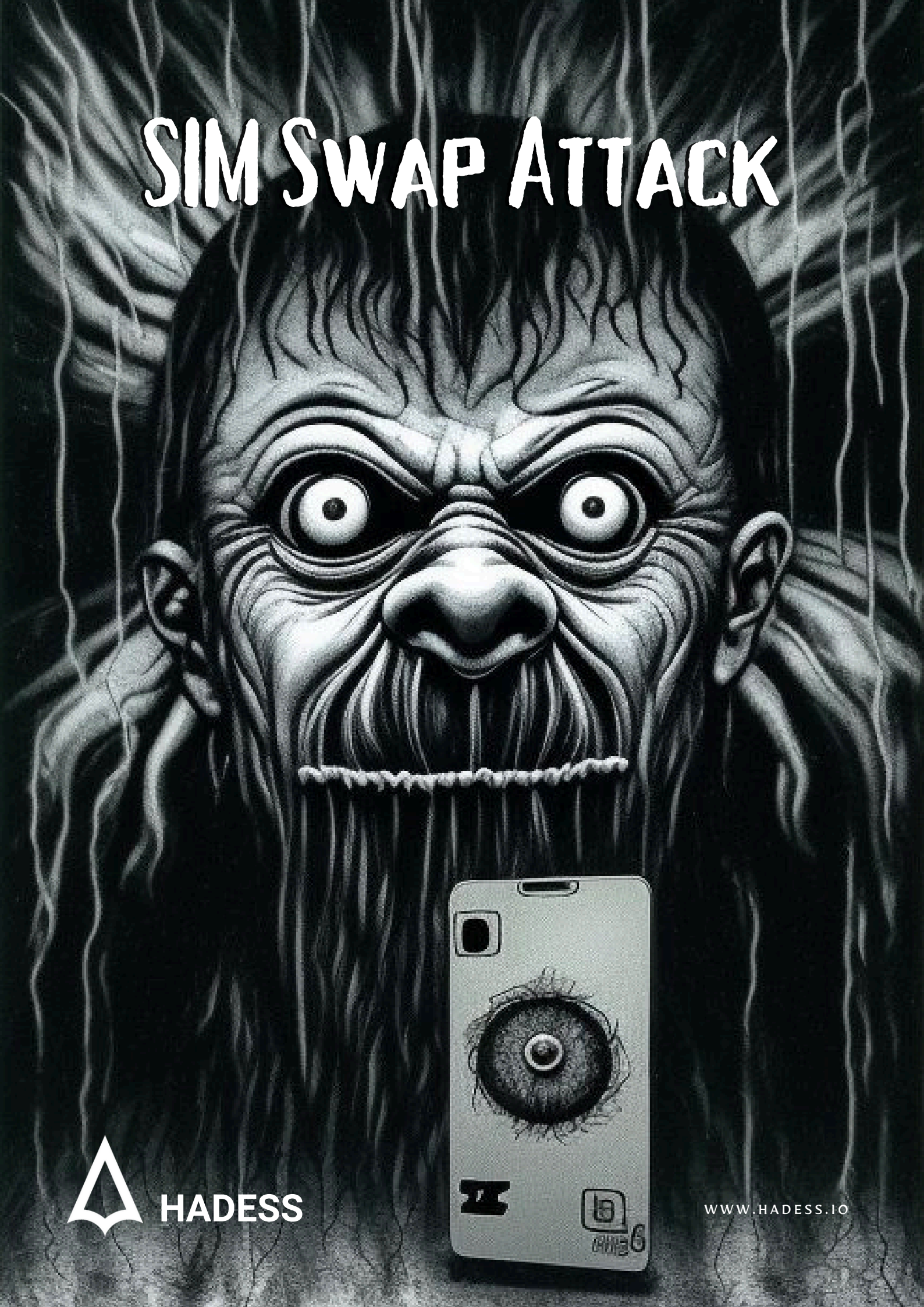
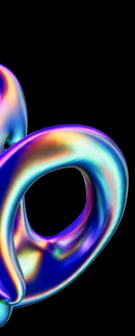

SIM Swap Attack
HADESS
WWW.HADESS.IO



DOCUMENT INFO

HADESS

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.

At Hadess, our mission is twofold: to unleash the power of white hat hacking in punishing black hat hackers and to fortify the digital defenses of our clients. We are committed to employing our elite team of expert cybersecurity professionals to identify, neutralize, and bring to justice those who seek to exploit vulnerabilities. Simultaneously, we provide comprehensive solutions and services to protect our client's digital assets, ensuring their resilience against cyber attacks. With an unwavering focus on integrity, innovation, and client satisfaction, we strive to be the guardian of trust and security in the digital realm.

