SentinelOne blog

GET A DEMO

The Good, the Bad and the Ugly in Cybersecurity – Week 5

February 3, 2023
by SentinelOne

The Good

The FTC this week has handed out a $1.5 million penalty to a U.S. healthcare company that promised its customers it would "never share personal health information with advertisers or third parties" and then allegedly did precisely that.

The Department of Justice filed an enforcement action on behalf of the FTC against GoodRx under its new Health Breach Notification rule. The complaint against the company accused it of failing to notify customers about unauthorized disclosure of health PII (personally identifiable information). According to the FTC, GoodRx repeatedly shared individually identifiable health information over a four year period with Facebook, Google, Twilio, Branch, and Criteo.

> FTC
> @FTC · Follow
>
> FTC enforcement action to bar GoodRx from sharing consumers' sensitive health info for advertising: bit.ly/3HNmvUT /1

> ftc.gov
> FTC Enforcement Action to Bar GoodRx from Sharing Consumer…
> The Federal Trade Commission has taken enforcement action for the first time under its Health Breach Notification Rule against th…
>
> 4:54 PM · Feb 1, 2023
>
> Read the full conversation on Twitter
>
> 133 Reply Copy link
>
> Read 13 replies

The FTC went on to complain that GoodRx had uploaded contact details of its own customers to Facebook along with advertising IDs, and that it used privileged information about those customers' previous medication purchases to target their profiles with health-related ads. In doing so, the company exposed their information to Facebook, which itself is facing multiple ongoing lawsuits related to scraping data from hospital websites for use in targeted ads.

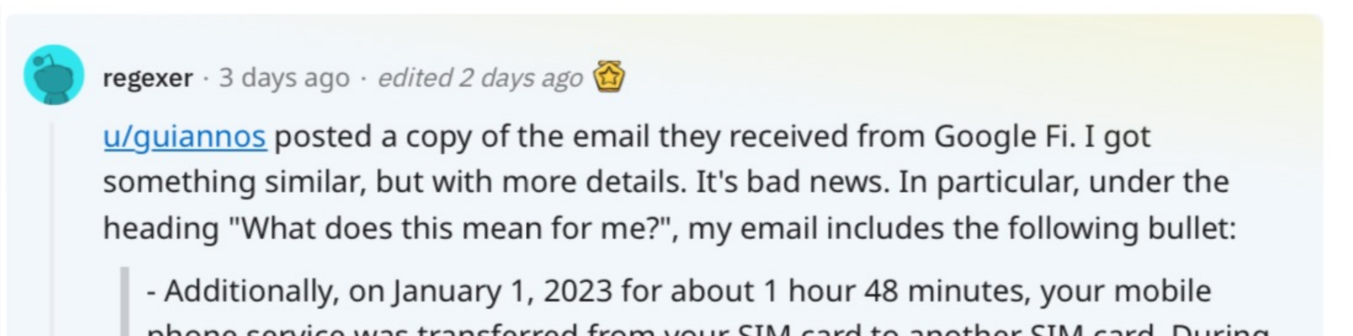
FTC director Samuel Levine said of the action that "Digital health companies and mobile apps should not cash in on consumer's extremely sensitive and personally identifiable health information" and that the FTC would continue to use its legal authority to protect American consumers.

The Bad

SIM swapping attacks, where a threat actor impersonates a customer of a mobile phone carrier and requests a transfer of the customer's number to a new device, have been utilized to pull off some high profile hacks recently. This week, it's bad news for Google Fi customers, who have been targeted by hackers that gained access to technical SIM data after breaching a Google Fi network provider.

Google's U.S. telecommunications and mobile internet service, Google Fi, informed customers this week that personal data had been exposed after a breach of one of its network providers. Google notified customers that the incident had exposed their phone numbers, SIM card serial numbers, and other details. However, the company emphasized that there was no access to Google's systems or any systems overseen by Google.

Users on social media, however, soon began reporting notifications from Google Fi that described SIM swapping attacks.


regexer · 3 days ago · edited 2 days ago

u/guiannos posted a copy of the email they received from Google Fi. I got something similar, but with more details. It's bad news. In particular, under the heading "What does this mean for me?", my email includes the following bullet:

> - Additionally, on January 1, 2023 for about 1 hour 48 minutes, your mobile phone service was transferred from your SIM card to another SIM card. During the time of this temporary transfer, the unauthorized access could have involved the use of your phone number to send and receive phone calls and text messages. Despite the SIM transfer, your voicemail could not have been accessed. We have restored Google Fi service to your SIM card.

SIM swapping attacks allow the attacker to receive both phone calls and SMS text messages intended for the legitimate user and, among other things, allow attacks to intercept text-based 2FA authentication messages.

Google says its incident response team investigated the breach and implemented measures to secure data on the provider's system and notified everyone potentially impacted. The SIM swapping attacks were temporary and Google Fi has since restored service to all customers' registered SIM cards.

The Ugly

Threat actors have been creating malicious OAuth applications as part of a phishing campaign aimed at breaching Microsoft cloud services, it was revealed this week.

According to MSRC, threat actors ran a consent phishing campaign after impersonating companies enrolling in MCPP/MPN (Microsoft Cloud Partner Program, *aka* Microsoft Partner Network). Consent phishing works by tricking users into granting permissions to malicious cloud applications that can then be weaponized to compromise legitimate cloud services and access sensitive data.

Once victims granted access to the malicious OAuth apps, threat actors used them to exfiltrate email mailboxes, likely with the further objective to use the stolen data in email Reply Chain attacks, Business Email Compromises (BEC), and spear phishing attacks.

The campaign, which primarily targeted MCPP customers in the UK and Ireland, was first spotted on December 15th last year, with the actors using fraudulent partner accounts to register OAuth applications in Azure AD that appeared to be from verified publishers.

The Redwood tech giant says that all identified fraudulent applications have now been disabled and affected customers informed. Even so, it comes amid turbulent times for the company. Despite announcing security sales of over $20 billion in 2022, the company's products across endpoint and cloud remain notorious for multiple high-impact vulnerabilities and cloud-based attack vectors.

Attacks using bogus OAuth apps have targeted Microsoft's cloud services before, with separate threat activities seen in January 2022 and September 2022, according to reports.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- SentinelOne Named to Deloitte Fast 500 List for 4th Consecutive Year
- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
- Cyber War Elements In The Ukrainian Conflict | Hosted by the Alperovitch Institute for Cybersecurity Studies