INTSIGHTS

Democratizing Threat Intelligence™

The Cyber Threat Landscape of the Telecommunications Industry

Introduction

The telecommunications industry is a significant target for both cybercriminal and state-sponsored attacks. Cyberattacks on this industry can affect a wider range of victims beyond the industry itself because the use of telecommunications services by businesses and consumers alike is so pervasive. In particular, many businesses in other industries depend on telecommunications service providers to manage relationships with customers, or for their own phone and internet services. Breaches at telecommunications service providers can impact other companies' external internet traffic and customer relationships.

For example, the use of unauthorized access or malicious insiders at mobile service providers to enable SIM swapping attacks on their mobile service customers is a key objective of many criminal attacks in this industry. SIM swapping attacks can enable criminals to bypass the SMS-enabled two-factor authentication (2FA) of financial institutions and other businesses. 2FA is a key line of defense against credential compromises and the fraudulent transactions or other attacks that they enable.

In contrast, state-sponsored threat actors seek access to telecommunications service providers primarily in order to collect signals intelligence (SIGINT) on their customers, in the form of their phone and internet traffic. This SIGINT collection can target both enterprises and individual retail customers.

Telecommunications companies also possess personally identifiable information (PII) on their customers that can be useful to both criminals and state-sponsored cyber espionage groups. Criminals can use this PII for various fraudulent purposes, whereas government intelligence services can use it to support human intelligence (HUMINT) operations or facilitate the collection of more SIGINT.

SIM Swapping Attacks

Criminals buy and sell unauthorized access to the networks of telecommunications service providers in underground criminal communities, just as they do for many other industries. For example, IntSights coverage of underground criminal forums in December 2020 revealed that username "x_04x" was auctioning off administrative and VPN accesses to a leading telecommunications provider in Jordan and Saudi Arabia. The VPN accesses would enable further access to other remote services, such as SSH, FTP, and Citrx. The bidding for these accesses began at $2,000 each and increased in increments of $1,500 USD, with a "buy now" price of $3,000.

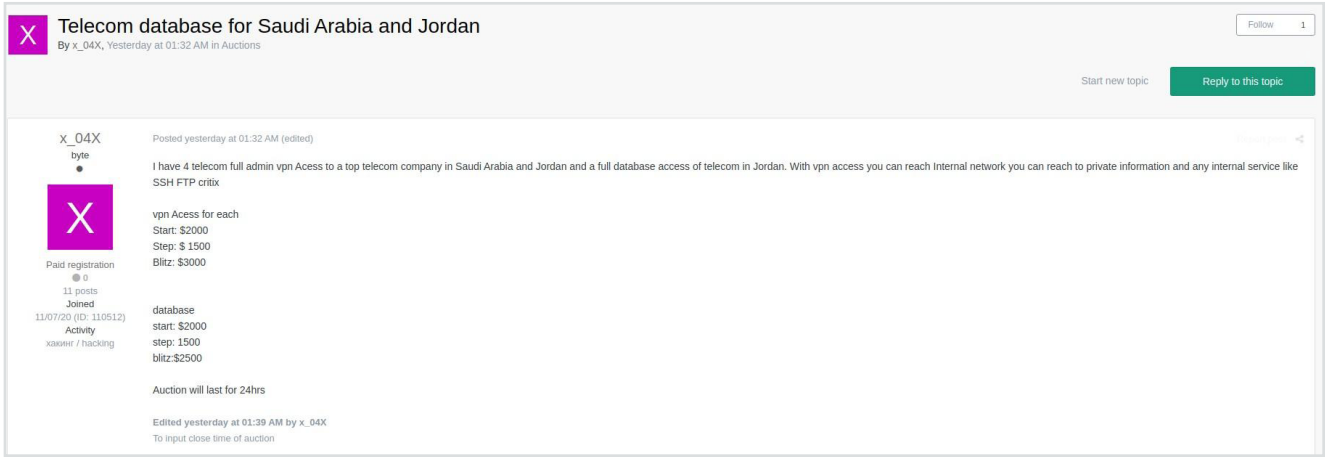

Figure 1: A cybercriminal auctions off administrative and VPN access to a telecommunications provider

Similarly, our coverage of underground criminal forums in November 2020 revealed that username "7h0rf1nn" offered to sell reverse shell access, with administrative privileges, to a US cable and telecommunications service provider for $1,950.