Security Researcher
SANA BELMEHDI (linkedin.com/in/sana-b-650823263)

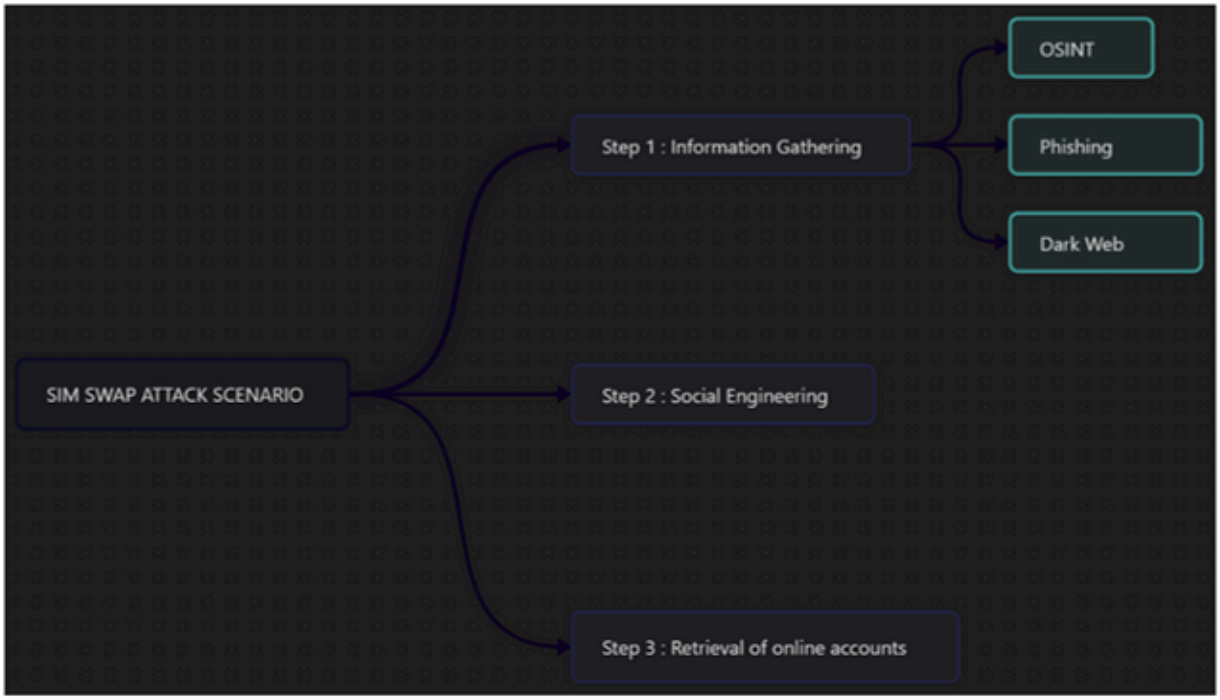
TABLE OF CONTENT

Introduction

SIM Swap attacks are well known to cybersecurity professionals. They allow an attacker to take control of the victim's SIM card, enabling them to validate online payments or change the victim's account passwords. This type of attack is widespread and has caused significant damage worldwide. Recently, in January 2024, the X account of the U.S. Securities and Exchange Commission (SEC) made announcements that rocked the cryptocurrency world. These revelations were actually published by attackers who successfully hacked the SEC's X account using a SIM Swap attack. This attack also caused numerous financial damages. Bart Stephens, co-founder of crypto fund Blockchain Capital, accuses a hacker of using a SIM Swap attack to steal $6.3 million worth of cryptocurrencies such as Bitcoin, Ethereum, and others.

The U.S. Securities and Exchange Commission (SEC) reports that their account was compromised in a SIM-swapping attack. The attacker gained control over the phone number associated with the "SECGov" account and reset its password. The SEC is puzzled about how the hackers knew which phone number was linked to the account. Previously, the SEC had asked support staff to disable Multi-Factor Authentication (MFA) in July 2023 due to "difficulties accessing the account," but they re-enabled MFA after the hacking incident. It appears that the attackers were aware of the specific phone number linked to the account, executed a SIM-swapping attack, and either guessed or knew about the disabled MFA since the summer of 2023.

Context



A Subscriber Identity Module (SIM) card is a chip containing a microcontroller and memory. It is used in mobile phones to store information such as the IMSI

(unique number identifying the subscriber to the SIM card), as well as to perform calculations to ensure network authentication, data confidentiality, and integrity. A few

years ago, when a subscriber wanted to transfer their SIM card to a new mobile phone, they had to physically transfer it from the old phone to the new one. However, today,

phone service providers can virtually reassign SIM cards in modern phones from an old phone to a new one.

Most of time we need two thing:

1. SIM Number

A SIM (Subscriber Identity Module) number, also known as the IMSI (International Mobile Subscriber Identity), is a unique identifier associated with the mobile subscriber. This number is stored in the SIM card and used by the mobile network to recognize and authenticate the subscriber. During a SIM swap attack, the attacker persuades the victim's mobile carrier to associate the victim's SIM number with a new SIM card that the attacker possesses. This can be done through social engineering tactics, where the attacker convinces customer service representatives that they are the legitimate owner of the number, often by providing personal information obtained through phishing or data breaches.

2. ICCID

The Integrated Circuit Card Identification number (ICCID) is an 18-22-digit number typically printed on the back of a SIM card. It is a globally unique serial number that identifies the SIM card itself, distinguishing it from all other SIM cards. No two SIM cards have the same ICCID number, making it a critical component for identifying and authenticating the card.

