kindred

Security Newsletter

15 July 2019

Subscribe to this newsletter

Dear BA and Marriott: Your GDPR Fines Are Important to Us

British Airways hit with £183M GDPR fine—could your business be next?

The data protection gloves have finally come off in Europe after the EU's General Data Protection Regulation went into effect last May. Consider the tables now turned on organizations that fail to take their data protection responsibilities seriously.

On Monday, Britain's data protection authority, the Information Commissioner's Office, announced a proposed fine of £184 million ($230 million) against British Airways after breaches last September and October enabled attackers to route customers to a fraudulent site, exposing 500,000 customers' personal details. On Tuesday, the ICO confirmed a proposed fine of £99 million ($125 million) against Marriott International for its failure to stop a four-

year breach that globally exposed approximately 339 million customer records. Both fines are the first major, proposed sanctions - they are not yet final - over data breaches that have occurred since GDPR enforcement began on May 25, 2018.

More GDPR fines are likely on the way, says Brian Honan, who heads Dublin-based cybersecurity consultancy BH Consulting. "Many GDPR breaches, especially the highly publicized ones, can take a long time for proper investigations by the supervisory authorities," Honan tells me. "What we are seeing now are the beginnings of the supervisory authorities issuing penalties under GDPR, and I expect we will see many more over the coming months." Already, both British Airways and Marriott are attempting to spin the proposed sanctions from the same playbook, using emotive language to stand in for inconvenient facts.

Marriott's fine was first revealed after the hotel giant warned investors that it might be on the hook, via a notice to the U.S. Securities and Exchange Commission. Investors will likely now be asking the company why it failed to spend a relatively small amount to protect its systems, versus the risk of incurring a much larger fine. The proposed $230 million fine against British Airways represents about $40 per record exposed in the breach, with the total equaling about 6 percent of airlines' 2018 profit. So, the total cost of this one incident is about $500 million, or over 10 percent of BA's 2018 profit.

The message from regulators is clear: If you buy it, you own it. Also, any organization's ability to process customer data remains a privilege, not a right. Memo to all businesses that store Europeans' personal data: Act now to avoid disappointment.

Read More on BankInfoSecurity

Even More on TechRepublic

GDPR Fines: Everything You Need To Know

Magecart Hackers Infect 17,000 Sites Through Misconfigured Amazon S3 Buckets

Cybersecurity researchers have identified yet another supply-chain attack carried out by payment card hackers against more than 17,000 web domains, which also include websites in the top 2,000 of Alexa rankings. Since Magecart is neither a single group nor a specific malware instead an umbrella term given to all those cyber criminal groups and individuals who inject digital card skimmers on compromised websites, it is not necessary for every one of them to use similar techniques with the same sophistication.

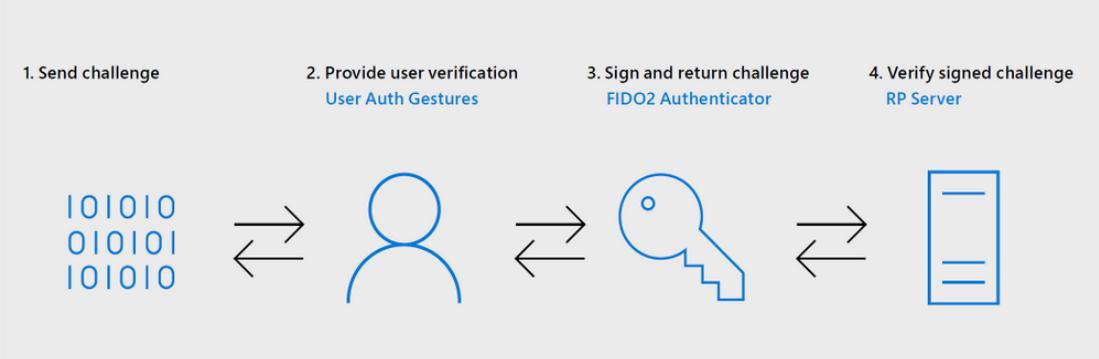
Almost two months ago, security researchers from RiskIQ discovered supply-chain attacks involving credit card skimmers placed on several web-based suppliers, including AdMaxim, CloudCMS, and Picreel intending to infect as many websites as possible. However, upon continuous monitoring of their activities, researchers found that the actual scale of this campaign, which started in early April 2019, is much larger than previously reported.

