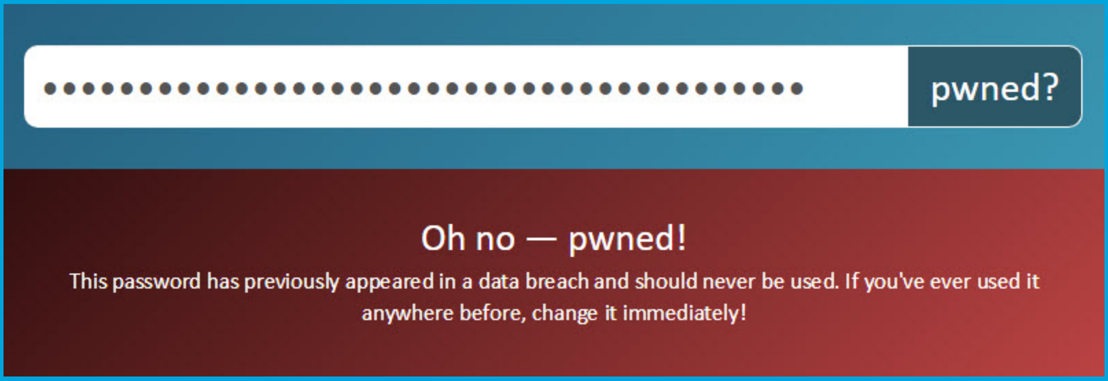
kindred

Security Newsletter

7 August 2017

Introducing 306 Million Freely Downloadable Pwned Passwords



Oh no — pwned!

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it immediately!

This blog post introduces a new service I call "Pwned Passwords", gives you guidance on how to use it and ultimately, provides you with 306 million passwords you can download for free and use to protect your own systems.

Last week Troy Hunt wrote about Passwords Evolved: Authentication Guidance for the Modern Era with the aim of helping those building services which require authentication to move into the modern era of how we think about protecting accounts. In that post, I talked about NIST's Digital Identity Guidelines which were recently released. Of particular interest to me was the section advising organisations to block subscribers from using passwords that have previously appeared in a data breach.

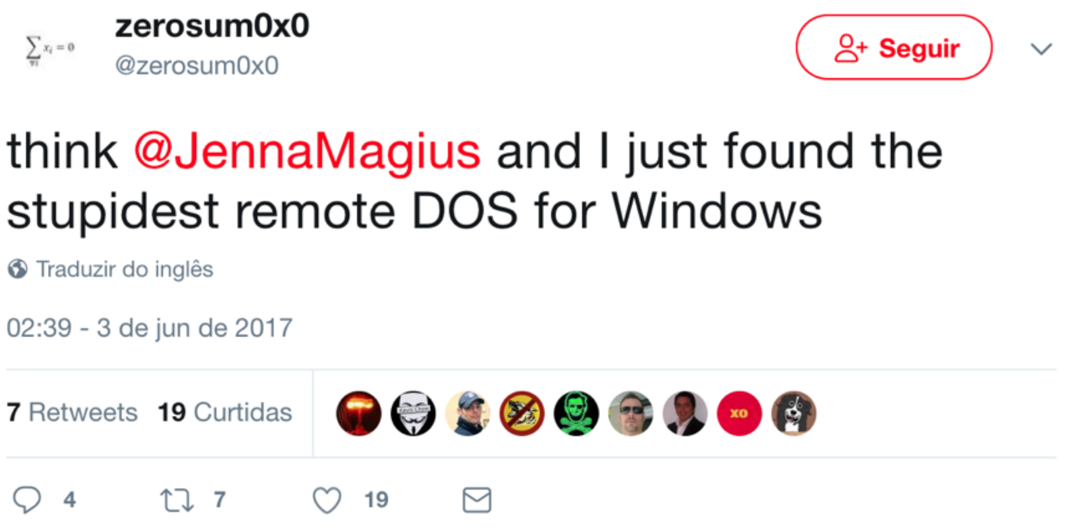
People will probably come up with other ways of using this data. Perhaps, for example, a Pwned Password is only allowed if multi-step verification is enabled. Maybe there are certain features of the service that are not available if the password has a hit on the pwned list. Or consider whether you could even provide an incentive if the user proactively opts to change a Pwned Password after being prompted. As an example, MailChimp provides a 10%discount if you enabled 2FA.

It goes without saying (although he said it anyway in his article page), but don't enter a password you currently use into any third-party service like this! Even if Troy Hunt is saying he does not explicitly log them and he is quite well known in the industry, don't.

