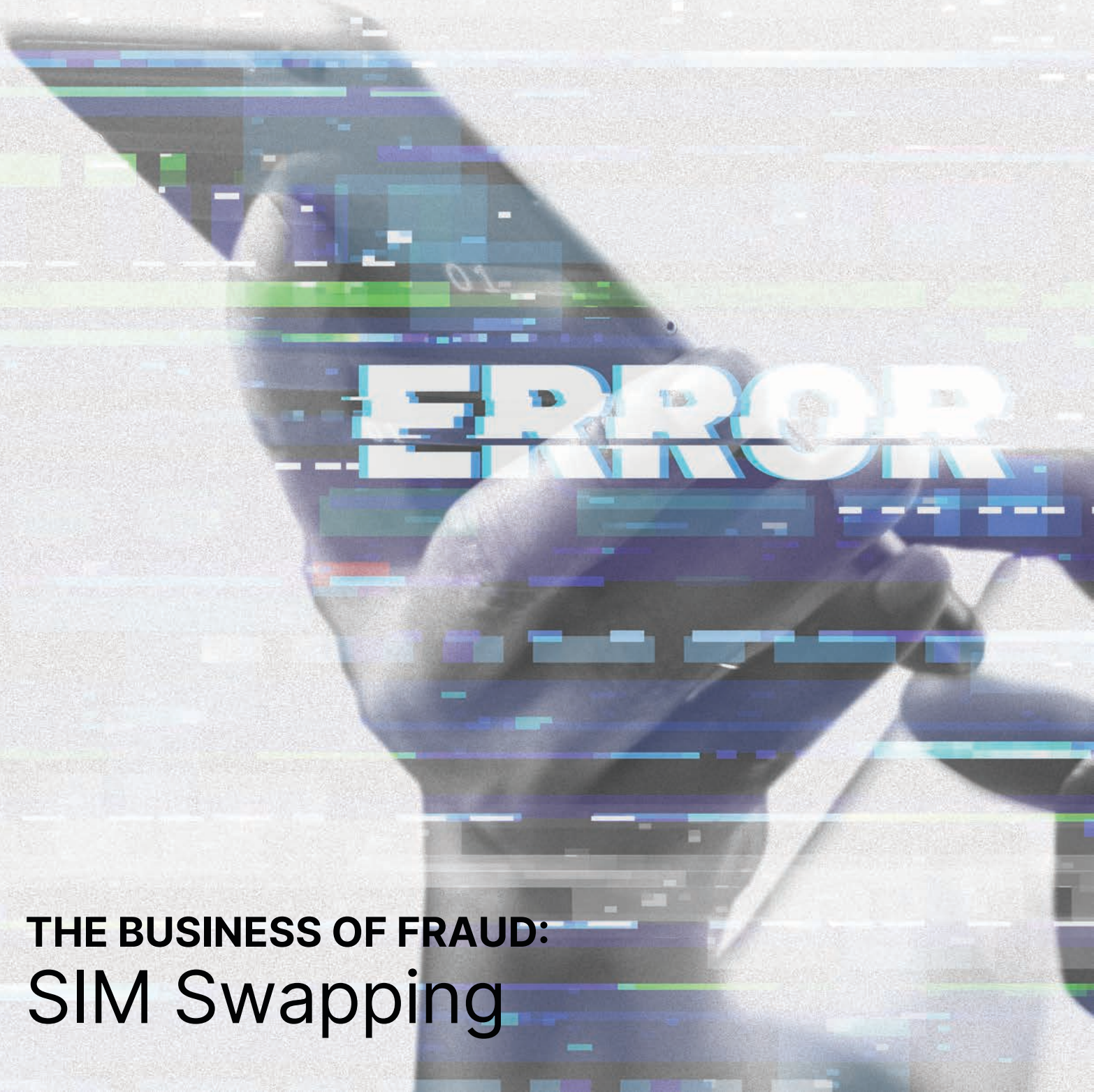
CYBER
THREAT
ANALYSIS

Recorded Future®

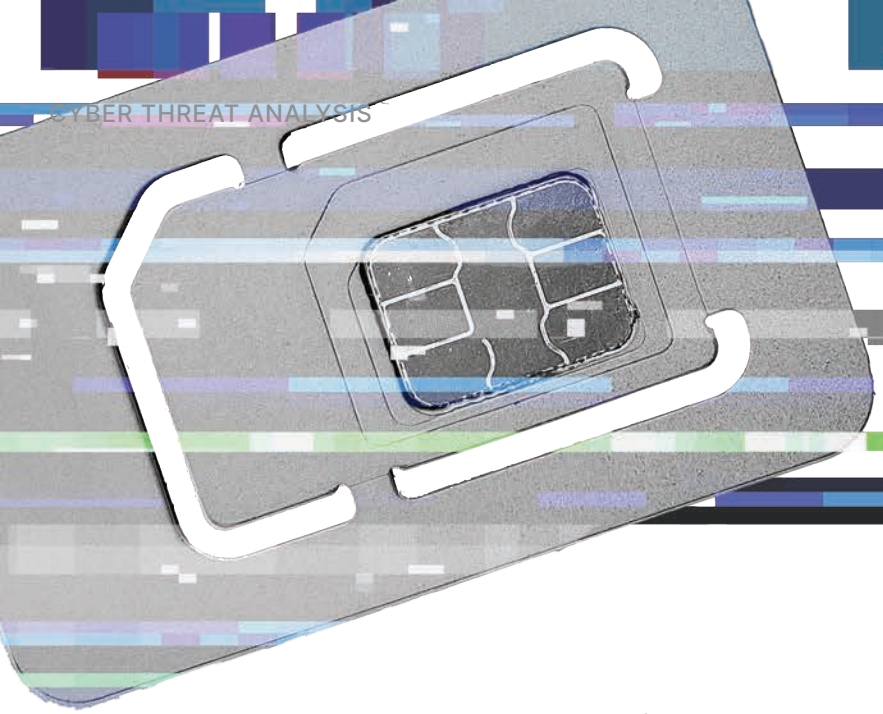
By Insikt Group®

August 25, 2021



THE BUSINESS OF FRAUD:
SIM Swapping

Recorded Future®



Recorded Future analyzed current data from the Recorded Future® Platform, dark web sources, and open-source intelligence (OSINT) from June 2020 to June 2021 to review the current landscape of SIM swapping fraud. This report expands upon findings addressed in the first report of the Insikt Group's Fraud Series, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized".

Executive Summary

SIM swapping involves deceiving a mobile provider (usually through social engineering) into transferring a victim's phone number to a SIM card controlled by a cybercriminal. Once the SIM card has been activated, a cybercriminal controls the phone number and can reset victim passwords and take control of social media, online banking, and cryptocurrency accounts. In some instances, even security measures such as two-factor authentication (2FA) can be bypassed. Among the primary targets for cybercriminals are organizations and services in telecommunications, banking, financial, cryptocurrency, and information technology (IT). There is a stable demand for SIM swapping services and how-to guides, predominantly on English- and Russian-language dark web marketplaces and forums. We look at those services in this report and identify several of the most active threat actors involved in fraud related to SIM swapping.

Key Findings

- Threat actors advertise and request SIM swapping services mostly on English- and Russian-language dark web forums. Cybercriminals primarily advertise and sell SIM swapping tutorials and how-to guides on dark web marketplaces.
- Typical prices for SIM swapping how-to guides and tutorials range between $40 and $200; however, in rare cases, they can reach up to several thousand US dollars.
- Among the primary TTPs used to perform SIM swapping fraud are social engineering, phishing, insider threats, and purchasing compromised personally identifiable information (PII) data on dark web forums, marketplaces, and shops.
- We believe that insider threats, in which threat actors receive assistance from an employee of an organization that can assign the phone number to a different SIM, are currently one of the most popular and successful ways to perform SIM swapping attacks.
- How-to guides on SIM swapping, for sale or freely available, outline some of the most popular TTPs for SIM swapping attacks. They show how to stay anonymous, outline how to gather intelligence on the carrier to conduct a social engineering attack (including test calls), and give advice on purchasing compromised PII on the targeted victim and acquiring SIM cards.

