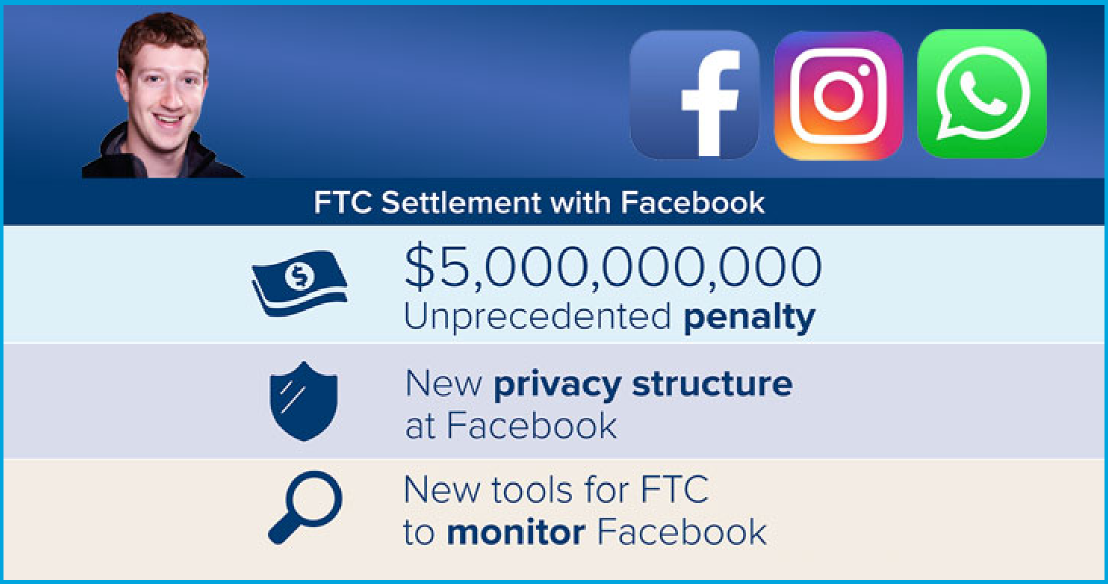
kindred

Security Newsletter

29 July 2019

Subscribe to this newsletter

It's Official: FTC Fines Facebook $5 Billion


FTC Settlement with Facebook
$5,000,000,000
Unprecedented **penalty**
New **privacy structure** at Facebook
New tools for FTC to **monitor** Facebook

The Federal Trade Commission (FTC) today officially confirmed that Facebook has agreed to pay a record-breaking $5 billion fine over privacy violations surrounding the Cambridge Analytica scandal. Besides the multibillion-dollar penalty, the company has also accepted a 20-year-long agreement that enforces it to implement a new organizational framework designed to strengthen its data privacy practices and policies.

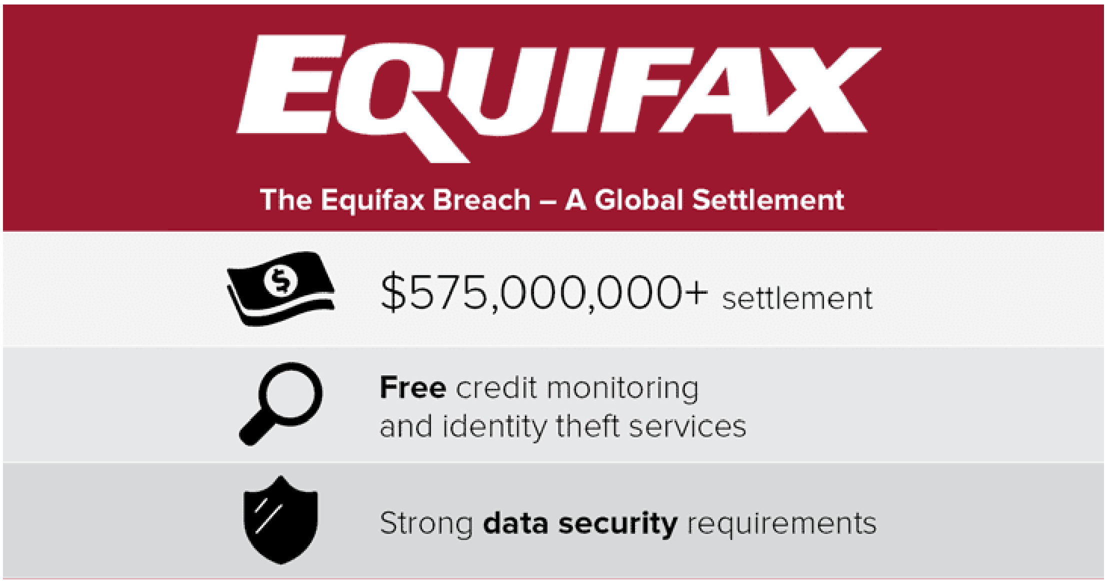
"The order requires Facebook to restructure its approach to privacy from the corporate board-level down, and establishes strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy and that those decisions are subject to meaningful oversight," the FTC said in a press release.

