Security Newsletter

8 May 2017

Password reuse: Another company got breached, YOU should worry!

There's a lot of stuff getting hacked and a lot of credentials floating around the place, but then what? I mean what do evil-minded people do with all those email addresses and passwords? Among other things, they attempt to break into accounts on totally unrelated websites.

As fallible humans, we reuse passwords. We've all done it at one time or another and most people are just out there YOLO'ing away with the same password or three across all their things. Hackers know that too. As such, they're going to try and break into as many other accounts as they can using the credentials from a data breach. Which brings us to credential stuffing.

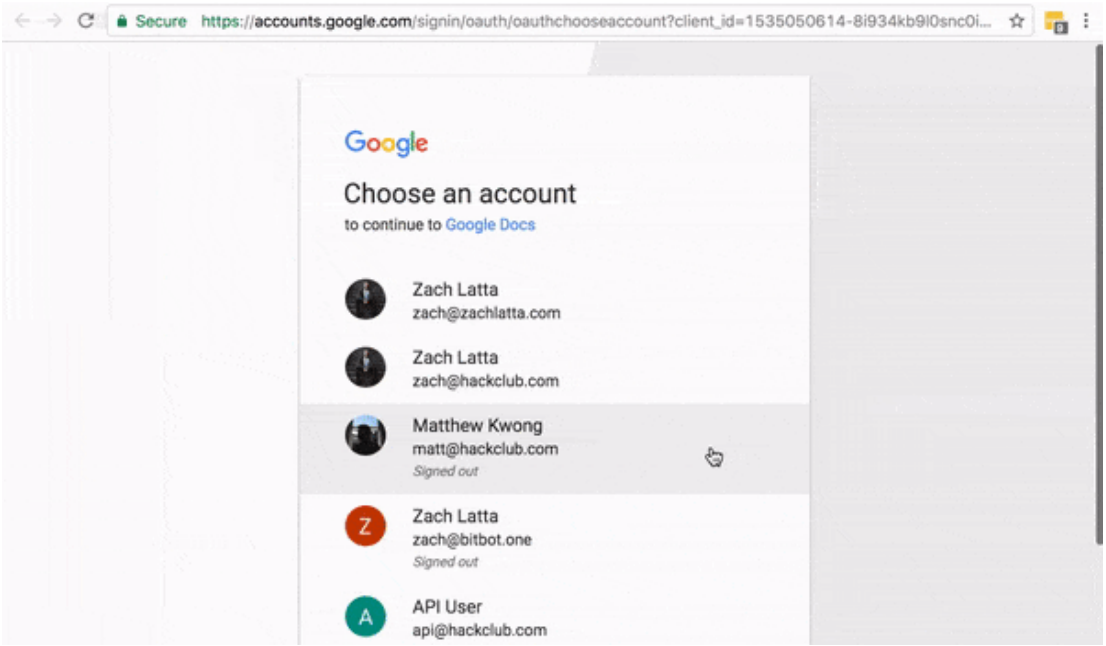
Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. Large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.

Over 1 billion breached accounts have been loaded into the breach notification service HaveIBeenPwned (HIBP). These are from 2 different "combo lists", collections of email addresses and passwords from all sorts of different locations. Troy Hunt has verified their accuracy (including his own record in one of them) and many hundreds of millions of the email addresses are not already in HIBP. Because of the nature of the data coming from different places, if you're in there then treat it as a reminder that your data is out there circulating around and that you need to go and get yourself a password manager and create strong, unique passwords.

If one of your clients credentials got leaked from another website, chances are they used the same password on your service! Companies like Spotify started programs to actively look for new data breaches and make sure they're client are not impacted. What are you doing to protect them?

Read More

Gmail Oauth-based phishing. Traditional advice don't cut it!



Google customers have been targeted with a phishing attack that gave hackers access to the contents of emails, contact lists and online documents of victims. The attack tricked victims into clicking a link that gave attackers access through OAuth authentication connections commonly used by third-party applications. The attackers did so by sending victims lure messages, coming from previously infected contacts you know, claiming to contain links to a shared Google Doc.

On opening the link, Google's login and permissions page asked users to grant the fake Docs app the ability to "read, send, delete and manage your email", as well as "manage your contacts", using the OAuth protocol we described in the featured article last week. Once the malicious service got access to the user's mailbox, it would send the scam to his/her whole contact list, using the user's email account.

Google has now shut down the attack, but it could return in a different form. A sign of the scam is the extensive permissions it asks for. Most applications, especially Google-run ones, will not ask for the ability to delete and send email addresses on a users' behalf. Users should make sure they always read what is being requested before granting permission. If you have already given the scammers access to your account, you can still revoke the privilege in the "permissions" section of your Google account.