Background

SIM swapping fraud, also known as SIM card hijacking, is a technique used by threat actors to gain access to a victim's phone number with the end goal of using multi-factor authentication (MFA) to obtain access to the victim's online accounts, such as banking, social media, cryptocurrency, and other personal or corporate accounts. This attack vector most commonly involves deceiving a telecommunications (carrier) provider into transferring a victim's phone number to a SIM card under the control of the cybercriminal. This is accomplished by obtaining user information via phishing and reconnaissance (using open sources, leaked databases, dark web forums, and marketplaces), which is then used to convince the victim's carrier to transfer or "port" the victim's phone number to the SIM card under the cybercriminal's control. Our data collections identified 774 SIM swapping-related references over the past year, indicating that cybercriminals primarily target the following industries when using SIM swapping attacks: telecommunications, IT and software, consumer electronics, finance and cryptocurrency exchanges, and publishing.

A normal practice for mobile phone users who lose their phone is to ask their carrier to replace the old SIM card with all of their contact information while continuing to use the original phone number .This step is important for a successful SIM swapping attack and requires threat actors to collect as much information as possible regarding a potential victim using the following attack vectors:

- Social engineering
- Phishing
- Purchase of compromised PII data on dark web forums, marketplaces, and shops
- Insider threats

The primary steps to perform a successful SIM swapping attack through social engineering techniques are as follows:

- Identify the phone number of the victim and their PII.
- Call the carrier to report the loss of the phone to block the SIM card.
- Carriers transfer the phone number to the controlled SIM card. In this case, the attacker can use the SIM card on a separate mobile device and still maintain access to the victim's contact list, make and receive phone calls, and send short message service (SMS) messages. By intercepting SMS verification codes, cybercriminals gain access to most multi-factor authentication methods used by financial organizations.