In a blog post published today, Facebook said it is building a new privacy program in compliance with the latest FTC requirements which will change the way Facebook handles its users' data and helpful in "rebuilding trust with people."

Read More on HackerNewsletter

Even More on BankInfoSecurity

Equifax to Pay up to $700 Million in 2017 Data Breach Settlement



EQUIFAX

The Equifax Breach – A Global Settlement

$575,000,000+ settlement

Free credit monitoring
and identity theft services

Strong **data security** requirements

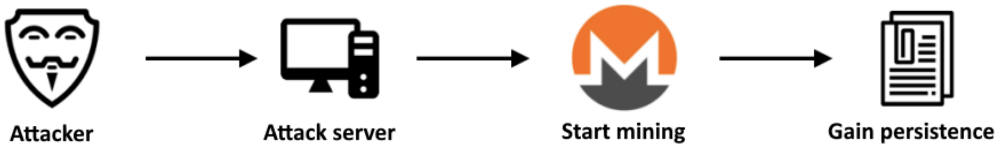
Equifax, one of the three largest credit-reporting firms in the United States, has to pay up to $700 million in fines to settle a series of state and federal investigations into the massive 2017 data breach that exposed the personal and financial data of nearly 150 million Americans—that's almost half the country.

Besides the penalty, the company has also been ordered to provide all American consumers with six free credit reports each year for seven years, along with the one free annual credit report, starting from January 2020. In September 2017, Equifax suffered a massive data breach that allowed hackers to steal personal information, including names, birth dates, addresses, social security numbers, and, in some cases, driver's license numbers, of as many as 147 million people.

The commission has even set up a dedicated email (equifax@ftc.gov), encouraging Equifax employees to mail FTC if they "believe the company is failing to adhere to its data security promises." The breach, which has been called one of the worst in American history, occurred due to failure of the company to patch a critical security vulnerability in its systems it was made aware of in March that year.

Read More on HackerNewsletter

Hackers Exploit Jira, Exim Linux Servers and add Cryptominers



Hackers are exploiting vulnerable Jira and Exim servers with the end goal of infecting them with a new Watchbog Linux Trojan variant and using the resulting botnet as part of a Monero cryptomining operation.

Watchbog's infection process is quite straightforward as it drops a Monero coinminer after exploiting the vulnerabilities it targets and it gains persistence to fend off the users' attempts of removing it. After getting a foothold on the vulnerable servers, Watchbog will download and execute malicious commands from pastebin that will eventually deploy and launch the final cryptocurrency miner payload on the compromised Linux boxes. The malware will also achieve persistence by adding itself to multiple crontab files to make sure that it can come back and reinfect the system if the user will not find all of the altered crontabs.

Read More on BleepingComputer

More #News

- Your Android Phone Can Get Hacked Just By Playing This Video
- Why Hackers Abuse Active Directory
- Microsoft Office 365 Webmail Exposes User's IP Address in Emails
- BlueKeep RCE Exploit Module Added to Penetration Testing Tool
- No love lost between security specialists and developers
- Robinhood discovered they stored some passwords in cleartext, prompts for reset
- Phishing Campaign Bypasses Email Gateways via WeTransfer Alerts
- Equifax's data breach disaster. Will it change executive attitudes toward security?
- Siemens Contractor Pleads Guilty to Planting 'Logic Bomb' in Spreadsheets
- Consumer Advocates Criticize Equifax Settlement Plan
- Big password hole in iOS 13 beta spotted by testers
- Phishers Target Office 365 Admins with Fake Admin Alerts
- A proactive approach to more secure code, looking into Rust
- Louisiana Declares Emergency After Malware Attacks
- Essential Active Directory Security Defenses

#Patch Time!

- Keep Calm, Carry On. VLC Not Affected by Critical Vulnerability

- Unpatched vulnerabilities lurk in Comodo Antivirus
- ProFTPD Vulnerability Lets Users Copy Files Without Permission
- Hackers Exploit Recent WordPress Plugin Bugs for Malvertising
- Windows 10 1903 Update Blocked by Old Intel Rapid Storage Drivers

#Tech and #Tools

- Active Directory Security
- Microsoft Email Phishing Protection Guide - Enhance Your Organization's Security Posture
- 8 methods for bypassing cameras and facial recognition software
- How (not) to sign a JSON object
- wordlistctl: Script to fetch, install, update and search wordlist archives
- Grabbing Hashes and Forging External Footholds
- Lesspass: Stateless Password Manager
- A Deep Dive into XXE Injection
- Under the Hoodie 2019
- AWS IAM Privilege Escalation – Methods and Mitigation – Part 2
- Administrative Templates (.admx) for Windows 10 May 2019 Update (1903)
- IRMA: Advanced Suspicious file Analysis
- https://github.com/quarkslab/irma
- Introduction to physical penetration tests

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career 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 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