This new phishing techniques, using OAuth permissions instead of credentials, is concerning as classic advice don't cut it. The URL you get asked for permission is a legit address from Google, and changing your password once you detect you've been victim won't revoke access. Time to update your awareness campaign!

Read More

Google Security Checkup

WordPress Zero-Day Could Expose Password Reset Emails

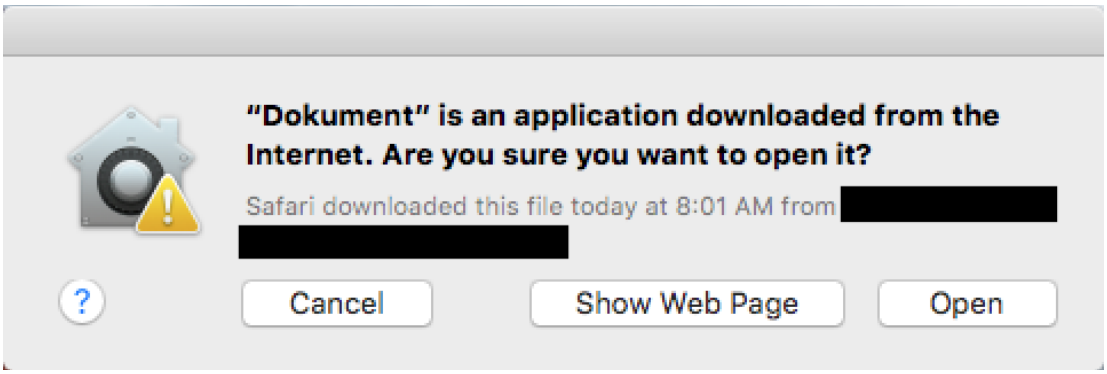
WordPress is a free and open-source content management system (CMS) based on PHP and MySQL. Wordpress has a password reset feature that contains a vulnerability which might in some cases allow attackers to get hold of the password reset link without previous authentication. Such attack could lead to an attacker gaining unauthorised access to a victim's WordPress account.

The vulnerability stems from WordPress using untrusted data by default when creating a password reset e-mail that is supposed to be delivered only to the e-mail associated with the owner's account. Depending on the configuration of the mail server, it may result in an email that gets sent to the victim WordPress user with a malicious From/Return-Path address set in the email headers.

Attacker can perform a prior DoS attack on the victim's email account/server, in order to prevent the password reset email from reaching the victim's account and bounce back to the malicious sender address that is pointed at the attacker. An alternative would be targeting emails with "out of office" setup. Autoresponders might attach a copy of the email sent in the body of the auto-replied message (no user interaction required)

Read More

New OSX.Dok malware intercepts web traffic



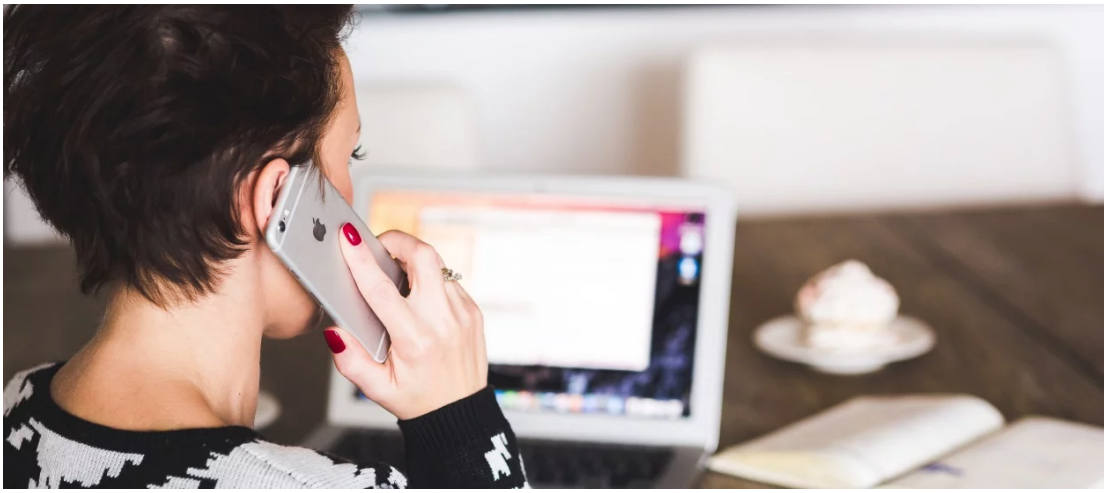
Most Mac malware tends to be unsophisticated. Although it has some rather unpolished and awkward aspects, a new piece of Mac malware, dubbed OSX.Dok, breaks out of that typical mold. OSX.Dok, which was discovered by Check Point, uses sophisticated means to monitor—and potentially alter—all HTTP and HTTPS traffic to and from the infected Mac. This means that the malware is capable, for example, of capturing account credentials for any website users log into, which offers many opportunities for theft of cash and data.

