kindred

Security Newsletter

6 August 2018

Subscribe to this newsletter

Reddit Breach Highlights Limits of SMS-Based Authentication

Reddit.com today disclosed that a data breach exposed some internal data, as well as email addresses and passwords for some Reddit users. As Web site breaches go, this one doesn't seem too severe. What's interesting about the incident is that it showcases once again why relying on mobile text messages (SMS) for two-factor authentication (2FA) can lull companies and end users into a false sense of security.

Reddit said the exposed data included internal source code as well as email addresses and obfuscated passwords for all Reddit users who registered accounts on the site prior to May 2007. The incident also exposed the email addresses of some users who had signed up to receive daily email digests of specific discussion threads.

Of particular note is that although the Reddit employee accounts tied to the breach were

protected by SMS-based two-factor authentication, the intruder(s) managed to intercept that second factor. “Already having our primary access points for code and infrastructure behind strong authentication requiring two factor authentication (2FA), we learned that SMS-based authentication is not nearly as secure as we would hope, and the main attack was via SMS intercept,” Reddit disclosed. “We point this out to encourage everyone here to move to token-based 2FA.”

Reddit didn’t specify how the SMS code was stolen, although it did say the intruders did not hack Reddit employees’ phones directly. In one common scenario, known as a SIM-swap, the attacker masquerading as the target tricks the target’s mobile provider into tying the customer’s service to a new SIM card that the bad guys control. Customers can request a SIM swap when their existing SIM card has been damaged, or when they are switching to a different phone that requires a SIM card of another size.

Another typical scheme involves mobile number port-out scams, wherein the attacker impersonates a customer and requests that the customer’s mobile number be transferred to another mobile network provider. If the only 2FA options offered by a site you frequent are SMS and/or phone calls, this is still better than simply relying on a password. But it’s high time that popular Web sites of all stripes start giving their users more robust authentication options like TOTP and security keys.

Read More

Reddit Hacked – Emails, Passwords, Private Messages Stolen

Official Statement

How a man hacked his victims' SIM cards to steal millions of dollars

Californian Authorities have arrested and charged a 20-year old college student Joel Ortiz for being part of a mobile phone hijacking group who hacked SIM cards. According to reports the detainee managed to hijack over 40 phone numbers and stole $5 million as well from high-profile targets including cryptocurrency investors. Detectives at the Regional Enforcement Allied Computer Team were tipped by one of the victims, a blockchain investor, informing that his cellphone number has been hijacked.

According to Motherboard, his cellphone number was hijacked twice and the hacker not only reset the password of his email ID and cryptocurrency accounts but also replaced the 2FA Google authenticator app with another one. Hacker, claims the victim, also harassed his daughter. On 20th March, the hacker allegedly called his wife from the stolen phone number and also messaged his daughter and friends to send him Bitcoin.

Reportedly, Ortiz pulled off this feat using SIM swapping technique, which allowed him to access the numbers and execute port out scams. His targets were the attendees of the cryptocurrency/blockchain conference Consensus held in New York in May 2018. With help from some of his accomplices and using SIM swapping, Ortiz could trick cellular service providers into sending out phone numbers to SIM cards owned by them.

SIM swapping can be prevented if you add a PIN code to your smartphone account. You may also set up a verbal password to further complicate the verification process.

Read More

Even More

Dixons Carphone Data Breach Affects not 1.2, but 10 Million Customers

Dixons Carphone's 2017 data breach was worse than initially anticipated. In an announcement on Monday, Dixons Carphone, one of the largest consumer electronics and telecommunication retailers in Europe, admitted that the breach affected around 10 million customers, up from an initial estimate of 1.2 million people the company acknowledged back in June.

The Carphone Warehouse and Currys PC World owner said the hackers may have accessed personal information of its affected customers including their names, addresses and email addresses last year. The hackers also got access to 5.9 million payments cards used at Currys PC World and Dixons Travel, but nearly all of those cards were protected by the chip-and-pin system.

However, Dixons Carphone assured its customers that no bank details, including pin codes, card verification values and authentication data used to make purchases, were taken and that there's no evidence any fraud had resulted from the security breach.

This is second time in three years Dixons Carphone has become the victim of a major cyber attack. In 2015, a data breach hit around 3 million customers, for which the company was fined £400,000 earlier this year.

An ICO spokesperson said: “Dixons Carphone reported a data breach to the ICO in June. The company has now confirmed that the incident affected the personal data of 10 million records, which is significantly higher than initially stated. Our investigation into the incident is ongoing and we will take time to assess this new information. In the meantime, we would expect the company to alert all those affected in the UK as soon as possible and to take all steps necessary to reduce any potential harm to consumers.”

Read More

ICO statement in response to Dixons Carphone breach announcement

Cutting room floor

- Patching Windows for Spectre and Meltdown: A complete guide
- Fake Websites for Keepass, 7Zip, Audacity, Others Found Pushing Adware
- Atlassian: Jira email server passwords blabbed to strangers
- Massive Malvertising Campaign Discovered Attempting 40,000 Infections per Week
- Cryptojacking for beginners – what you need to know
- 3 Carbanak (FIN7) Hackers Charged With Stealing 15 Million Credit Card
- Why No HTTPS? Questions Answered, New Data, Path Forward
- Microsoft Edge Flaw Lets Hackers Steal Local Files
- Microsoft Edge adds WebAuthn as passwords near the end
- The rolling tide that is GDPR … say hello to the CCPA
- Massive Coinhive Cryptojacking Campaign Touches Over 200,000 MikroTik Routers
- Symfony Flaw Leaves Drupal Sites Vulnerable to Hackers—Patch Now

#Tech and #Tools

- My arsenal of AWS security tools
- Humble book bundle: Cybersecurity 2.0 by Wiley
- Exploiting a Microsoft Edge Vulnerability to Steal Files - PoC
- Bypassing and exploiting Bucket Upload Policies and Signed URLs
- Escaping the Sandbox – Microsoft Office on MacOS
- Attacking the attackers
- PowerShell Inside a Certificate? – Part 1 (Part 2)
- Identifying web user social accounts, by exploiting user-blocking mechanisms
- Making a Blind SQL Injection a Little Less Blind

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