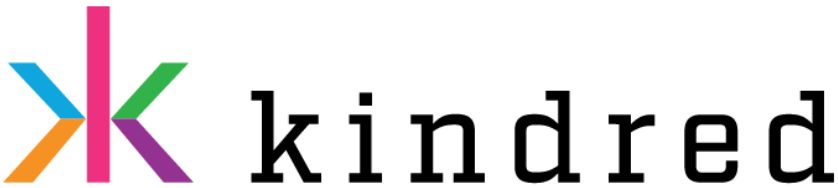


Security Newsletter

10 August 2020

Subscribe to this newsletter

Capital One Fined $80 Million for 2019 Data Breach Affecting 106 Million Users

A United States regulator has fined the credit card provider Capital One Financial Corp with $80 million over last year's data breach that exposed the personal information of more than 100 million credit card applicants of Americans.

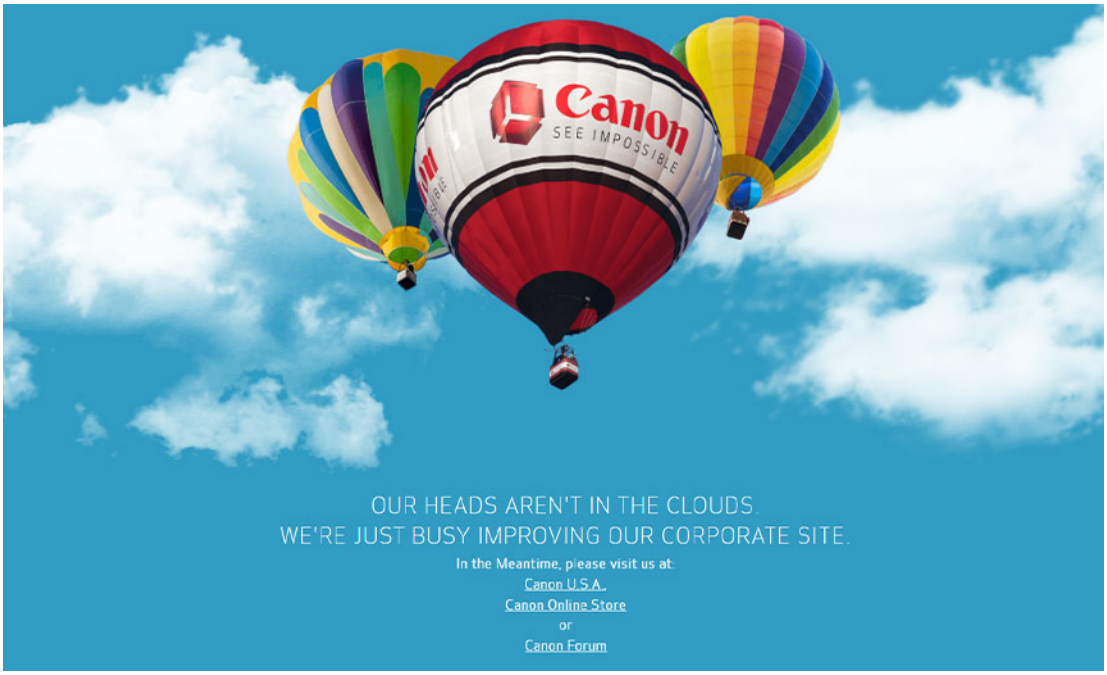
According to a press release published by the OCC on Thursday, Capital One failed to establish appropriate risk management before migrating its IT operations to a public cloud-based service, which included appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts. The OCC also said that the credit card provider also left numerous weaknesses in its cloud-based data storage in an internal audit in 2015 as well as failed to patch security vulnerabilities, violating the "Interagency Guidelines Establishing Information Security Standards," that all US banks must comply with.

Besides credit card information, the hacker also managed to steal approx 140,000 Social Security numbers and 80,000 bank account numbers linked to US customers, and 1 million Canadian Social Insurance numbers. In addition to the civil money penalty of 80 million dollars, the OCC also ordered Capital One Finance to enhance its cybersecurity security defenses and submit a plan to the OCC within 90 days outlining how it intends to do so.

Read More on TheHackerNews

Even More on ZDNet

Canon USA Websites Offline Following Cyber Incident, internal memo confirms ransomware attack



The website outage began Wednesday, two days after the imaging company issued a statement reporting that user data was missing from a cloud storage database. Brett Callow, a threat analyst with the security firm Emsisoft, says the ransomware group Maze has claimed responsibility for the security incident. So far, however, Maze has not posted to its website any exfiltrated data or updates on the attack, he adds.

Although there's no evidence connecting the website outages with the missing data, exfiltration of data is common Maze tactic, security experts note. Maze Group ransomware operators use 'name and shame' tactics whereby victims' data is exfiltrated prior to encryption and used to leverage ransomware payments," Walmsley says. "The bullying tactics used by such ransomware groups are making attacks even more expensive, and they are not going to stop any time soon, particularly within the current climate. These attackers will attempt to exploit, coerce and capitalize on organizations' valuable digital assets."

Read More on BankInfoSecurity

Even More on BleepingComputer

More #News

- https://www.bleepingcomputer.com/news/security/zello-resets-all-user-passwords-after-data-breach/
- Microsoft Paid Out Nearly $14 Million via Bug Bounty Programs in Past Year
- Hacker leaks passwords for 900+ enterprise VPN servers
- Hackers can abuse Microsoft Teams updater to install malware
- I'm Open Sourcing the Have I Been Pwned Code Base
- Evasive Credit Card Skimmers Using Homograph Domains and Infected Favicon
- Intel leak: 20GB of source code, internal docs from alleged breach
- Garmin Reportedly Paid a Ransom
- New EtherOops attack takes advantage of faulty Ethernet cables

#Patch Time!

- Intel, ARM, IBM, AMD Processors Vulnerable to New Side-Channel Attacks

#Tech and #Tools

- Network-layer DDoS attack trends for Q2 2020
- Microsoft releases Windows 10 Version 2004 security baseline
- Twitter Rushes to Fix Flaw in Android Version
- Weaklayer: Browser Detection & Response
- The danger of world writable NFS shares
- Manticore Adversary Emulation Client Tool
- Link Lock: Password-protect URLs using AES in the browser.
- TikTok: Logs, Logs, Logs
- A Pentesters Guide - Part 5 (Unmasking WAFs and Finding the Source)
- Certificate Transparency: a bird's-eye view
- Attack Detection Fundamentals

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 a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. 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 is an innovation driven company that builds on trust.

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