Secret Hacking Techniques

by: Wisdom (Antonius)

https://bluedragonsec.com

https://github.com/bluedragonsecurity

Example Hacking Scenario by Exploiting the Victim's Phone Number

This technique is very dangerous because the victim's phone number is usually linked to various other account logins such as WhatsApp accounts, Facebook accounts, Instagram accounts, mobile banking accounts, and other accounts.

This time we will not practice it directly because it is not feasible. I will only share the method. Here are some example scenarios that hackers can use to take over the target's phone number, which then extends to taking over all victim accounts linked to that phone number:

SCENARIO 1. SIM CARD SWAPPING ATTACK

For example, a hacker targets someone and the hacker knows the target's phone number which is still active on the target's phone. That number is linked to various victim accounts such as WhatsApp account, Gmail, social media, etc.

Step 1.

If the hacker already knows detailed data about the target's ID card. There are various ways, for example:

Method 1: for example, the hacker obtains a scan of the target's ID card from the internet

Method 2: the hacker has access to population data on the civil registry server

Method 3: the hacker successfully tricks the victim into providing their ID card data using social engineering techniques, for example by pretending to offer a fake job vacancy that requires the victim to submit scanned ID card, diploma scan, certificates, etc.

Method 4: the hacker buys Indonesian population data dumps on the darknet and obtains the victim's population data. Various population data dumps have been found several times being sold on the darknet and hacker forums (such as BreachForums).

Step 2.

The hacker then comes to the store carrying a fake ID card that has been prepared according to the victim's real ID card data and a police loss report about a lost mobile phone.

Sometimes store staff will request additional proof that the phone number to be claimed truly belongs to the hacker by asking for visual proof that the claimant's social media accounts are related to the phone number to be claimed, so the method is very easy. Simply bring a laptop with fake social media websites that have been prepared before coming to the store, with that laptop the hacker can show that the hacker's social media accounts use the claimed phone number.

Example method: the hacker brings a laptop that proves that the number is related to the hacker's social media accounts such as Facebook, LinkedIn, Instagram and Twitter.

How? The hacker creates fake social media websites on their own computer then manipulates the /etc/hosts of those domains to point to the fake websites on localhost.

The fake social media websites essentially show the hacker's social media accounts where the victim's phone number appears to be linked to those social media accounts.

Step 3.

After successfully deceiving the store staff, the hacker will obtain the victim's phone number.

After obtaining the victim's phone number which is active on the hacker's phone, it will be very easy for the hacker to take over other accounts such as Gmail account, WhatsApp, social media accounts or other accounts linked to the victim's phone number.

This action is called SIM Swap Fraud combined with Social Engineering techniques.

How Does the Hacker Do It?

In this scenario, the hacker performs physical verification to convince the store staff (Customer Service). Here is a breakdown of the stages:

1. Identity Theft: The hacker already has the real ID card data. With this data, creating a fake (physical) ID card with the hacker's photo but the victim's data is relatively easy for professional fraudsters.

2. Fabricated Evidence: A police loss report adds legitimacy. Store staff usually do not have direct access to validate the authenticity of police reports in real-time.

3. Local DNS Poisoning (/etc/hosts): This is the clever part. By directing popular domains (FB, IG) to modified local IPs, the hacker visually deceives the store staff. The staff sees that 'the account is logged in on the hacker's laptop,' which strengthens the claim of ownership of that number.

4. Psychological Pressure: The hacker comes with thorough preparation to convince the staff that they are the 'rightful owner who has suffered a misfortune (lost phone).'

Why Is This Dangerous?

Once the store staff issues a new SIM card with the victim's number, then:

• The old SIM card (belonging to the victim) automatically dies.

• The hacker has full control over SMS and phone calls.

• The hacker can perform Password Reset using the 'Forgot Password' feature on banking accounts, social media, and email because the OTP code will go to the hacker's phone.

What Is This Technique Called?

Specifically, this involves several techniques that the hacker combines:

- **SIM Swapping:** The process of transferring phone number service from the victim's SIM card to the hacker's SIM card.
- **Social Engineering:** Psychological manipulation of store staff so they ignore strict security protocols or feel confident with the fake evidence brought.
- **Visual Spoofing:** Using technical manipulation (such as editing /etc/hosts) to create a deceptive visual appearance.

SCENARIO 2. SIM CARD RECYCLING ATTACK

For example, the target previously used a certain phone number, then now that phone number is no longer active.

Step 1.

The hacker who knows that the victim's number is no longer active then buys that number and activates it again, where that number is related to social media such as Facebook, Instagram, Gmail and others.

This condition occurs due to the phone number recycling policy (SIM Recycling) by mobile operators. If a number is not topped up or not used within a certain period of time (grace period expires), the number will expire and after several months will be resold to the market as a new starter number.

Step 2.

After obtaining the victim's phone number which is active on the hacker's phone, it will be very easy for the hacker to take over other accounts such as Gmail account, WhatsApp, social media accounts or other accounts linked to the victim's phone number.

What Is the Technique Called?

In the cybersecurity world, this phenomenon is specifically often referred to as:

- **SIM Recycling Attack:** This is the technical term when someone exploits a recycled phone number to take over the previous owner's account.

- **Account Takeover (ATO) via Recycled Number:** Account takeover that occurs due to physical/legal access to the phone number connected to that account.

Unlike SIM Swap (where a hacker tricks the operator into duplicating your still-active SIM card), in this case the hacker legally owns the number because they bought it officially.

How Does the Hacking Process Occur?

Hackers typically perform the following steps:

1. Target Identification

if the target is an individual:

if the hacker targets someone, it happens that the person has a phone number that has expired and because the time period has been quite long, that number is being resold in the market

if the target is mass (fish in the sea):

The hacker searches for phone numbers that have previously leaked on the internet (through old data breaches) and checks whether the number is still active or not.

2. Number Acquisition: If the number has expired and is available again in the market, the hacker buys it.

3. Account Recovery: The hacker goes to the Facebook, Instagram, or Gmail login page, then enters that phone number and selects the 'Forgot Password' option. Or if it's a WhatsApp account, the hacker simply installs a new WhatsApp application on the phone then fills it with the victim's phone number.

4. OTP (One-Time Password): The password reset code will be sent via SMS to the number now held by the hacker. With that code, the hacker can change the password and fully control the victim's account.

Why Is This Dangerous?

• **Access to Personal Data:** The hacker can view private messages, photos, and contact lists.

• **Access to Finances:** If that number is connected to WhatsApp, Mobile Banking, digital wallets (GoPay, OVO, Dana), or e-commerce, the hacker can drain balances or make transactions.

• **Fraud:** The hacker can pretend to be you to borrow money from friends in your contact list.