OSX.Dok comes in the form of a file named Dokument.zip, which is found being emailed to victims in phishing emails. This “document” is, of course, actually an application. After several minutes, the app will obscure the entire screen with a fake update notification.

Fortunately, when the user attempts to open this app, the macOS will display a standard notification to warn the user. Apple has already revoked the certificate used to sign the app, so, at this point, anyone who encounters this malware will be unable to open the app and unable to be infected by it.

Read More

Hackers Use Flaws in Telephony Core Protocol to Bypass 2FA on Bank Accounts



Hackers have exploited decades-old flaws in the SS7 mobile telephony protocol to hijack phone numbers and SMS messages, in order to bypass two-factor authentication (2FA) and steal money from bank accounts.

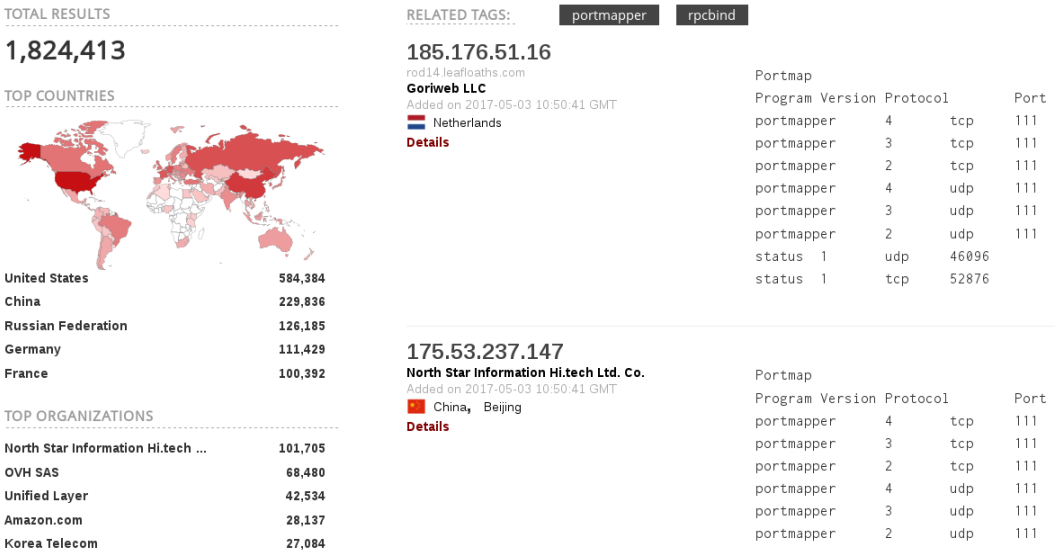
The SS7 (Signalling System No. 7) protocol was developed in 1975 and is a so-called telephony signaling protocol, used to route calls between different telephony providers. SS7's woeful security was brought up again this week after a German bank and telecom confirmed unauthorized wire transfers from a victim's accounts.

According to the German newspaper, crooks first obtained the victim's credentials for his banking account, then used the SS7 flaws to hijack his phone number and receive the transaction confirmation code on the attacker's device.

Everyone's accounts protected by text-based two-factor authentication, such as bank accounts, are potentially at risk until the FCC and telecom industry fix the devastating SS7 security flaw.

Read More

RPCbomb: remote rpcbind denial-of-service



This vulnerability allows an attacker to allocate any amount of bytes (up to 4 gigabytes per attack) on a remote rpcbind host, and the memory is never freed unless the process crashes or the administrator halts or restarts the rpcbind service.

Attacking a system is trivial; a single attack consists of sending a specially crafted payload of around 60 bytes through a UDP socket. This can slow down the system's operations significantly or prevent other services (such as a web server) from spawning processes entirely.

Shodan reports 1.8 million hosts serving on port 111 (rpcbind). Many of those appear to be Amazon AWS instances and other mass hosting services where the owner is presumably using their default Linux distribution configuration that leaves rpcbind open to the internet.

Read More

The Quest for the Universal Fingerprint

Researchers are working towards a "universal fingerprint" - a master pattern (or small number of master patterns) that ring enough bells to unlock any of today's fingerprint readers. They are currently have an approach that takes partial impressions and combines them until it "matches enough" to unlock a phone (or otherwise match a biometric reader) - essentially a dictionary attack against your fingerprint. They are currently at a 65% success rate, but of course that can only get better.

Their advice? Get better readers (that can read depth of fingerprint patterns, add in heartbeat sensors etc), or combine multiple authentication mechanisms if your plan needs to account for attacks of this type.

Add this to the well-known fact that once compromised, you cannot revoke your fingerprints, or change them either. If a successful and simple fingerprint attack is possible, either we need to look at better fingerprint readers going forward, or this takes fingerprint authentication off the table entirely.

Read More

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.