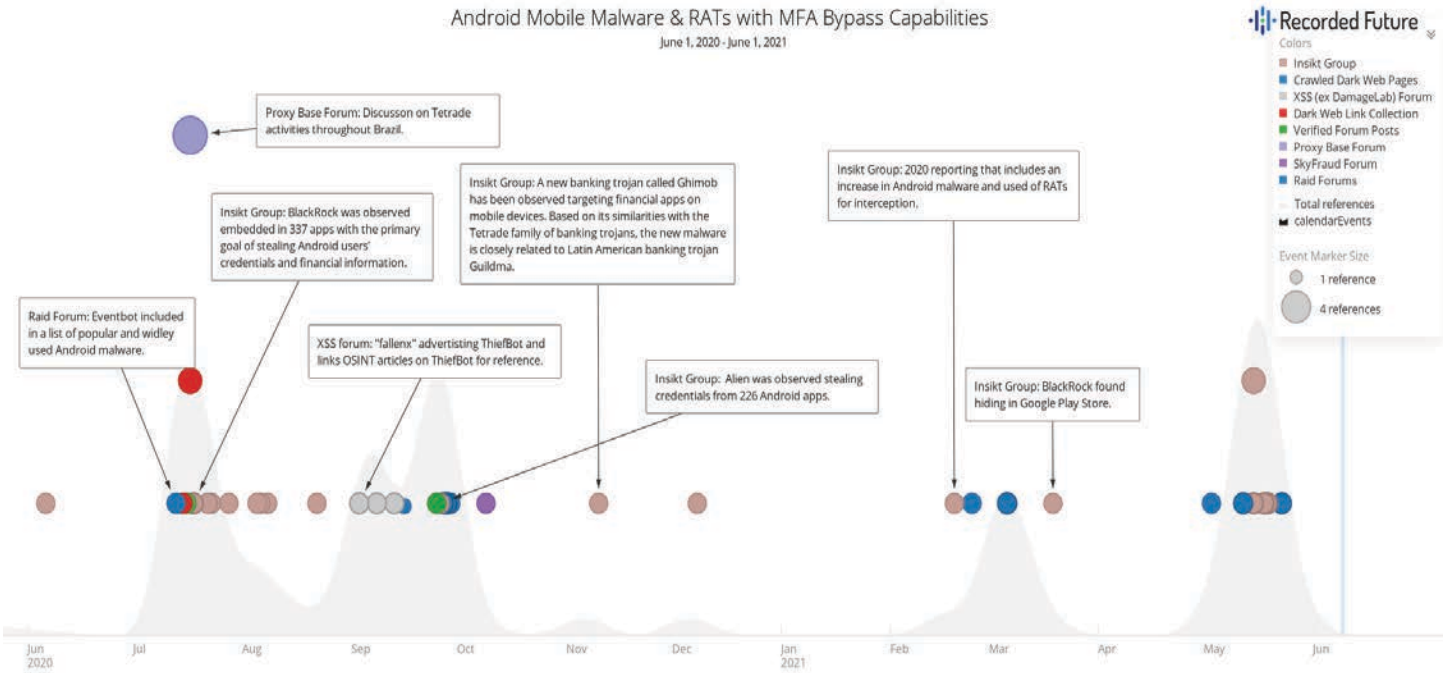


Figure 1: Sample of activities associated with mobile malware that defeats MFA (Source: Recorded Future)

As carriers and telecommunications-related entities have become better aware of and trained in identifying social engineering, threat actors have continued to update their tactics to defeat enhanced security measures. One such SIM swapping-related method is phone porting, a tactic by which cybercriminals transfer a phone number from one carrier to another without the need to change the SIM card. Attackers will obtain user information via phishing and reconnaissance (using open sources, leaked databases, dark web forums, and marketplaces) and then use it to convince the victim's carrier to transfer or "port" the victim's number to the phone in the attacker's possession. We observed cybercriminals showing interest in SIM porting; however, its popularity is significantly less than SIM swapping based on the small number of references found on the dark web forums and marketplaces for the past year.

Lastly, SMS interception is a different attack vector based on targeting the global telephony protocols Signaling System 7 (SS7), increasing in popularity and use. SS7 protocols allow phone networks to exchange calls and SMS with each other; gaining access to this interchange system allows attackers to mimic a telephone number and man-in-the-middle (MitM) the telecommunication system to intercept communication. SMS interception requires technical proficiency from a hacker and is usually performed by threat actors who operate botnets, web injects, phishing kits, or other malware, specifically remote access trojans (RATs), to compromise high-value targets. We observed more requests than offerings for this service on dark web sources. As carriers continue to update security measures to defeat SIM swapping attacks, we believe that cybercriminals will continue to develop and evolve SMS interception methods so that it becomes easier to defeat MFA.

Cybercriminals use different types of malware to circumvent multi-factor authentication (MFA). MFA is a security enhancement in which a user is granted access to an account only after successfully submitting 2 or more layers of protection (factors). We identified the following sample of mobile malware and Android RAT variants that contain call forwarding/intercept features capable of defeating MFA: Alien, TrickMo (TrickBot mobile variant), Eventbot, Tetrade, BlackRock, Thiefbot, and Wroba. Figure 1, below, highlights activities of these variants over the last year, as reported by Insikt Group and collected across dark web sources:

Threat Actors and SIM Swapping

As part of our research, we examined our data sets from June 2020 to June 2021 and conducted manual research to identify sources where threat actors discuss SIM swapping, specifically requests for services; advertisements of how-to guides, tutorials, and products; and announcements for recruitment and cash-out services via SIM swapping conducted in specific countries. We identified that dark web and special-access sources are the preferred sources for threat actors when advertising, discussing, or purchasing these products and services. Analysis of findings identified the following themes:

- Dark web and special-access forums, ranging from low- to high-tier, are primarily used for recruitment (meeting like-minded threat actors) and advertising the following SIM swapping services: cashing out, targeting specific entities (global or country-specific companies), and having access to an insider.

Threat Actor	**Intelligence**
"Brand"	In May 2021, the threat actor advertised a SIM swapping course on an English-speaking forum for $200 that included the following learning objectives: • How to find and verify a carrier's PIN • How to bypass MFA to gain access to a carrier's online account • How to dox a victim and cash out (wire transfer tutorial) for bank accounts Access to the course includes scripts for live chat.
"Smaill00"	In August 2020, the threat actor expressed interest on WWH Forum in partnering with US-based threat actors for their SIM swapping and SMS intercept services. The threat actor stated they also conducted fraudulent calls. Based on forum threads, the threat actor successfully partnered with other users (monikers not identified via thread).
"asxushuai"	In June 2020, the threat actor requested services and indicated an interest in cooperating with another in SS7 SMS interceptions on Hack Forums. The threat actor stated that candidates must prove their capabilities using phone numbers provided by asxushuai. The threat actor instructed interested partners to contact them via asbet365@protonmail[.]com.
"novaking"	From June to November 2020, the threat actor offered SIM swapping services against various US carriers to bypass SMS 2FA and to get access to victims' bank accounts with subsequent cashing out of stolen funds. The threat actor stated that their profit share for this service is 70%.

