kindred

Security Newsletter

10 September 2018

Subscribe to this newsletter

British Airways hit with customer data theft

British Airways has notified the police after the theft of customer data from its website and mobile app. The airline said the personal and financial details of customers who made bookings on its website or app from 10.58pm local time on August 21 until 9.45pm on September 5 had been compromised. Around 380,000 payment cards were compromised. BA said the stolen data did not include travel or passport details, adding that it was investigating the security breach as a matter of urgency.

The airline is scarce with details at the moment because the investigation is ongoing and it's too soon to evaluate the damages. They stopped the breach and notified the relevant

authorities. "We will be contacting affected customers directly to advise them of what has happened and are advising them to contact their banks or credit card providers and follow their recommended advice," British Airways says in a statement.

All operations are running normally at the moment, but users are advised to change their passwords and choose a unique and strong one. The air carrier also recommends affected customers to call their bank and follow their instructions, to minimize potential financial damage. To make sure their message reaches a large portion of its customers, British Airways pinned the breach announcement on its Twitter page, for all its 1.17 million followers to see.

A similar incident was reported by Air Canada on August 28. Data from the mobile application had been accessed without authorization during a two-day interval, forcing the company to lock all its 1.7 million accounts. 20,000 customers were affected by that incident. The intruder could steal at least the owner's name, email address, and telephone number, because this is the required information for the mobile app account.

Read More on Zdnet

Even More on BleepingComputer

Official statement from British Airways

Someone Hijacked MEGA Chrome Extension to Steal Users' Passwords

Warning! If you are using Chrome browser extension from the MEGA file storage service, uninstall it right now. The official Chrome extension for the MEGA.nz cloud storage service had been compromised and replaced with a malicious version that can steal users' credentials for popular websites like Amazon, Microsoft, Github, and Google, as well as private keys for users' cryptocurrency wallets.

On 4 September at 14:30 UTC, an unknown attacker managed to hack into MEGA's Google Chrome web store account and upload a malicious version 3.39.4 of an extension to the web

store, according to a blog post published by the company. Upon installation or auto-update, the malicious extension asked for elevated permissions to access personal information, allowing it to steal credentials from sites like Amazon, Github, and Google, along with online wallets such as MyEtherWallet and MyMonero, and Idex.market cryptocurrency trading platform. The trojanized Mega extension then sent all the stolen information back to an attacker's server located at megaopac[.]host in Ukraine, which is then used by the attackers to log in to the victims' accounts, and also extract the cryptocurrency private keys to steal users' digital currencies.

The Firefox version of MEGA has not been impacted or tampered with, and users accessing MEGA through its official website (https://mega.nz) without the Chrome extension are also not affected by the breach. However, users should consider their credentials being compromised on websites and applications they visited while the trojanized MEGA Chrome extension was active. This attack serves as a fresh reminder that legitimate browser extensions can and periodically do fall into the wrong hands, and that it makes good security sense to limit your exposure to such attacks by getting rid of extensions that are no longer useful or actively maintained by developers.

Never download and install an extension just because a Web site says you need it to view some type of content. “If you didn't go looking for it, don't install it."

Read More on TheHackerNews

Browser Extensions: Are They Worth the Risk?

Official statement from Mega

Cutting room floor

- How US authorities tracked down the North Korean hacker behind WannaCry
- New Fallout Exploit Kit Drops GandCrab Ransomware or Redirects to PUPs
- The SOC Gets a Makeover
- Sextortion – When Persistent Phishing Pays Off
- Visualizing Amazon GuardDuty findings
- Tor Browser gets a redesign, switches to new Firefox Quantum engine
- https://www.zdnet.com/article/chrome-69-released-with-new-ui-and-random-password-generator/
- Google fixes Chrome issue that allowed theft of WiFi logins
- Hackers Hijacked 7,500+ MikroTik Routers and Redirecting User Traffic to Attackers
- Here Are The Essential Security Tips To Stay Safe On Social Media
- Knock, knock: Digital key flaw unlocks door control systems
- USA Is the Top Country for Hosting Malicious Domains According to Report
- Russia tries more precise technology to block Telegram messenger
- Public IP Addresses of Tor Sites Exposed via SSL Certificates

#Tech and #Tools

- XSS using quirky implementations of ACME http-01
- Using AWS Account ID's for IAM User Enumeration
- Penetration Testing / OSCP Biggest Reference Bank
- Wi-Jacking: Accessing your neighbour's WiFi without cracking
- Red Teaming Microsoft: Part 1 – Active Directory Leaks via Azure
- NTLM password overflow via integer overflow
- Remote Mac Exploitation Via Custom URL Schemes

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.

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