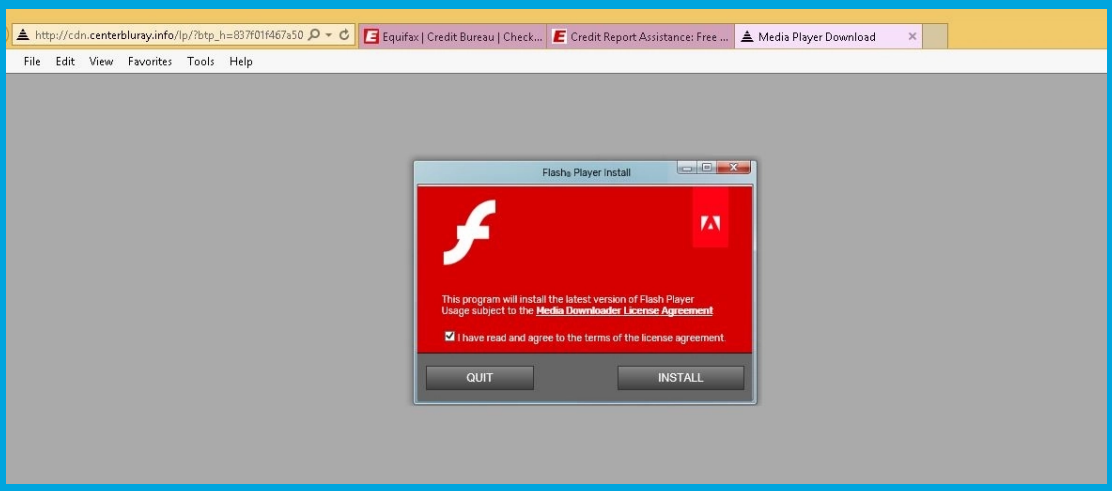
kindred

Security Newsletter

16 October 2017

Subscribe to this newsletter

Equifax Website Redirected Users to Adware, Scam Sites



Equifax is not having its best moments these days, and the much-maligned organization was again at the center of another cyber-security-related incident.

On Wednesday, and probably the previous days, Equifax's credit report assistance website (aa.econsumer.equifax.com) was caught redirecting users to all sort of nasty websites that were peddling fake Flash Player update files laced with adware, fake Android and iOS updates, and scam sites offering products at cheap prices.

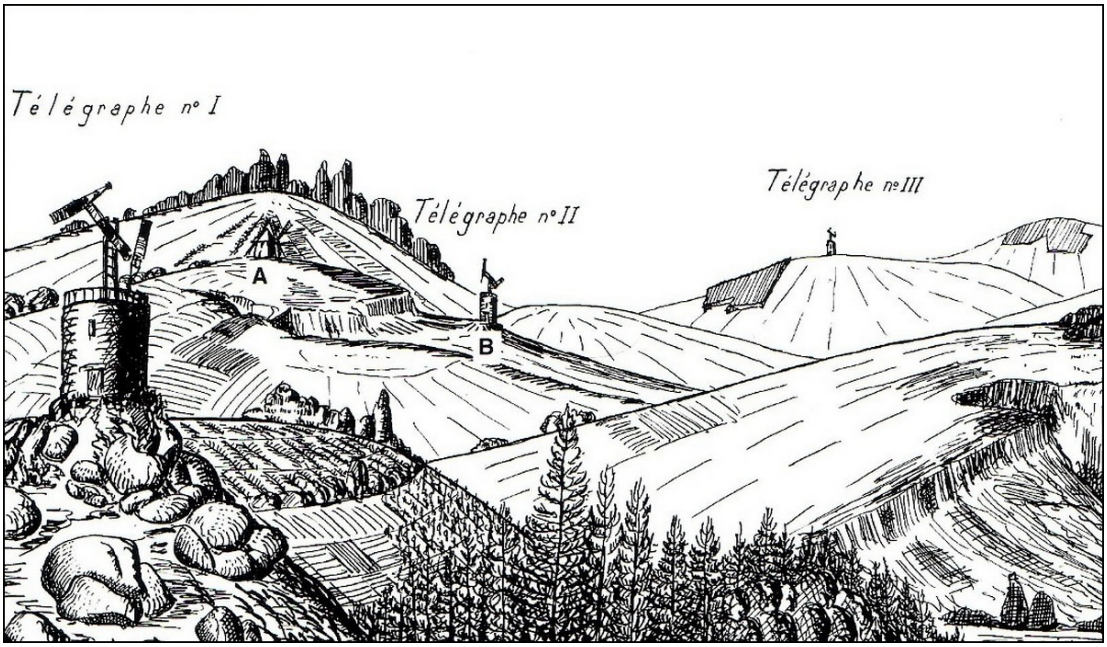
In May credit reporting service Equifax's website was breached by attackers who eventually made off with Social Security numbers, names, and a dizzying amount of other details for some 145.5 million US consumers.

Read More

More on ArsTechnica

IRS suspends Equifax's "taxpayer identity" contract

Nearly two centuries ago, France was hit by the world's first cyber-attack.