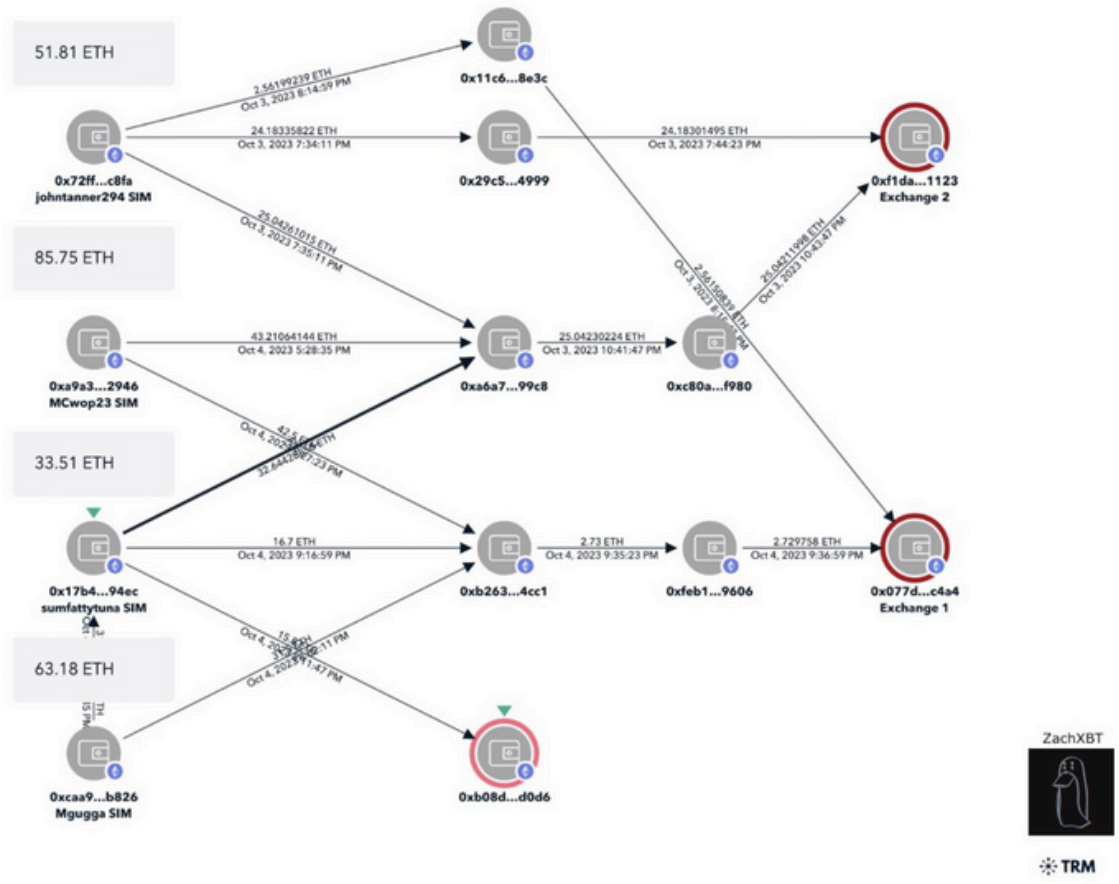
The ICCID consists of several parts:

- Issuer Identification Number (IIN): The initial set of digits identifies the card issuer, usually including a country code and a network code.
- Individual Account Identification: The subsequent digits are unique to the individual SIM card.
- Checksum: The final digit is a checksum for error detection.

In a SIM swap attack, once the attacker gains control of a victim's mobile number, the ICCID of the victim's SIM card is also associated with the attacker's new SIM card in the mobile carrier's database. This change effectively reroutes all communications intended for the victim to the attacker.

Sim Swap Attack

Information Gathering



First, the attacker must target their victim. Once the victim is chosen, they must gather information about them that will allow them to impersonate the victim with the victim's

mobile service provider. To do this, the attacker can use various sources of publicly available information to collect all the elements they will need. This is referred to as OSINT (Open Source Intelligence): obtaining publicly available data. The attacker can also send phishing emails or messages to the victim to obtain as much information as possible.

Phishing is a form of fraud that involves deceiving the victim and extracting personal information from them. Typically, attackers impersonate known organizations of the victim

(banks, social networks, etc.)using their logo and name, and ask the victim to enter personal information. This practice

can be very effective because it allows the attacker to know exactly the information they want. Finally, some attackers purchase people's data on the dark web.

The attacker collects sufficient information about the victim to impersonate them convincingly.

Techniques:

- OSINT (Open Source Intelligence): Gathering publicly available data from social media, public records, and other sources.
- Phishing: Sending deceptive emails or messages that appear to come from trusted organizations to trick the victim into revealing personal information.
- Data Purchases: Buying personal data from the dark web.

Commands and Code Examples:

OSINT Gathering Script

Here's an example Python script that uses the `whois` library to gather basic domain information and the `BeautifulSoup` library to scrape public profiles:

```
import whois
import requests
from bs4 import BeautifulSoup

def gather_domain_info(domain):
    domain_info = whois.whois(domain)
    return domain_info

def scrape_public_profile(url):
    headers = {'User-Agent': 'Mozilla/5.0'}
    response = requests.get(url, headers=headers)
    soup = BeautifulSoup(response.text, 'html.parser')

    profile_info = {}
    profile_info['name'] = soup.find('span', {'class': 'name'}).text
    profile_info['email'] = soup.find('a', {'class': 'email'}).text
    profile_info['phone'] = soup.find('span', {'class': 'phone'}).text

    return profile_info

# Example usage
domain = 'example.com'
profile_url = 'https://socialmedia.com/user/profile'

domain_info = gather_domain_info(domain)
print(f"Domain Info: {domain_info}")

profile_info = scrape_public_profile(profile_url)
print(f"Profile Info: {profile_info}")
```

Social Engineering

Once the attacker has gathered enough information, they call the victim's mobile service provider pretending to be the victim and claiming to have lost their SIM card. They employ social engineerings techniques : the art of manipulating individuals. Using the information collected during the

gathering phase, they can justify their claim by mentioning the victim's name, surname, date of birth, address, and other details, leading the operator's employee to believe they are genuinely speaking with the victim. The attacker then asks the employee to transfer the victim's SIM card to a SIM card they own (or to send them a new one). Once this manipulation is carried out by the employee, the victim's SIM card is deactivated and cloned onto the attacker's SIM card. This is why it's called SIM Swap. Consequently, the attacker now receives the victim's calls and messages on their mobile phone.

