**Sprint Data Breach**

Bradford Hogge, Kyle Tolliver,

Eduardo Urbiola, McKayla Plummer

CIT 270 - 02, Systems Security I

March 7, 2020

Table of contents

Executive Summary ………….. 3

Breach Details …..…………….. 3

Security Concerns ……….…… 4

T-Mobile Merger ………..…….. 4

Vulnerabilities ……………..….. 5

Impact and Implications ……..... 6

Recommendations ………….… 7

Conclusion ……………………. 8

References …………………….. 9

Executive Summary

Hackers were able to get into Sprint and by finding both backdoors and leaks into Boost users’ information. The hackers were able to use their Boost numbers and accounts to get into sprint accounts and breach. The hackers also were able to access Sprint data using samsung.com accounts. With the back door into Sprint through Samsung there are limits. “Since this Sprint breach was through the Samsung website, the scale was limited” (Fingas 2019). The hackers used pin numbers as well to get into Sprint’s data. Sprint was able to reset the pins to fix this backdoor into their accounts. “Sprint says it ‘re-secured’ the customer's account if they received a notification that the account PIN had been reset” (Sprint Confirms Data Breach 2019). This shows us as customers and consumers how unsecure things really are. It’s shocking that the partner cell companies don’t have security blocks on the communication to the main company.

Breach Details

Hackers retrieved Sprint customer’s account information including the account PIN through a backdoor on Samsung’s website. In Sprint’s notice to the customers, Sprint stated “On June 22, Sprint was informed of unauthorized access to your Sprint account using your account credentials via the Samsung.com “add a line” website” (Cimpanu 2019). Sprint goes on to inform the customer that “The personal information of yours that may have been viewed includes the following: phone number, device type, device ID, monthly recurring charges, subscriber ID,

account number, account creation date, upgrade eligibility, first and last name, billing address and add-on services” (Cimpanu 2019). Then Sprint misleads the customer in saying, “No other information that could create a substantial risk of fraud or identity theft was acquired” (Cimpanu 2019). Sprint then informs the customer their account was re-secured on the 25 of June, 3 days after the attack. Sprint then worked to deploy new security measures that will prevent future attacks on their customers on samsung.com and Samsung user accounts. A spokesperson for Sprint reassured CNET “the company takes security very seriously… [information was obtained] using Sprint login credentials that were not obtained from Samsung … [but] no Samsung user account information was accessed as part of these attempts” (Reichert 2019).

Security Concerns

There are great concerns when dealing with cell phone networks. One thing to deal with is SIM card swap. SIM card swaps allow people to breach data by controlling who has access to data. There are also ways to breach data using SMS (Short Message Service). There are two factor authentication which is similar to an agreement between the devices in the SMS conversion. There are ways to bypass the two-factor authentication and allows people to breach data. There are many other ways to breach data with cell phone networks. We need to be concerned with the security of cell phone networks.

T-Mobile Merger

On June 18, 2018, the process officially began to merge T-Mobile and Sprint. With the announcement of this breach, how does it affect this merger between the two companies? This

wasn’t the first time that a breach was discovered in recent years for either company. Both of these companies have been targets, including a T-Mobile breach in the summer of 2018. With these security concerns, there was testing in which, “A security researcher was able to gain unauthorized access to Sprint’s network simply by guessing some very poorly-secured user/password combination” (Ikeda 2019). Since this breach took place, the merger has successfully gone through, so although the breach brought questions and concerns, it ultimately didn’t stop the merger. Both of these companies need to make customer protection a higher priority, as just in the last month, T-Mobile announced yet another breach.

Hopefully, merging the two companies will be a benefit to cybersecurity rather than a downfall. They need to learn from their mistakes and help consumers have peace of mind when giving their private information to cell phone companies.

Vulnerabilities

TrickBot trojan is one of today’s most dynamic and widespread malware strains which are currently capable of carrying out SIM swapping attacks.

TrickBot is one of the prevalent malware families that we see today. It has been active for about three years; the first version was ever seen in 2016 and it is still being actively developed by the threat actors. It started as a banking trojan, but it has evolved into something much more than that, it has info-stealing capabilities. Therefore, TrickBot can also be used as spyware and it is also capable of installing backdoors and other malware, such as the Ryuk ransomware.

TrickBot operators have created new ways and versions of malwares that can intercept and finally steal customers data information. The data that TrickBot collects can allow its operators to carry out SIM swapping attacks.

SIM swapping attack is basically social engineering where hackers will research customers in advance and they will learn names and addresses and all kind of basic information that can usually be found online, they will call and pretend to be the carrier customer service and then trick the customer asking personal information in exchange for promotions such as the last four digits of social security number, once they will get that that will give them enough information to call the wireless company and convince them that they are actually the person who just stole information from and ask to switch their SIM card into their devices.

Threat actors using this method are able to have full access to customers information including bank accounts, this allows the TrickBot operators to bypass SMS-based multi-factor authentication and reset passwords for a victim's bank accounts, they can backdoor their way into customer email accounts and basically get into any online account customers ever created by doing reset password link. TrickBot can also intercept both the victim's account credentials and PIN code. This way hackers can get into customers’ accounts.