According to the researchers, since the beginning of the campaign, this group of Magecart attackers has continuously been scanning the Internet for misconfigured Amazon S3 buckets, which allows anyone to view and edit files it contains, and injecting their digital card skimming code at the bottom of every JavaScript file they find. Magecart made headlines last year after payment card hackers conducted several high-profile attacks against major international companies including British Airways, Ticketmaster, and Newegg.

Read More on TheHackerNews

Even More on ZDNet

Microsoft Azure AD FIDO2 Passwordless Sign-In in Public Preview



Microsoft announced public preview support for FIDO2 security keys in Azure Active Directory (Azure AD) to provide users with passwordless authentication capabilities, eliminating passwords out of the logging in process.

With the help of a FIDO2 security key, as well as the Microsoft Authenticator app and Windows Hello, all Azure AD users can now log in without having to enter a password. "These strong authentication factors are based off the same world class, public key/private key encryption standards and protocols, which are protected by a biometric factor (fingerprint or facial recognition) or a PIN," added the Microsoft 365 team.

The end goal is to add support for the entire spectrum of available authentication factors, dramatically decrease the risk of account compromise by making the login process substantially more secure in the long term. Microsoft integrated the new public preview passwordless authentication solutions with the help of Feitian Technologies, Yubico, and HID Global, which provide security keys and cards compatible with the new Azure AD FIDO2 support.

Read More on BleepingComputer

Even More on Microsoft Security portal

More #News

- Youtube's ban on "hacking techniques" threatens to shut down all of infosec Youtube
- Over 90 Million Records Leaked by Chinese Public Security Department
- “Mozilla aren't villains after all” – ISPs back down after public outcry
- New Android malware replaces legitimate apps with ad-infested doppelgangers
- Troll lawyer uploads porn to Pirate Bay, extorts downloaders to settle ‘copyright' claims
- ChatOps is Your Bridge to a True DevSecOps Environment
- Malwarebytes is Now Enforcing Lifetime Licenses to One PC
- Mozilla bans surveillance vendor from Firefox certificate whitelist
- Fake DeepNude Downloads Gives You Malware Instead of Nudes
- Watch Out! Microsoft Spotted Spike in Astaroth Fileless Malware Attacks

- Canonical Investigating Hack of Its GitHub Page
- Dark web takedowns make good headlines, do little for security
- Leak Confirms Google Speakers Often Record Without Warning
- Cybersecurity Frameworks — Types, Strategies, Implementation and Benefits
- Will mobile devices replace passwords?
- MongoDB Database Exposed 188 Million Records
- Ransomware Targets QNAP Storage Devices

#Patch Time!

- Patch Tuesday Lowdown, July 2019 Edition
- Jira Server and Data Center Update Patches Critical Vulnerability
- Adobe tackles vulnerabilities in Dreamweaver, Experience Manager, Bridge
- Two zero days and 15 critical flaws fixed in July's Patch Tuesday
- Researchers Disclose Vulnerability in Siemens' ICS Software
- Intel Fixes Priv Escalation Vulnerability in Enterprise SSD
- Logitech Unifying Receivers Vulnerable to Key Injection Attacks
- Unpatched Prototype Pollution Flaw Affects All Versions of Popular Lodash Library
- Backdoor discovered in Ruby strong_password library
- Flaw in Walkie-Talkie App on Apple Watch Allows Spying
- SAP Patches Critical Flaw in Diagnostics Agent
- Flaw in Zoom Video Conferencing Software Lets Websites Hijack Mac Webcams

#Tech and #Tools

- Detecting Phishing with SPF macros
- strong_password v0.0.7 rubygem hijacked
- Kali Linux Now Available for Raspberry Pi 4
- Office-Addin backdoor with C2 in Azure Cloud
- Pyattck: A Python Module to interact with the Mitre ATT&CK Framework
- Cellular hacking compilation
- Mainframe hacking cimpilation
- Targeting AD FS With External Brute-Force Attacks
- Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!
- Osquery-ATT&CK: map the MITRE ATT&CK with the Osquery for enterprise threat hunting
- Preventing Mimikatz Attacks
- How to Secure SharePoint
- Breach → ATT&CK →OSQUERY

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 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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