UBINODES

Research

SIM ATTACKS

Research: SIM Attacks.

Updated 28 November 2017.

The truth about real-life SIM attacks.

We often hear secondhand stories about mobile users' security and privacy being compromised in various ways. The problem with these tales is that they tend to become urban legends or watered-down versions of the original incidents. Due to their seemingly mythical nature, carriers and state-sponsored criminals have been able to continue privacy breaches without facing repercussions.

We have gathered several stories highlighting the vulnerabilities of mobile users' SIM cards. It's crucial to remember that your SIM card contains information about who you are calling, your personal details, and even your location. Here are some examples illustrating the importance of being vigilant about how much our privacy is compromised daily.

1. Data uploading when the device is off The Background

In this example, the user lived in France and owned an iPad Air LTE with a SIM card. The national mobile carrier in France is Orange, so this situation could happen to any Orange subscriber.

While on vacation in Spain, the user was unable to connect to the local 4G signal, despite assurances from the carrier that he should have been able to. Upon returning to France, he found that his iPad was still unable to access the French network, prompting him to contact Orange for assistance.

Orange's customer service asked him to turn off the device to upload the proper SIM settings. After following these instructions, the device worked correctly.

1.1 Conclusion

In this situation, it was discovered that the carrier had access to the user's SIM card, even when the device was powered down. This indicates that some signal is emitted even when the device is not operational. The problem is that both the carrier and state-sponsored criminals could potentially access the user's SIM card without permission or knowledge, even on an iOS device.

Unfortunately, much of the information on a SIM card cannot be altered or removed since it is integral to the carrier network. However, there are some actions you can take to protect your privacy. By purchasing a SIM reader, which is a USB device that plugs into your computer, you can view your SIM card and delete any non-essential stored information.

Additionally, you can contact your carrier and request that they lock your SIM card. This prevents anyone from reading your card but also makes it impossible for the card to be used on another device.

2. Disappearing text messages - The background

In this situation, the user was expecting a new credit card from his bank. The bank informed him that the PIN number for the new card would arrive via text message following his registration of the card, and that the text would disappear after three days. As promised, the text message disappeared after the three-day period.

2.1 Conclusion

This situation demonstrated that not only do carriers have the capability to delete messages from your phone or device, but even banks can do so. The type of text message that can disappear is known as a Flash SMS. This kind of message is not stored in your message inbox and is typically used to capture the user's attention for marketing purposes. While the fact that the message is not stored can be positive, companies can use this method to intrude on the user's device by spamming them.

Fortunately, if you are bothered by Flash SMS messages, there is a way to block them. Depending on your device, there should be an option to disable flash message spam, preventing these messages from appearing. However, if your bank uses this method to send you information, you might not be able to receive those messages.

3. Changing device settings - The Background

A user purchased a new smartphone but wanted to use the old SIM card to retain their phone number and contacts. However, the new phone's internet was not working, prompting the user to contact the carrier for assistance. The carrier sent a text message to the user, and once the text was opened, the internet started functioning on the phone.

3.1 Conclusion

This situation proved that carriers can remotely alter a device's settings through the SIM card, without needing physical access to the device. Carriers use this method to update device firmware, configure handsets, or even lock devices remotely.

Researchers Mathew Solnik and Marc Blanchou tested and found that nearly all devices have a vulnerability in accessing settings remotely. Depending on a hacker's capabilities, much of a user’s phone could be altered remotely. While there have not been reports of hackers or state-sponsored criminals exploiting this vulnerability, the risk remains.

4. Locating you with your device - The Background

A user with a basic phone was near a crime scene and was later contacted by the police. The police used information showing all mobile numbers in the vicinity of the crime to locate the user’s device and interview him about the incident.

4.1 Conclusion

Your device’s location can generally be tracked whenever you are near a cell tower. Carriers triangulate your signal approximately every 10 seconds to provide internet or cellular access. While this ensures connectivity, it also means your location can be monitored whenever your phone or device is active.

It’s important to note that this triangulation provides a general location and cannot pinpoint your exact whereabouts. However, if you wish to use a mobile device, you cannot avoid this process because towers must detect your signal to provide service. Unfortunately, this also means that state-sponsored criminals could potentially exploit this information. Your only defense is to remove the battery or be in a remote area without carrier signal coverage.

5. Finding you with a new SIM - The Background

In this case, a user switched to a new SIM card and carrier, resulting in a new phone number. Despite the change, the previous carrier contacted him on his new number to inquire about switching carriers, which they should not have known about.

5.1 Conclusion

Even though SIM cards have unique identifiers, a person's new information can still be discovered. Both your phone and SIM card contain unique identifiers, allowing entities to track you even if you change your SIM card. In the case mentioned, the previous carrier used the phone's identifier to find the user's new phone number.

If a state-sponsored criminal or hacker wanted to track someone, they could do so even if the individual changes their phone number, as long as they have access to the phone's identifier. To prevent this kind of tracking, it's advisable to purchase a new phone when changing SIM cards, thereby severing the link from the previous SIM card.

6. How to stay safe

The key takeaway from these incidents is that your SIM card contains sensitive information that may be accessible to state-sponsored criminals. To protect yourself, consider using a SIM reader to manage your SIM card securely in case it is lost or compromised. Simply changing your SIM card may not be sufficient for a complete break from your carrier's tracking capabilities. You may need to change both your phone and your carrier to prevent your previous carrier from locating you through your phone's unique identifiers.

It's important to note that you cannot completely prevent your general location from being tracked as long as your device is connected to a carrier network, unless you remove the battery from your device. Stay vigilant about privacy risks related to your SIM card and take steps to safeguard your personal information.