Use the collected information to deceive the mobile service provider into transferring the victim's phone number to the attacker's SIM card.

Methods:

1. Calling the Carrier: The attacker calls the mobile carrier, impersonating the victim.
2. Manipulating the Representative: Using the collected personal information (name, address, date of birth), the attacker convinces the customer service representative to transfer the phone number to a new SIM card.

Code Example: Social Engineering Script

While it's unethical and illegal to create a script for social engineering purposes, here's a conceptual overview of how attackers might prepare to make the call:

Social Engineering Preparation Script (Conceptual)

```
def prepare_social_engineering_script(victim_info):
    script = f"""
    Hi, my name is {victim_info['name']}. I recently lost my phone and need to transfer my number to a new
SIM card.
    Here are my details for verification:
    - Full Name: {victim_info['name']}
    - Date of Birth: {victim_info['dob']}
    - Address: {victim_info['address']}
    - Last 4 digits of SSN: {victim_info['ssn']}
    """
    return script

# Example usage
victim_info = {
    'name': 'John Doe',
    'dob': '01/01/1980',
    'address': '1234 Elm Street, Anytown, USA',
    'ssn': '1234'
}

script = prepare_social_engineering_script(victim_info)
print("Prepared Social Engineering Script:")
print(script)
```

In this scenario, the goal is to deceive customer support representatives of mobile operators to replace an old SIM card (belonging to another person) with a new one controlled by the attacker. Here's how it unfolds:

1. Establish Call History: The attackers use SIM cards to make a series of random real calls to create a call history.
2. Contact Customer Support: They then call the mobile operator's customer support and request a SIM card replacement.
3. Fake PIN Attempt: The support representative asks for the PIN. The attackers provide a fake, incorrect PIN.
4. Forgetful Customer Tactic: When the support representative indicates that the PIN is incorrect, the attackers claim they have forgotten the PIN and make various excuses.
5. Call History Verification: The support representative then asks for the details of the two most recent calls. Since the attackers have access to the call history, they can provide accurate details. (In a real scenario, this could involve tricking the victim into making specific calls by claiming they won a contest and need to call a certain number, then redirecting them to another number to complete the process.)
6. SIM Replacement Completion: Seeing the correct call details, the support representative proceeds with the SIM card replacement request.

The attackers tested this scenario with various operators and found it successful every time. They used this method to target several individuals and discovered that they could hijack accounts on 17 different websites that use two-factor authentication (2FA), such as social media platforms.

Retrieval of Online Accounts

To enhance security, most websites and applications implement two-factor authentication for tasks such as changing passwords or making bank transfers. This system verifies the identity of a user attempting to log into an online account. For example, when a user wants to change their password, they receive an authentication code via SMS to a number they provided during registration. They must then enter this code to change their password. This prevents an attacker from changing passwords for accounts they don't own.

