer would do for a fee.

Users can recognize Belonard's proxy servers because of a bug in its code that displayed the server game type as "Counter-Strike 1," "Counter-Strike 2," or ""Counter-Strike 3" instead of the standard "Counter-Strike 1.6." Unfortunately, the only way to prevent this botnet from being created again is to patch the vulnerabilities in the client. As Counter-Strike 1.6 was the last client to be released by Valve, a fix is not expected to be forthcoming.

Read More on ZDNet

Even More on BleepingComputer

More #News

- Citrix Data Breach – Iranian Hackers Stole 6TB of Sensitive Data
- New BitLocker attack puts laptops storing sensitive data at risk
- Multiple Security Flaws Discovered in Visitor Management Systems, including Envoy
- GPS Spoof Hits Geneva Motor Show
- MageCart: Malicious Javascript Active on FILA UK and Other Websites
- These Cookie Warning Shenanigans Have Got to Stop

- Multi-Factor Auth Bypassed in Office 365 and G Suite IMAP Attacks
- Two-thirds of all Android antivirus apps are frauds
- Breach of 'Verifications.io' Exposes 763 Million Records
- Unsecured Database Exposed 33 Million Job Profiles in China
- Deprecate download in ad frames without user gesture
- Google Now Lets G Suite Admins Disable Insecure Phone 2FA
- Equifax Was Aware of Cybersecurity Weaknesses for Years, Senate Report Says
- Creepy Database Lists 'BreedReady' Status for 1.8 Million Women
- Georgia County Pays $400,000 to Ransomware Attackers
- Multi-Factor Auth Bypassed in Office 365 and G Suite IMAP Attacks
- Report – Gearbest Hack: Hundreds of Thousands Affected Daily by Huge Data Breach

#Patch Time!

- Patch Tuesday, March 2019 Edition
- Windows security updates that require new registry keys
- WordPress 5.1.1 Security and Maintenance Release
- Severe Flaw Disclosed In StackStorm DevOps Automation Software
- Adobe Releases Patches for Critical Flaws in Photoshop CC and Digital Edition
- Windows 10 Now Automatically Uninstalls Updates That Cause Problems
- Patched WinRAR Bug Still Under Active Attack—Thanks to No Auto-Updates
- Windows file activity monitoring

#Tech and #Tools

- Call For Papers (CFP) directory for Security Conferences
- The Definitive 2019 Guide to Cryptographic Key Sizes and Algorithm Recommendations
- Local privilege escalation via the Windows I/O Manager: a variant finding collaboration
- Shr3dKit: Red Team Tool Kit
- An Exercise in Practical Container Escapology
- Extracting Bitlocker keys from a TPM
- Millions of Binaries Later: a Look Into Linux Hardening in the Wild
- Hubble is a modular, open-source security compliance framework.
- Tiger: The Unix security audit and intrusion detection tool
- DLL Hijacking & Ghidra
- Penetration Testing Active Directory, Part II
- Silencing Cylance: A Case Study in Modern EDRs

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 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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.

You can access the previous newsletters at https://news.infosecgur.us