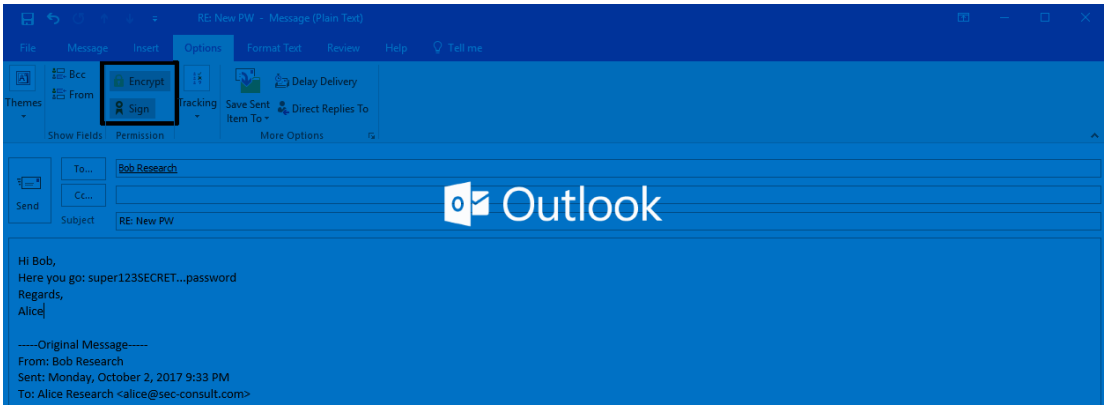
The world's first national data network was constructed in France during the 1790s. It was a mechanical telegraph system, consisting of chains of towers, each of which had a system of movable wooden arms on top.

The network was reserved for government use but in 1834 two bankers, François and Joseph Blanc, devised a way to subvert it to their own ends. With the help of an accomplice, they introduced some extraneous characters in the message flows to get quick information on market movements. The scam was only discovered two years later.

All this holds lessons for us as we grapple with online mischief today. Network intrusions often go unnoticed for many years, and many (if not most) may never be detected: most attackers, like the Blancs, do not advertise their presence.

Read More

Outlook Might Not Have Encrypted Your Emails If You Used S/MIME Encryption



A vulnerability was present in Outlook's S/MIME functionality. The short version: If you used Outlook's S/MIME encryption in the past 6 months (at least, this has still to be confirmed by Microsoft) your mails might not have been encrypted as expected. In the context of encryption this can be considered a worst-case bug.

S/MIME is an IETF standard for end-to-end encryption and signing of mails. Most popular mail clients, including Microsoft Outlook, Mozilla Thunderbird, Apple Mail, and the Mail Clients on Apple iOS and Samsung Knox devices, support S/MIME. Along with similar technologies like PGP/GPG, it is used by security/privacy conscious individuals and organizations to protect the mail communication.

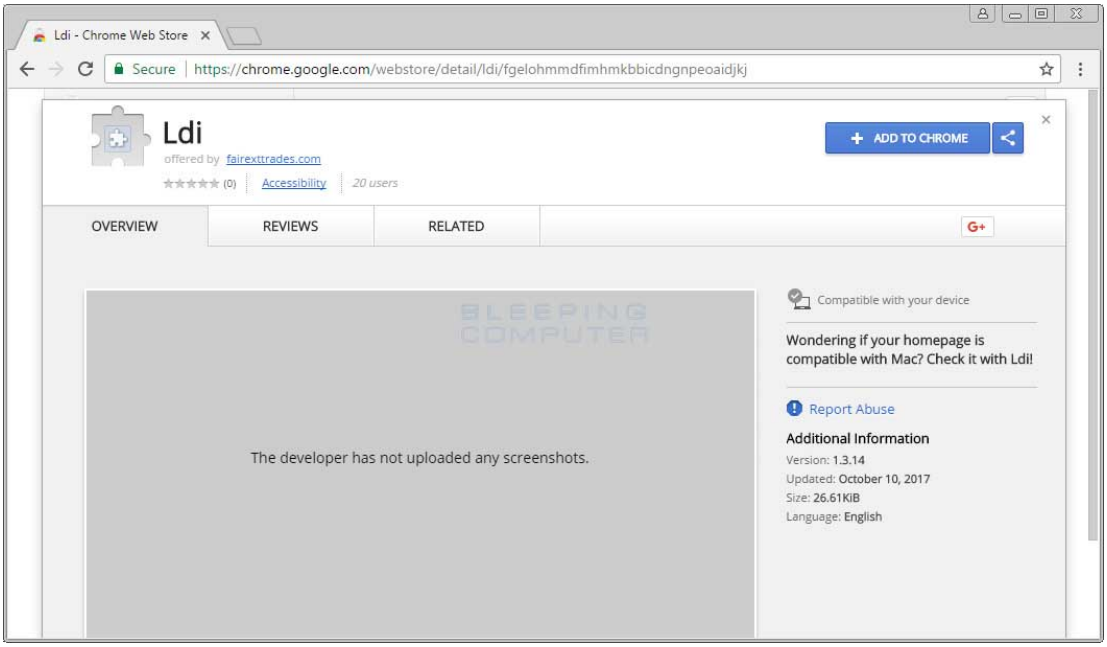
There is a bug in Outlook that causes S/MIME encrypted mails to be send in encrypted and unencrypted form (within one single mail) to your mail server (and the recipient's mail server and client and any intermediate mail servers). The impact is that a supposedly S/MIME encrypted mail can be read without the private keys of the recipient. This results in total loss of security properties provided by S/MIME encryption.