Online SMS Receiver Websites

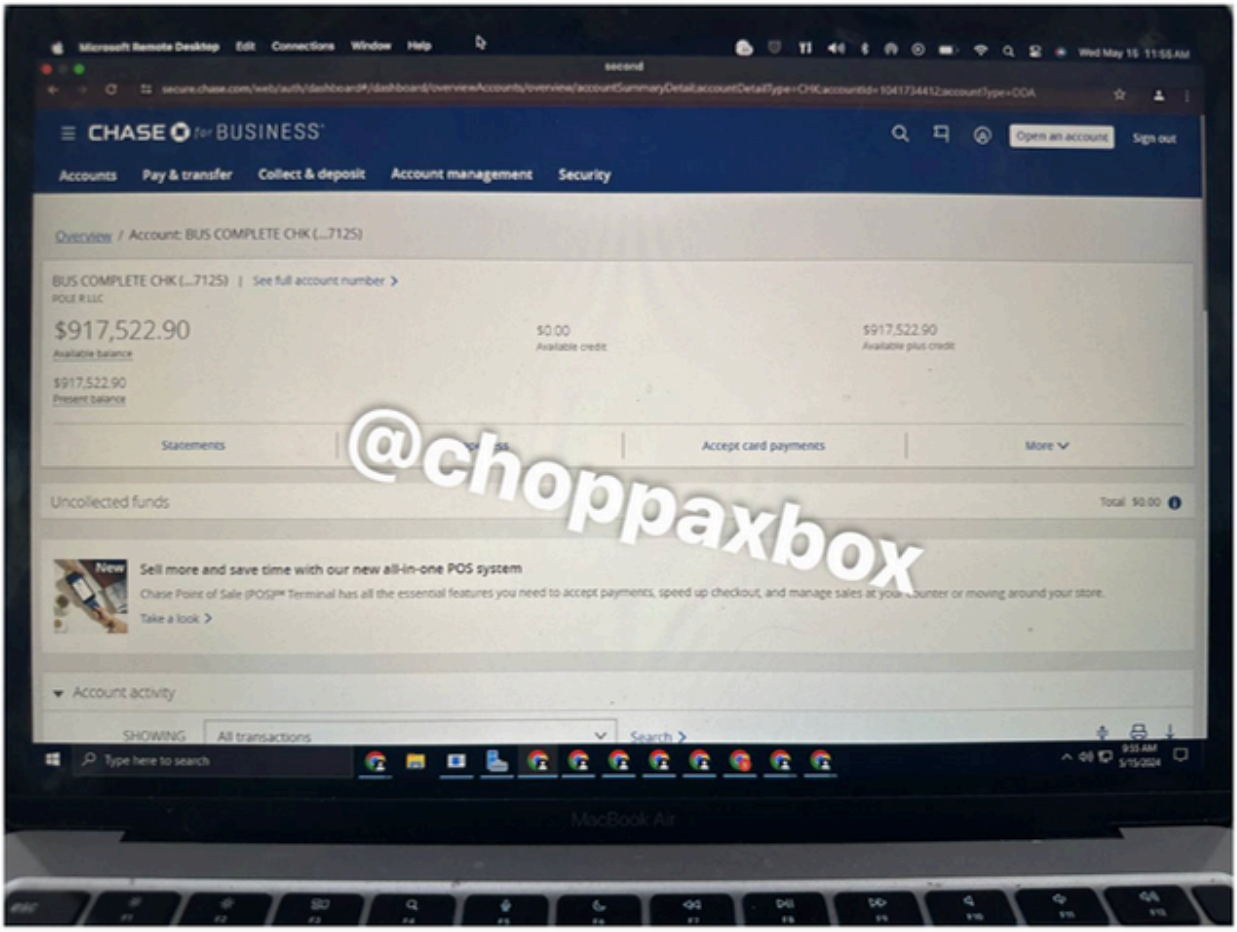
1. AnonymSMS.com: Offers free service with temporary numbers based on real SIM cards[1].
2. FreePhoneNum.com: Provides fresh new phone numbers from various countries, updated every 2 weeks[1].
3. SMS-Online: A platform to send and receive SMS online without registration, offering numbers from the US to the UK[2].
4. Fakenum: An online SMS receiver and sender with a simple refresh system to view new incoming SMS[2].
5. FreeTempSMS: Offers phone numbers from the US and Canada, and allows receiving SMS online without registration[2].
6. Sellaite SMS RECEIVER: Provides public phone numbers from Estonia to receive SMS online[2].
7. Twilio: Known for its reliable service and extensive features[2].
8. Mytrashmobile: Offers disposable phone numbers for receiving SMS online[2].
9. Receive-SMS: Allows you to receive SMS messages without the need for a real phone number[2].
10. Online-sms: Provides a range of phone numbers to receive SMS messages online[2].

Online SMS Receiver APIs

1. Twilio SMS API: Offers scalable SMS solutions with a programmable messaging API[3].
2. Textlocal SMS Gateway API: Allows integration with your website, app, or CRM to send and receive SMS[4].
3. Nexmo: Provides APIs for SMS, voice, phone verifications, and more[5].
4. Tropo: Offers APIs for messaging and voice calls[5].
5. Abstract API: A guide to various SMS APIs with updated information for 2024[6].

These services can be used for various purposes, such as verification, alerts, and two-factor authentication. Remember to review the terms of service and privacy policies of these platforms to ensure they meet your requirements and to understand the potential risks involved in using such services.

Telecom



1. Vodacom

Vodacom, a leading mobile network operator in South Africa, is a prime target for SIM swap attacks due to its extensive user base. Attackers gather personal information through OSINT and phishing techniques, then contact Vodacom's customer service. Posing as the legitimate customer, they claim to have lost their SIM card and request a SIM swap. Once the swap is completed, they intercept the user's SMS-based 2FA codes, allowing them to access sensitive accounts.

2. MTN

MTN, another major telecom provider in South Africa and other African countries, is vulnerable to SIM swap attacks. Attackers exploit social engineering tactics to deceive MTN's customer support. They provide detailed personal information about the victim, which was previously gathered, to convince the support staff to issue a new SIM card. This enables the attackers to intercept 2FA codes and gain unauthorized access to the victim's accounts.

3. Telkom

Telkom, a key telecom operator in South Africa, faces similar threats from SIM swap attacks. Attackers use gathered personal information to impersonate the victim when contacting Telkom's support center. By claiming their SIM card is lost or damaged, they request a new SIM to be activated with the victim's number. Once the swap is successful, they receive all SMS-based 2FA codes and can breach the victim's online accounts.

4. Cell C

Cell C, a prominent telecom service provider in South Africa, is also targeted by SIM swap attackers. The attackers gather sufficient personal information and contact Cell C's customer service, pretending to be the victim. They claim that they need to replace their lost SIM card and provide the necessary verification details. After the swap, they intercept SMS messages, including 2FA codes, to gain access to the victim's accounts.

5. Airtel

Airtel, a major telecom operator in India and various African countries, is susceptible to SIM swap attacks. Attackers collect personal information through various means and then contact Airtel's customer support. They impersonate the victim and report their SIM card as lost or stolen, requesting a replacement. Once the new SIM is activated, the attackers receive all SMS communications, including 2FA codes, compromising the victim's online security.

6. MCI

MCI, a significant telecom provider in Iran, is not immune to SIM swap attacks. Attackers use personal information obtained via OSINT or phishing to deceive MCI's customer service. They claim their SIM card is lost or malfunctioning and request a new one. After successfully swapping the SIM, the attackers intercept SMS messages, including 2FA codes, enabling them to access the victim's accounts.