Impact and Implications

Sprint’s accounts could be accessed with the account pins that were obtained. These accounts contain customer names, social security numbers, phone numbers, phone models, phone/data plan, subscriber ID, account numbers, account creation date, upgrade eligibility and add-on services. As well as, the customer’s billing information street address, email address, debit or credit card information, and monthly charges. The hacker could do so much with this information. For example, with the phone numbers and models they could catfish the phone or become the man in the middle or hack the phone and get data off that. But of course, the hacker would be able to do the most damage with the billing information, especially the payment card data. The hacker could gain access to the individual’s bank information and ultimately the individual's finances. Again, Sprint does not believe customers are at risk saying in their statement to the customers “the exposed customer data does not pose a substantial risk of fraud or identity theft” because social security numbers and payment card information was not compromised (Cimpanu 2019). However, the hackers would have all the information needed to create a highly believable phishing scheme to obtain that information. Then individuals hit by this data breach are at serious risk and might end up experiencing identity theft, increased junk mail and spam, or breaches in personal data from their phone, or other devices. In a statement sent to CNET a spokesperson for sprint assures “[Sprint] deployed measures to prevent further attempts of this kind” (Reichert 2019). Prior to this statement Sprint notified customers of the need to reset their account pin numbers, seemingly downplaying the urgency some by saying “just in case” (Mathews 2019). Sprint then reset pin numbers of any accounts they thought might be compromised.

Recommendations

After all the information provided about the sprint breach, there are some recommendations that will protect customers against a SIM Swap attack, as it has been already stated SIM swapping is essentially the process of hackers activating customer numbers onto a SIM card in their possession when hackers get ahold of customer phone number and use it to reset customer’s passwords for anything linked to that number. If someone suspect a SIM swap attack it is recommended to do the following: Find a connection as soon as possible and get in touch with the carrier. SIM swapping is a known issue, so if they find evidence of it, they will know what to do. Customers should monitor their email and any accounts that they know are tied to their number.

If any suspicious activity pops up, the first thing to do is to remove the phone number from customer’s accounts, or, if possible, change it to a VoIP number or someone else’s number. Customers need to make sure that the customer service representative locks down their account and gets them a new SIM, protected from unauthorized changes by a PIN.

Even if customers are not sure which accounts have been compromised, it is safest to follow the standard post-hack practice and change customer’s passwords and any sensitive information, such account numbers, that may have been involved. If it happened once, the information that’s floating around the Web could come back to haunt customers again.

Conclusion

This situation has brought more attention to the severity of data breaches. Both Sprint and T-Mobile have been the victims of attacks, in which millions of pieces of data have been accessed by those not authorized. From backdoor attacks to phishing attacks, there needs to be more to protect this information. The good news is that through these attacks, Sprint believes that no serious consequences will come from it. The bad news is that Sprint probably isn’t taking all these data breaches seriously enough. Customers trust companies like Sprint and T-Mobile with their data, but that trust won’t last forever if these attacks keep popping up. To try to help against these issues, Sprint has gone on to help protect consumers by referring to different ways to keep their accounts protected. Though it is a good start, security in these companies needs to be increased.

The Boost attack and the Samsung website attacks could help us to get on track to protecting customer information. Security should be a top priority, and with more research customer information breaches in the cellular industry might not be as common as it seemingly is today.

References

Abel, R. (2019, July 17). Sprint customer data breached via Samsung website flaw. Retrieved from <https://www.scmagazine.com/home/security-news/data-breach/sprint-is-notifying-customers-that-threat-actors-gained-unauthorized-access-to-an-undisclosed-number-of-customer-accounts-via-a-compromised-samsung-website/>

Amir, U. (2019, July 29). Hackers used Samsung website to access Sprint's customer data. Retrieved from <https://www.hackread.com/hackers-used-samsung-website-to-access-sprints-customer-data/>

Cimpanu, C. (2019, July 16). Sprint says hackers breached customer accounts via Samsung website. Retrieved from <https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/>

Fingas, J. (2019, July 16). Hackers broke into Sprint accounts through Samsung's website. Retrieved from

<https://www.engadget.com/2019/07/16/sprint-samsung-account-data-breach/>

Ikeda, Scott. (2019, July 25). Sprint Data Breach Exposes Customers to Unknown Attackers; Will This Impact the T-Mobile Merger? Retreived from <https://www.cpomagazine.com/cyber-security/sprint-data-breach-exposes-customers-to-unknown-attackers-will-this-impact-the-t-mobile-merger/>

Looper, C. de. (2020, February 11). T-Mobile and Sprint Merger: Everything You Need to Know. Retrieved from

<https://www.digitaltrends.com/mobile/t-mobile-sprint-merger/>

Mathews, L. (2019, July 17). Sprint Customer Data Exposed After A Samsung Website Gets Hacked. Retrieved from <https://www.forbes.com/sites/leemathews/2019/07/17/sprint-customer-data-exposed-after-a-samsung-website-gets-hacked/#472add4a16ab>

Reichert, C. (2019, July 16). Sprint customer details have been hacked. Retrieved from <https://www.cnet.com/news/sprint-customer-accounts-breached-by-hackers/>

Security Experts. (2019, July 18). Telecoms Giant Sprint Suffers Data Breach via Samsung Website. Retrieved from <https://www.informationsecuritybuzz.com/expert-comments/telecoms-giant-sprint-suffers-data-breach-via-samsung-website/>

Sprint Confirms Data Breach for Second Time in 2019. (2019, October 21). Retrieved from <https://www.securitymagazine.com/articles/90560-sprint-confirms-data-breach-for-second-time-in-2019>