Read More

HIBP Password check

SMBLoris: DoS vulnerability affecting all SMB version, from Windows 2000 to Windows 10



zerosum0x0
@zerosum0x0

think @JennaMagius and I just found the stupidest remote DOS for Windows

02:39 - 3 de jun de 2017

7 Retweets 19 Curtidas

"SMBLoris" is a proof-of-concept exploit that takes advantage of a vulnerability in the implementation of SMB services on both Windows and Linux, enabling attackers to "kill you softly" with a clever, low-profile application-level denial of service (DoS). This vulnerability impacts all versions of Windows and Samba (the Linux software that provides SMB services on that platform) and Microsoft has stated that is has no current intention to provide a fix for the issue.

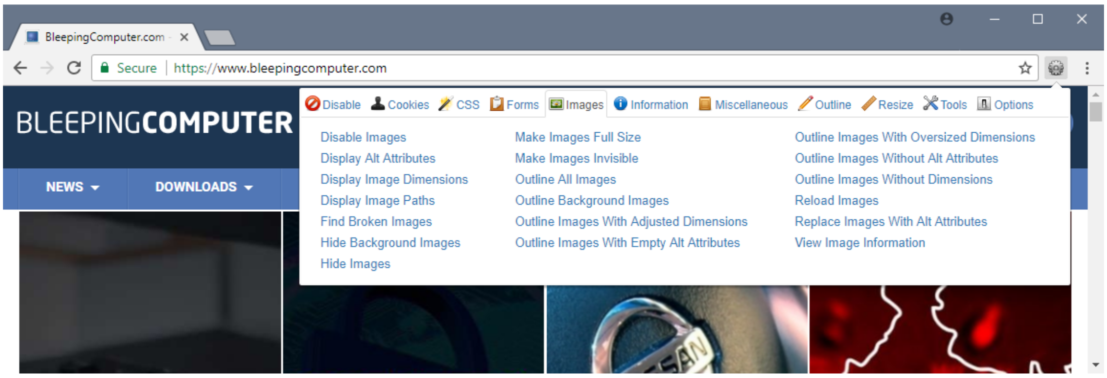
This means that the current situation is that all Windows systems exposing port 445 and the majority of Linux systems exposing port 445 are vulnerable to this application-level denial of service attack. If the attack is successful, the system being attacked will need to be rebooted and will still be vulnerable. Researchers have noted that this vulnerability is similar to one from 2009 — Slowloris — that impacted different types of systems with the same technique. It appears, however, that SMBLoris can have a much faster negative impact even on Windows systems with robust hardware configurations.

Your internal systems are also vulnerable to this attack as most organizations do not implement granular controls over port 445 system-to-system communications. This means that an attacker who compromises a system within your network can launch SMBLoris attacks against any assets exposing port 445. If you have an active, mobile user base, then those devices should be configured to block access to port 445 when not on the corporate network. Even then, it's a good idea to have well-crafted host firewall rules to restrict access on this port.

Read More

"Official" page

Chrome Extensions With Over One Million Users Hijacked to Serve Adware



Copyfish is supposed to let you grab subtitles from films, captions from cartoons, and so on, while you're browsing. Web Developer, a tool developed by Chris Pederick, Director of Engineering at Bleacher Report. The extension overlays a popup with various debug tools that developers can use when building or editing their websites.

What does those two extensions have in common? Both have been hijacked to inject an adware as their developers fell for a phishing attack.

The crooks who'd acquired the password had lost no time: Locking Copyfish out of its own Chrome Web Store account. "Upgrading" the plugin to an unofficial release and adding in a bunch of ad-serving malware code. Moving the extension code to a different account to lock the original developer out of their own creation.

About Web Developer

About CopyFish

New U.S. Bill Seeks Basic IoT Security Standards

Lawmakers in the U.S. Senate today introduced a bill that would set baseline security standards for the government's purchase and use of a broad range of Internet-connected devices, including computers, routers and security cameras. The legislation, which also seeks to remedy some widely-perceived shortcomings in existing cybercrime law, was developed in direct response to a series of massive cyber attacks in 2016 that were fuelled for the most part by poorly-secured "Internet of Things" (IoT) devices.

For example, the bill would require vendors of Internet-connected devices purchased by the federal government make sure the devices can be patched when security updates are available; that the devices do not use hard-coded (unchangeable) passwords; and that vendors ensure the devices are free from known vulnerabilities when sold.

Specifically, the bill would "exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when in engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines"

Read More

JavaScript Packages Caught Stealing Environment Variables

On August 1, npm Inc. — the company that runs the biggest JavaScript package repository — removed 38 JavaScript npm packages that were caught stealing environment variables from infected projects.