7. Golan Telecom

Golan Telecom, an Israeli telecom operator, faces threats from SIM swap attacks. Attackers gather personal information about their target and contact Golan Telecom's support, posing as the victim. They claim to have lost their SIM card and request a new one. Once the SIM swap is done, they intercept 2FA codes sent via SMS to gain unauthorized access to the victim's accounts.

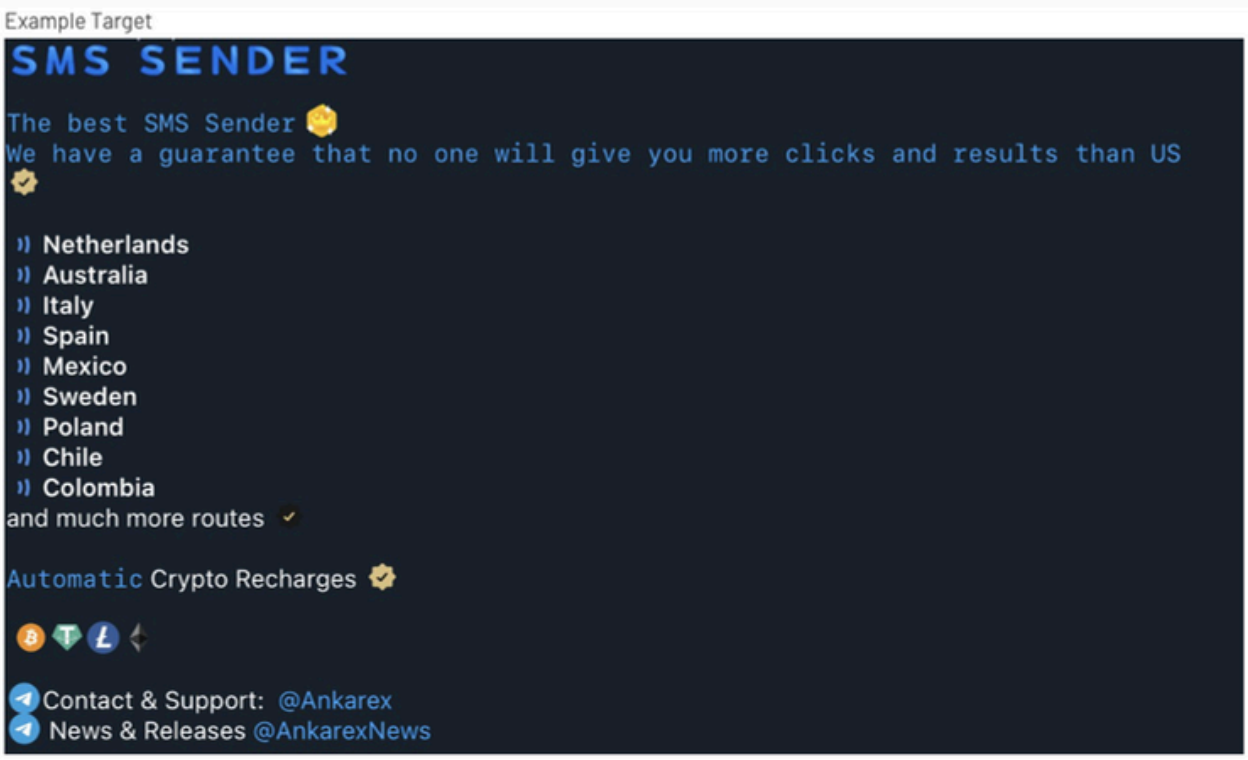
8. Verizon and T-mobile

Verizon, a leading telecom provider in the United States, is a frequent target for SIM swap attacks. Attackers use social engineering techniques to gather enough personal information to impersonate the victim. They contact Verizon's customer service, claim to have lost their SIM card, and request a new one. After the swap, they intercept SMS-based 2FA codes, allowing them to breach the victim's accounts.

9. Vivo

Vivo, a major telecom operator in Brazil, is also at risk of SIM swap attacks. Attackers gather personal information through various methods and contact Vivo's customer support. They impersonate the victim, report their SIM card as lost or stolen, and request a replacement. Once the new SIM is activated, the attackers intercept SMS messages, including 2FA codes, compromising the victim's online security.

Example Target



This service provides access to SIM swaps for T-Mobile, AT&T, and Verizon mobile phone numbers. Each carrier has specific requirements and pricing for the service.

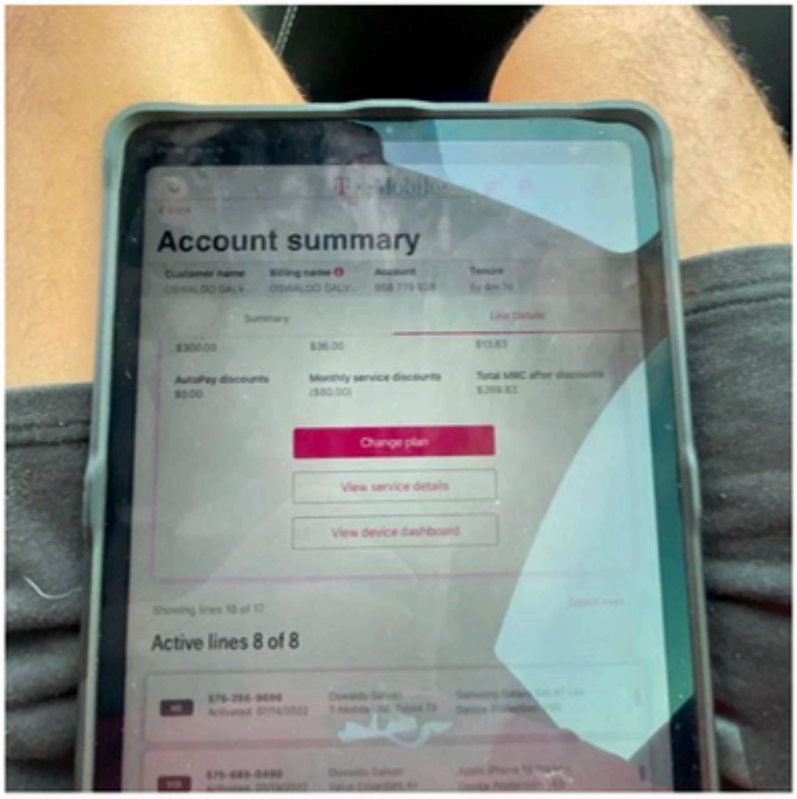
Figure 1: A cybercriminal auctions off administrative and VPN access to a telecommunications provider