Table 1: Threat actors offering SIM swapping guides and services on dark web forums between June 2020 and June 2021 (Source: Recorded Future data)

- Dark web marketplaces are used by threat actors to advertise and sell how-to guides and tutorials on SIM swapping and defeating MFA. A majority of these guides and tutorials are not brand-centric but instead designed to defeat any carrier's MFA security measures.
- In addition to marketplaces, dark web and special-access forums also advertised how-to guides and tutorials, with threat actors providing free samples in exchange for reviews.

Dark Web and Special-Access Forums

Using our data sets on dark web and special-access forums, we identified the following to be the most widely used sources for those interested in SIM swapping: Raid, Verified, Hack Forums, Club2CRD, Sinisterly, WWH Club, and others.

The following table provides a sample of relevant and unique posts obtained from these sources, highlighting how threat actors are using these sources to discuss SIM swapping topics, services, and advertisements:

Analysis of SIM swapping Guide on Forums

In addition to the forum activities outlined above, we identified forum users posting tutorials, some for a price and some for free, and how-to guides on conducting a SIM swapping attack. One threat actor, "PKBonaFide", publicly shared on a top-tier Russian-speaking dark web forum (March 24, 2021) a SIM swapping tutorial against US mobile carriers where they explained in detail steps for a successful SIM swapping attack:

1. Purchase compromised bank account login credentials (on unspecified dark web sources: forums, shops, and marketplaces).
2. Log in to the purchased bank account and check transactions related to mobile phone bill payments (some of them indicate mobile carrier account number (SIM cards)).
3. After obtaining the account number, an attacker should find a PIN or passcode to replace a phone number.
4. Use a background check to collect information regarding a victim. PKBonaFide stated that in 70% of cases, cybercriminals can obtain PINs and passcodes through social engineering targeting the carrier's customer support. According to the threat actor, customer support will ask questions to validate a customer's identity, including questions related to their addresses, paid phone bills, or information about family members.
5. To obtain a PIN or passcode, the attacker should call a provider using the victim's phone number through substitution with the help of voice over internet protocol (VoIP).
6. After obtaining a PIN or passcode, it is necessary to purchase a new SIM card of the same mobile carrier (using a drop in the US) and wait for approximately 1 to 2 weeks. After waiting, call the carrier using a newly purchased SIM card. Some mobile operators can monitor international calls to identify fraud.
7. Additional security measures suggested before calling the carrier:
    a. Refill a balance using virtual credit cards.
    b. If the caller reports a lost or stolen phone, the carrier can check their most recent calls and geolocation.
    c. Prepare for answering security questions using obtained victim PII information.
8. After the carrier's approval, the SIM card replacement usually takes between 24 and 72 hours.

The threat actor stated that it is better to purchase a compromised bank account with balances that exceed $100,000 or more.