Researchers said they contacted Microsoft about the issue and the company released a fix for the bug — tracked as CVE-2017-11776 — last week, during the October 2017 Patch Tuesday.

Read More

Technical details of the vulnerability

Chrome Extension Uses Your Gmail to Register Domains Names & Injects Coinhive



With Chrome being the most widely used web browser, attackers are starting to develop more advanced and malicious extensions for it every day. Whether it's impersonating popular extensions to deliver ads, hijacking search queries, or injecting the CoinHive browser miner, it is easy to see that malicious extensions are on the rise.

The extension examined in this article, called Ldi, takes it to the next level when it comes to malicious behavior. This is because it not only loads the Coinhive browser miner into a victim's browser and uses up all the CPU, but it also uses that victim's Gmail account to register free domains for the attackers using Freenom.

Read More

Australian defense firm was hacked and F-35 data stolen, DOD confirms

The Australian Cyber Security Centre noted in its just-issued 2017 Threat Report that a small Australian defense company "with contracting links to national security projects" had been the victim of a cyber-espionage attack detected last November.

The attacker stole approximately 30 gigabytes of data, including data related to Australia's involvement in the F-35 Joint Strike Fighter program, as well as data on the P-8 Poseidon patrol plane, planned future Australian Navy ships, the C-130 Hercules cargo plane, and the Joint Direct Attack Munition (JDAM) bomb. The breach began in July of 2016. The breach was achieved by "exploiting an Internet-facing server," the ACSC reported, "then [by] using administrative credentials to move laterally within the network, where they were able to install multiple webshells—a script that can be uploaded to a webserver to enable remote administration of the machine—throughout the network to gain and maintain further access."

The investigation found that internet-facing services still had their default passwords, admin::admin and guest::guest.

Read More

How Kaspersky AV reportedly was caught helping Russian hackers steal NSA secrets

It was a case of spies watching spies watching spies: Israeli intelligence officers looked on in real time as Russian government hackers searched computers around the world for the code names of American intelligence programs.

Moscow-based Kaspersky Lab disclosed the intrusion into its network in mid-2015. Kaspersky released a detailed report that said some of the attack code shared digital fingerprints first found in the Stuxnet worm that sabotaged Iran's nuclear program. When combined with other clues—including the attackers' targeting of entities located in the US, which is off limits to the NSA—most analysts concluded that the 2014 hack was carried out by Israel.

The New York Times, citing unnamed people, said on Tuesday that Israeli spies indeed carried out the attack. More revealing still, the report said, that during the course of the hack, the spies watched in real time as Russian government hackers turned Kaspersky antivirus software used by 400 million people worldwide into an improvised search tool that scoured computers for code names of US intelligence programs. The NYT likened to a "sort of Google search for sensitive information."

The Israeli officials who had hacked into Kaspersky's own network alerted the United States to the broad Russian intrusion, which has not been previously reported, leading to a decision just last month to order Kaspersky software removed from government computers.

Read More

Summary article by Ars Technica

OnePlus Secretly Collects Way More Data Than It Should

Your OnePlus handset, running OxygenOS—the company's custom version of the Android operating system, is collecting way more data on its users than it requires.

A recent blog post published today by security researcher Christopher Moore on his website detailed the data collection practice by the Shenzhen-based Chinese smartphone maker, revealing that OxygenOS built-in analytics is regularly sending users' telemetry data to OnePlus' servers.

Collecting basic telemetry device data is a usual practice that every software maker and device manufacturers do to identify, analyse and fix software issues and help improve the quality of their products, but OnePlus found collecting user identification information as well.

While One Plus does not offer a method to disable the data collection easily through the graphical interface, it is possible to do it by plugging the phone on a computer and running a command through the Android Debugger.

Read More

Original Article

Cutting room floor

- Using Binary Diffing To Discover Windows Kernel Memory Bugs
- Using Binary Diffing to Rediscover macOs Last Week Bug
- The Absurdly Underestimated Dangers of CSV Injection
- Multiple Heap Buffer Overflows In the Windows DNS Client
- Reverse engineering a Gameboy ROM with radare2
- Exploiting The Wi-Fi Stack on Apple Devices (Part 3)
- Running Tor on HardenedBSD
- Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys (PDF)
- FBI Arrests A Cyberstalker After Shady "No-Logs" VPN Provider Shared User Logs
- Remote Code Execution on rubygems.org
- Watch Out! Difficult-to-Detect Phishing Attack Can Steal Your Apple ID Password