Carrier Requirements

1. T-Mobile (TMO)
   - Condition: The phone number must not be a business number.
   - Price: $7,000 + 15% service fee.
2. AT&T (ATT)
   - Condition: The phone number must not have extra security. Confirmation on this can be provided immediately.
   - Price: $8,000 + 15% service fee.
3. Verizon (VZ)
   - Condition: The phone number must not be a business number.
   - Price: $10,000 + 15% service fee.

Vouch Swaps

To establish credibility and demonstrate the effectiveness of the service, I am offering two vouch swaps for each carrier. These vouch swaps are available to highly reputed and known forum members. Participants in the vouch swap will receive a 25% share of the service fee.



Available Vouch Swaps:

- T-Mobile: 0/2 vouch swaps available
- AT&T: 0/2 vouch swaps available
- Verizon: 0/2 vouch swaps available

Available Vouch Swaps:

- T-Mobile: 0/2 vouch swaps available
- AT&T: 0/2 vouch swaps available
- Verizon: 0/2 vouch swaps available

Contact and Participation

If you meet the criteria and are interested in participating in a vouch swap or using the service, please reach out. The process is straightforward, and for AT&T, confirmation of the number's security status can be provided instantly. This ensures a smooth and efficient transaction.

Pricing Summary

- T-Mobile: $7,000 + 15% service fee
- AT&T: $8,000 + 15% service fee
- Verizon: $10,000 + 15% service fee

By participating in this service, you agree to the terms and conditions outlined above. For those interested in the vouch swap, the 25% share is a significant discount, allowing you to experience the service at a reduced cost while contributing to its credibility within the community.

Signs of a SIM Swap attack

When one is a victim of a SIM Swap attack, the shorter our reaction time, the lighter the consequences. Indeed, if we realize quickly that we are undergoing this type of attack,we can contact our operator and deactivate the attacker's mobile phone SIM card, preventing them from accessing all our online accounts.
That's why it's important to mention the signs of such an attack. Three signs can be identified:

1. Inability to make calls, send SMS messages, or use cellular networks. Additionally, there is no longer any reception of messages or calls.
2. Email notifications of a SIM card change.
3. Loss of access to online accounts (social networks, etc.).

Howto Protect Yourself

There are several actions to implementin order to minimize our vulnerability to this type of attack. First, as mentioned earlier, the attack involves a data collection stage: the attacker needs information about their victim to impersonate them with the mobile operator. Thus, limiting one's exposure on the internet and being cautious about the personal information one shares online is crucial. Additionally, phishing is extremely dangerous in this type of attack. It is therefore crucial to pay attention to the emails and SMS messages received and to analyze them to ensure they are fromlegitimate services. Donothesitate tocall your bank or the service that contacted you to verify verbally that the emailtruly came from them. Where possible, using PIN codes and security questions to which only you know the answer, mandatory before performing any manipulation involving your SIM card and various online accounts, will also help mitigate risks.

Finally, it is beneficial to use authentication applications, which allow for 2FA mechanisms through a mobile application instead of via SMS.

The Federal Communications Commission (FCC) has issued a stern reminder to mobile phone service providers, emphasizing the need to enhance protections against fraudulent SIM swaps. This advisory follows the findings of the Cyber Safety Review Board (CSRB) announced in August, which highlighted the operations of the hacking group Lapsus$. This group is notorious for using SIM swaps to extort victims globally.

Background and Recent Developments

The CSRB's detailed report on Lapsus$ underscored the growing threat of SIM swap fraud. This type of cyberattack involves criminals deceiving mobile carriers into transferring a victim's phone number to a new device under their control. Once they have access, attackers can intercept text messages, including those used for multifactor authentication (MFA), to gain unauthorized access to the victim's financial and personal accounts.

FCC's Updated Advisory

On Monday, the FCC's Privacy and Data Protection Task Force issued a new advisory highlighting the increasing incidence of SIM swap fraud. The advisory included reminders about updated requirements for telecommunications service providers to bolster the security of consumer data. Key points from the advisory include:

1. Enhanced Customer Verification: The updated FCC rules mandate that carriers implement more stringent procedures to verify customers' identities before linking phone numbers to new devices or carriers. This aims to close the gaps that scammers exploit.
2. Alerting Customers: Carriers must promptly notify customers of any changes to their accounts. This includes alterations to passwords, customer responses to backup authentication methods, or any other significant records.