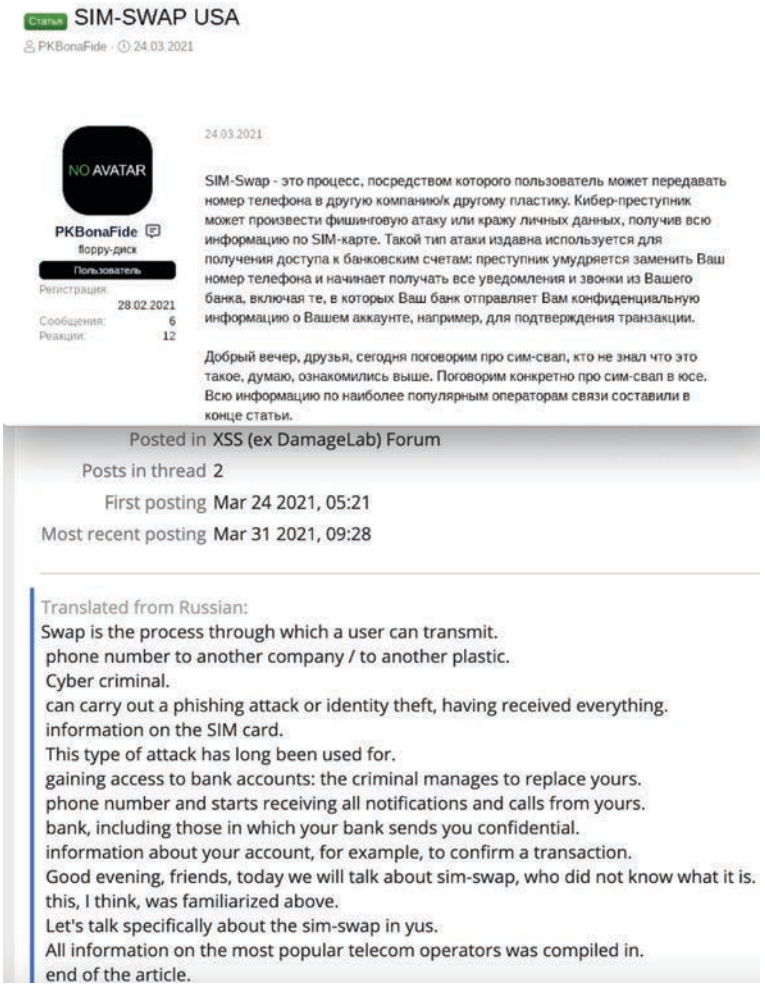


Figure 2: PKBonaFide shared a SIM swapping guide against US mobile provider (Source: Recorded Future)

Insider Threats

We also identified forum members looking for insiders at US and international carriers for subsequent SIM swapping attacks. As a rule, cybercriminals look for insiders when they identify compromised bank or cryptocurrency exchange accounts of high-profile victims. Typically, the profit share arrangement with these partners is between 30% and 50% of account balances; in some cases, cybercriminals are ready to pay insiders significant upfront payments for regular cooperation.

The following table includes a sample of threat actors requesting and offering access to insider threats at major carriers on high-tier forums:

Threat Actor	Intelligence
”sui“	In June ,2021 sui claimed to have access to an insider at a major telecom company and offered a SIM swapping service for 1,000$ per operation .According to the threat actor ,they will need a victim‘s phone number and Integrated Circuit Card Identification Number) ICCID ,(which consists of 19 to 20 characters and usually refers to the SIM card itself .The threat actor stated that SIM swapping will be done in 10 to 30 minutes after receiving payment and recommended interested parties to reach out via the Telegram@ Sergei093 .It is worth noting that sui posted the advertisement both in English and Russian ,with the Russian version including that sui has” preliminary assessment software “for that telecom company.
”chopo“	In June ,2021 chopo was looking for an insider at a major US telecom company who can perform SIM swapping for 500$or profit-sharing per attack.
”butterfly“	Since May ,2021 the threat actor has been searching for employees of the major US telecom providers whose primary responsibilities should be providing subscribers ‘ICCID and PINs .butterfly claims to be ready to pay up to200,000$ per year ,including upfront payments.
”Morphismblock“	In February ,2021 the threat actor claimed to be able to SIM swap US phone numbers of specific mobile carriers with an insider‘s help and compromise linked cryptocurrency and other accounts for subsequent cash out .The threat actor uses the following methods of communications :Telegram@) tools32Mob1 ,(Wickr@) shanjiru ,(and ICQ@) unknowm.(
” Rumble747“	In December 2020 through January ,2021 the threat actor offered a SIM swapping service against Verizon and AT&T with the help of insiders at the aforementioned organizations .According to the threat actor ,they could compromise users ‘Verizon and AT&T accounts ,accept payments ,and cash them out for a profit share .The threat actor uses the Telegram handle@ bigT121.
”simswap“	In July ,2020 the threat actor was seeking to recruit employees from a major US telecom provider .We also observed the aforementioned threat actor looking for an SMS gateway to perform SMS spamming primarily against victims in South America ,Europe ,and Australia .The threat actor uses 2 Telegram accounts@) *bigT121* and@ *tools32Mob1,*(Discord@) *simswap* ,(*0366#*and ICQ@ *AZ32719* as points of contact.

