SecurityGen
Telecom Security. Transcending Generations.

A CLOSER LOOK AT LAPSUS$ AND SIM SWAP

Introduction

Recently, the hacker group called LAPSUS$ has been spotlighted by IT publications worldwide. The intruders from LAPSUS$ are reported to have breached NVIDIA, leaked the source codes of Ubisoft, hacked Microsoft and Samsung, and compromised Okta. It was stated that hackers were running their Telegram channel with 50.000 people subscribed, where they were admitting their attacks and even recruiting employees, promising to pay up to $20,000 per week to perform "insider jobs."

As a result of the attacks, hackers were able to penetrate the internal IT systems of the following companies to steal source codes and other confidential information:

NVIDIA has confirmed that hackers gained access to employee credentials and proprietary information. This information included the source code for NVIDIA's latest DLSS technology, promising "groundbreaking" AI-powered rendering.

Samsung has admitted the hack of its systems as well. According to a Telegram post, the hackers leaked 190GB of internal files, including source code for Samsung Knox, the company's security management system.

Another high-profile company targeted by LAPSUS$ was Ubisoft. After hackers posted the news about their attack on the Telegram channel, Ubisoft acknowledged it was a "cybersecurity incident." It is not entirely clear yet how dramatic the attack was for the company.

Authentication software maker Okta has also suffered from the LAPSUS$ hacker attack. The fact that Okta software is being used to secure thousands of organizations obviously raises serious security concerns. Okta has confirmed that approximately 2.5% of its customers, which is about 366 companies, were affected by the attack.

Another victim of the LAPSUS$ hacker group was the British mobile operator Vodafone. The attackers claimed to have stolen about 200 GB of data, which is the source code of Vodafone's software developments. In addition to the Vodafone sources, the attackers also stole the source code and databases of the Portuguese media corporation Impresa and the sources of MercadoLibre and MercadoPago, working in E-commerce.

Even such a giant as Microsoft admitted that LAPSUS$ had "limited access" to its systems. Hackers posted 37 GB of the company's source code online, including 90% of the source code for the Bing search engine. Microsoft claimed that one of the types of attacks used was "SIM swapping" to gain access to critical accounts at target organizations[1]

Before the arrests, the Lapsus$ hack group managed to compromise the telecom giant T-Mobile. The company confirmed this information, saying that hackers penetrated the company's network, gained access to internal tools and source codes. It is emphasized that at the same time, the attackers were unable to steal confidential information about T-Mobile customers. The goal of the attackers was to compromise the accounts of T-Mobile employees, which ultimately allowed them to carry out SIM-swap attacks.[2]

Below, we will illustrate how this type of attack is performed and shed light on the precaution and remediation measures on how to tackle it.

What is the SIM swap?

The SIM swap attack is a malicious action when the malefactors reissue a victim's SIM card and get access to the second factor authentications sent via SMS. When the intruders can read one-time passwords, they can have access to any service that restores the passwords via SMS.

Types of SIM swap

Interception of the second-factor authentication is usually a goal of the SIM swap attackers, and several ways might achieve it.

1) A physical SIM card reissue via social engineering

An intruder needs to impersonate a victim. Often, the intruder knows some personal information about the victim subscriber, such as telephone number, passport ID, birthdate, etc. When the operator reissues a new SIM card, the old one becomes unavailable.

2) SMS interception from the roaming network

The attack works from a remote place, usually from a different country. The victim subscriber is registered in a bogus network controlled by the intruder. After that, all incoming SMS messages start going to the bogus network. Only incoming voice calls and SMS are affected; all other services become on. Moreover, the affected services are restored after the subscriber makes an outgoing call or reloads the device.

3) A physical SIM card reissue via insider

This case almost repeats the first one. Just one difference: the malefactor is not an external person but an internal one. This person usually has access to the operator's client databases, can change information, send, and implement requests. Thus, this malefactor can request a SIM card reissue and execute this request themselves.

Statistics

Complaints to the FBI's Internet Crime Complaint Center (IC3) have skyrocketed in the past year. From January 2018 to December 2020, the **FBI received 320 complaints** related to SIM-swapping incidents with approximately **$12 million** in losses. In 2021, the FBI warned in a new public service announcement that it received **1,611 SIM-swapping complaints** with more than **$68 million** in losses. [3]

According to a Princeton University survey, about **80% of SIM swap fraud** attempts are successful. Meanwhile, another study in the UK shows that the number of SIM swap attacks reported skyrocketed by **400%** between 2015 and 2020. [4]

According to the ENISA report, **52%** of European mobile operators faced SIM swapping attacks in 2021. [5]

What affects the business of MNOs?

The SIM swap attacks are aimed at banking or social media services from first sight. It looks like the MNO's business is not affected. However, if we look at the fines imposed on MNOs, we will see that the governments are aware of the problem and addressing it. For example, Spanish MNOs have imposed fines because the SIM swap attacked 15 subscribers. The total penalty among on three mobile operators was about **5.5 million euros.** [6]

How to protect the networks?

If the mobile operators want to protect their network against SIM swap attacks, they first need to assess the processes and procedures connected with SIM card reissue. This exercise gives a good outlook on the problem from an external point of view. The assessment result will highlight the deficiencies in the processes, which provide the intruder possibilities to perform the SIM swap attacks. As soon as the operator knows the lack, it can be tackled. Also, mobile operators can implement different technical solutions to mitigate the risk of SIM swap attacks. For example, it can be a monitoring solution, which collects information about all legal and illegitimate SIM changes and shares this information with all interested stakeholders such as banks, social media, etc. And, finally, the technical solutions implemented may block the suspicious SIM change attempts.

References

1. https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/
2. https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/
3. https://www.zdnet.com/finance/blockchain/fbi-warns-sim-swapping-attacks-are-rocketing-dont-brag-about-your-crypto-online/
4. https://www.incognia.com/the-authentication-reference/what-is-sim-swap-attack-and-why-fast-detection-is-important
5. https://www.enisa.europa.eu/publications/countering-sim-swapping
6. https://www.enforcementtracker.com/