Multifactor Authentication and Security Measures

The CSRB and FCC both advocate for moving away from SMS-based MFA methods, which are vulnerable to interception through SIM swaps. Instead, they recommend more secure alternatives, such as authentication apps or hardware tokens.

Loyaan Egal, FCC Enforcement Bureau Chief and chair of the Privacy and Data Protection Task Force, emphasized the high stakes involved: "Cell phone service providers are high-value targets for cybercriminals and scammers because they often serve as the primary means consumers use today to access their most important and valuable financial and personal information."

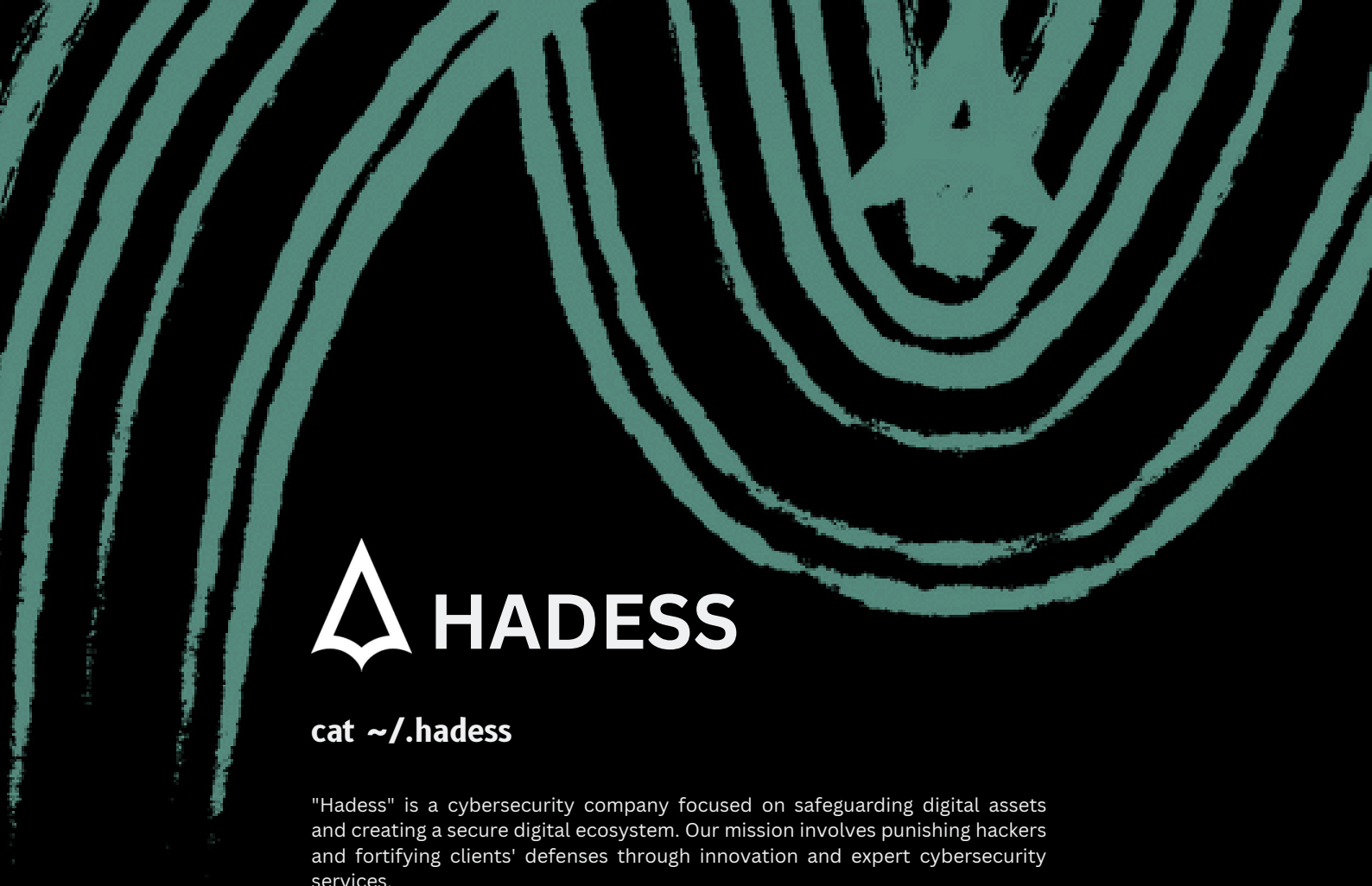
Case Study: Verizon Incident

A recent incident involving Verizon highlights the dangers of inadequate security measures by carriers. Last week, Verizon was reported to have given a woman's stalker access to her sensitive data, including her address and phone records, based on a fake search warrant. This incident, reported by 404 Media in collaboration with Court Watch, underscores the urgent need for carriers to strengthen their protocols for verifying legal requests and safeguarding customer information.

References

TY - BOOK, AU -Hallman,Roger, PY - 2023/12/04, SP - T1 , SIM Swapping Attacks forDigitalIdentity Theft: A threatto financial services and beyond, VL - ER -

- The Cyber Threat Landscape of the Telecommunications Industry by INTSIGHTS
- https://medium.com/geekculture/sim-swap-fraudhow-it-works-how-to-fix-it-b66b9afdf54b
- https://www.incognia.com/the-authenticationreference/what-is-sim-swap-attack-and-why-fastdetection-is-important?hs_amp=true



HADESS

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Email
MARKETING@HADESS.IO

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.