Table 2: Threat actors looking for or using carrier insiders for SIM swapping fraud (Source: Recorded Future data)

SIM swapping Guides on Dark Web Marketplaces and Shops

We examined dark web marketplaces for SIM swapping advertisements and services, specifically how-to methodologies, guides, and tutorials targeting carriers. Our data sets indicate the following dark web marketplaces and shops as having the most activity involving SIM swapping advertisements from June 2020 to June 2021: The Canadian HeadQuarters (hereafter referred to as Canadian HQ), Agartha, ToRReZ, Versus, DeepSea (closed in October 2020), and Infinity Market.

Table 3 outlines a sample of threat actors we found who are offering unique SIM swapping methods and how-to guides, as well as those who have received positive feedback and are experienced marketplace vendors:

Threat Actor	Intelligence
”A-Man“	In May ,2021 the threat actor advertised SIM swapping and SIM porting tutorials for.8,000$
”chernobyl“	In May ,2021 the threat actor was observed advertising a dark web shop specializing in the sales of compromised PII) payment data ,money laundering ,SIM swapping guides ,and more .(According to the advertisement ,the seller has been in the fraudulent business for more than 10 years and uses Telegram@) travisden and operates the Telegram channel@ darkveganchannel with over700 subscribers (for communication and advertisement.
”Kanuckk“	In April ,2021 the threat actor offered a SIM swapping method for .40$ According to the threat actor, all their methods are private and authored by them.
”stashthecash“	In April ,2021 the threat actor was observed selling 8 how-to methods ,including 2 SIM swapping and 2MFA spoofing tutorials .The price for the full package was.79$
”Jakeflakes“	From November 2020 to March ,2021 the threat actor listed a SIM swapping method that allows cashing out of compromised accounts .According to the threat actor ,the package included full debit card information and AT&T account details .The seller uses the following communication methods: Wickr) jakyflakes (and WhatsApp.(46769040617)
”Supreme“	In March ,2021 the reputable threat actor listed a SIM swapping method for 39$ and advertised a separate SIM swapping method for 38$ from October to December.2020
”CanadianSmoker12“	In March ,2021 the threat actor advertised a SIM swapping guide for.700$
”cashoutallday“	The threat actor first advertised a how-to method for SIM swapping any carrier in October ,2020 and has continued to update the advertisement .Our data indicates that cashoutallday has offered SIM swapping-related methods since at least July .2020 The listing is currently priced at.113$

Table 3: Threat actors advertising SIM swapping guides between June 2020 and June 2021 (Source: Recorded Future data)

Analysis of Purchased How-to Guides and Tutorials

Recorded Future analysts purchased multiple SIM swapping how-to guides and tutorials to identify overlaps in TTPs and any new methods being used to defeat and bypass MFA. These listings claimed to contain updated methods for defeating MFA in 2021 and current security measures being deployed by carriers to prevent both SIM swapping and social engineering attacks. Comparing the free how-to guide mentioned above, we identified the following relevant intelligence from the purchased how-to guides and tutorials. Below is a summary of recommendations and is not verbatim:

- **Carrier lookup and victim background check:** Select a specific carrier to target and a victim with a phone number with the desired area code. Open-source websites can be used to check and validate telecommunication information, such as freelookup[.]com and allageacodes[.]com. Once confirmed, purchase a physical SIM card from the matching carrier.
- **Purchase or acquire compromised PII data:** PII will be used to perform social engineering attacks on carrier representatives and convince them to activate the SIM card. The threat actors suggest acquiring and understanding previous billing information, as this is most relevant and will be used by the carrier when asking questions to validate your identity. One of the threat actors provided recommendations to acquire PII data on different dark web sources (with URLs).
- **Purchase a SIM card:** This will be used for activation, specifically telling the carrier to activate it (the new SIM card) with the same phone number used by the targeted victim.
- **Conduct test calls:** To perform an effective social engineering attack on a carrier, guides recommend first test-calling the targeted carrier to gather intelligence, specifically what kind of background questions they ask and what information is needed to activate the SIM card.