The attacker used a technique called "typo-squatting" to register packages with names similar to popular libraries, but containing typos in their names. The malicious code in these projects would execute when developers would compile and run their personal JavaScript projects. The code would collect local environment variables and upload them to the attacker's server located at: npm.hacktask.net..

The attack is dangerous because some information such as hard-coded passwords or API access tokens is stored as environment variables. The issue first came to light when Swedish developer Oscar Bolmsten ran across the cross-env npm package. The developer reported the issue to the npm security team who eventually tracked down the rest of the affected packages and banned HackTask's npm account.

Full list of malicious npm packages is available in the article. Developers who used any of these packages within their projects are advised to change any passwords or access tokens they stored in their configurations.

Read More

Winners of the 2017 Pwnie Awards

The winners of the 2017 Pwnie Awards were announced last night at the Black Hat USA security conference. The annual ceremony awards the very best and worst coming out of the security community. People previously nominated their opinions of the biggest achievements and failures over the last year; the award winners are chosen from the top nominees in each category by a panel of security researchers.

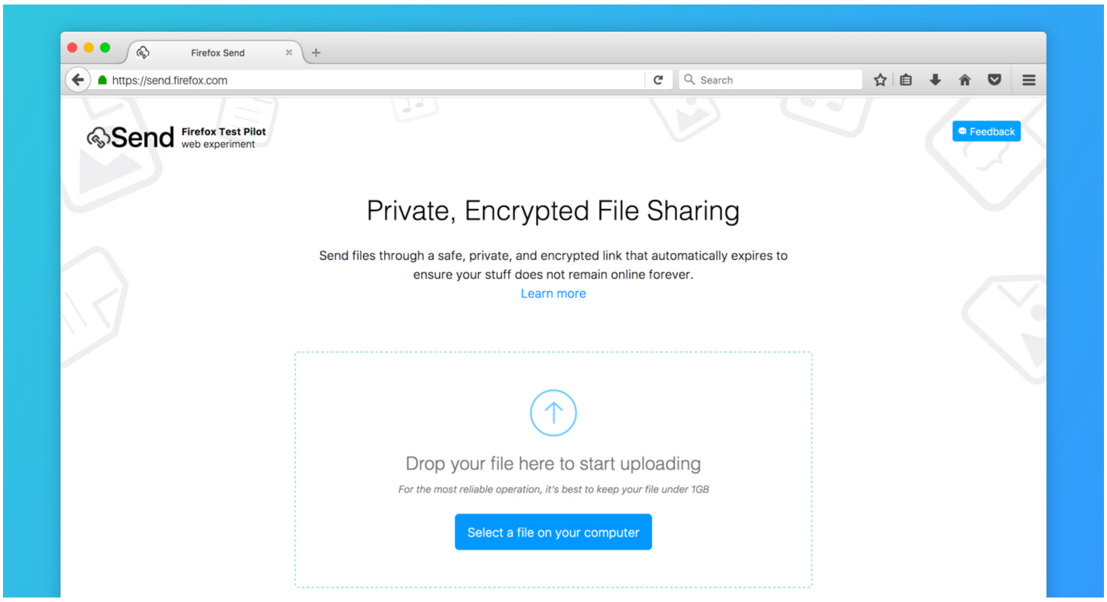
If you want to know who won the Pwnie for the best server-side bug, client-side bug, privilege-escalation bug, cryptographic attack, backdoor, branding, the most innovative research, the lamest vendor response or the most epic fail, check out the following article!

There was tie for epic ownage, so the Pwnie award went to both WannaCry, credited as “North Korea(?)” and the Shadow Brokers, credited as “Russia. Straight up: Russia.” The Pwnie Awards’ website has not yet been updated with a list of this year’s winners.

Read More

Official page

Mozilla Send, Open Source filesharing platform with client-side encryption



Private, Encrypted File Sharing

Send files through a safe, private, and encrypted link that automatically expires to ensure your stuff does not remain online forever.

Learn more

Drop your file here to start uploading

For the most reliable operation, it's best to keep your file under 1GB

Select a file on your computer

Firefox maker Mozilla has released a trio of new experimental tools, including a simple, secure file-sharing service, dubbed Firefox Send, which supports up to 1GB files. In the current version, you can securely send files to a contact using a link that only works once. The encrypted file, which is stored on Mozilla's server, is destroyed immediately after it has been downloaded once or after 24 hours have elapsed.

The clever part is that the file is encrypted client-side, and the key is provided as an anchor of the download link. This means the server never sees the encryption key and therefore cannot decrypt the shared file.

You may need to update to the latest version of Mozilla's desktop browser, Firefox 54, to use Send. It also works with Chrome, but not the current version of Safari, while Edge support is in the works.

Read More

Pilot 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.