In addition to these steps, anonymity is essential. The guides recommend that a buyer use re-shipping services when mailing purchased SIM cards and using methods of payments that do not link to them, such as purchased gift cards or cryptocurrencies.

SIM Swapping on Instant Messaging Platforms

Our search for SIM swapping fraud on various instant messaging platforms in the Recorded Future Platform found 643 references over the past year. The majority of these listings refer to Telegram activities. It is worth noting that they are predominantly related to various carding activities and are not entirely SIM swapping oriented.

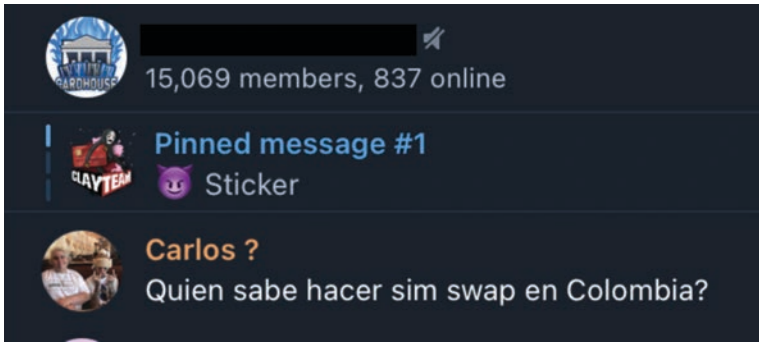


Figure 3: SIM swapping fraud on Latin American carding Telegram channels (Source: Telegram)

Although the number of Telegram sources that exclusively focus on SIM swapping fraud is significantly lower, it still shows that this attack vector is quite popular. Our analysis indicates that most channels consist of several to several dozen members and mostly discuss SIM swapping methods or request SIM swapping services. 2 of the most active Telegram channels we found that discuss and advertise SIM swapping were “Sims Swap OTP BOTS Service” and “Sim-Swap Tech”, with 3,557 and 561 members, respectively. We established that all of the Telegram channels and groups primarily target US telecom providers, with a lesser focus on British and other European mobile carriers. For example, Sims Swap OTP BOTS Service is currently offering both SIM swapping and SIM porting services against major US mobile providers. The price for SIM swapping service is $550 and for SIM porting is $300. The Telegram channel is also offering SIM swapping guides for cybercriminals for $850.

Mitigation

We recommend the following risk mitigation techniques against SIM swapping attacks:

- Set up a unique password or phrase that must be provided when calling a carrier's customer support, which many carriers provide as an option.
- In place of SMS MFA, use authenticator applications such as Google Authenticator, Duo Mobile, FreeOTP, Authy, or Microsoft Authenticator to securely access devices.
- Use one-time passwords or codes in addition to the primary password. Some services generate and display multiple one-time use codes that can later be used for authentication upon login. These codes can be printed out or written down and put in a safe place.
- Use hardware tokens based on Universal 2nd Factor (U2F) in place of SMS MFA.
- End-users must use a unique, strong password to protect their online mobile carrier account.

Outlook

SIM swapping remains a serious threat to carriers, social media organizations, and financial services, especially those involved in banking and cryptocurrency. It is a popular attack vector for many cybercriminals across the dark web and is tied to other fraudulent TTPs such as social engineering, insider threats, account takeovers, and money laundering. As mobile devices become more ubiquitous and more of our daily activities migrate from computers to mobile devices, SIM swapping, as an attack vector, is likely to continue to be used by threat actors to target global carriers in many countries, including the US, Canada, the United Kingdom, Spain, France, Germany, and Italy.

Based on reported intelligence, SIM swapping remains a popular attack vector among dark web cybercriminals who exclusively use forums as sources for advertising and requesting SIM swapping services, while dark web marketplaces and shops are primarily used for the sales and advertisements of SIM swapping tutorials and guides, as well as compromised PII data used in attacks. We believe that forums, marketplaces, and shops will remain popular and widely used sources for vendors and buyers to advertise, discuss, share, and purchase SIM swapping-related services for the foreseeable future and should be tracked closely.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.