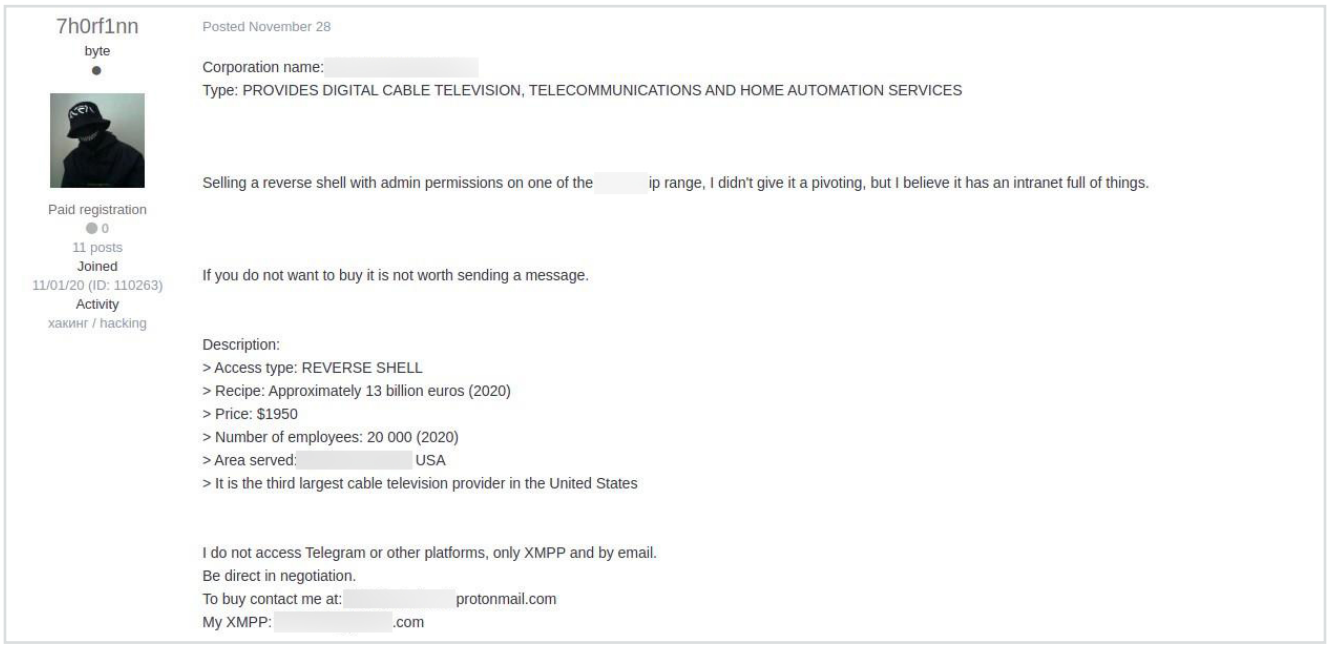

Figure 2: Reverse shell access with admin privileges to a major US telecom provider's network for sale on a cybercrime forum

Telecommunications companies are valuable enough targets that some criminals are willing to pay high prices for unauthorized access to their networks. For example, late 2020 IntSights coverage of underground criminal forums revealed that username "SHERIFF" offered to sell network access for what he described as the largest telecommunications service provider in Asia for 5 bitcoins (the equivalent of approximately $95,000 USD at that time).

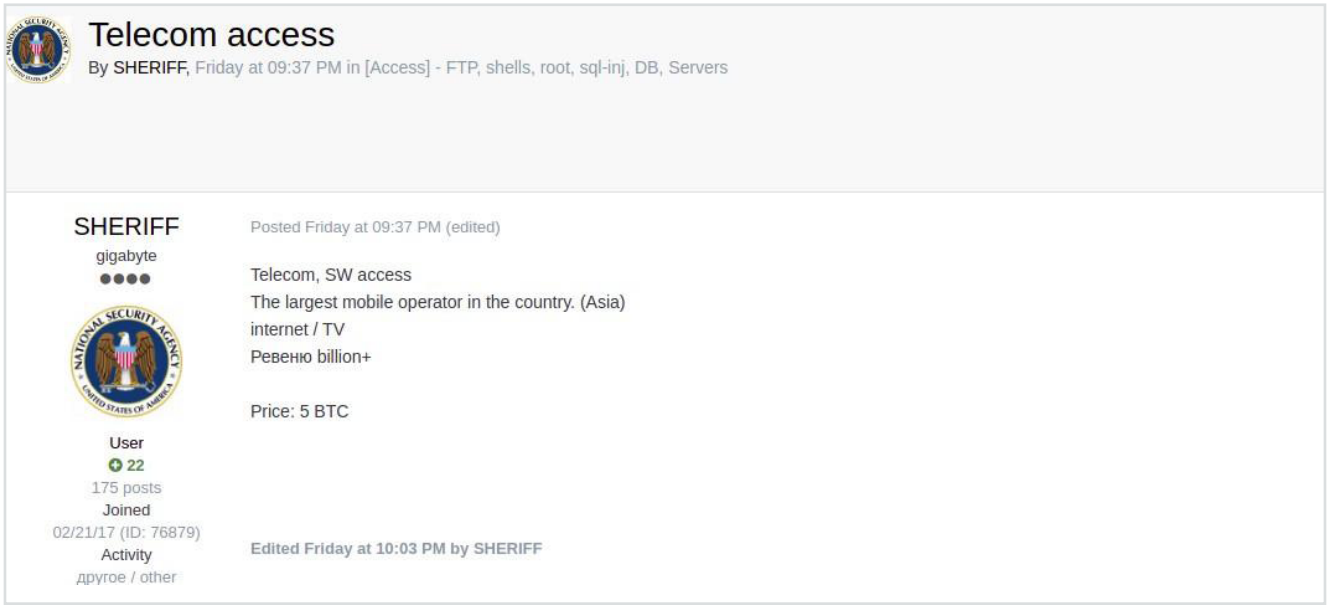

Figure 3: A user sells network access for the alleged largest mobile operator in Asia for 5 BTC

Shells are a common way for criminals to gain, maintain, and transfer unauthorized network access to telecommunications providers, as is the case for victims in other industries as well. RDP services are another common way for threat actors to gain, maintain, and transfer access to enterprise networks. For example, in October 2020, IntSights coverage of underground criminal forums revealed that username "true-knight" offered to sell RDP access to the network of a US telecommunications provider for 0.5 bitcoins (the equivalent of approximately $6,500 at the time).

Criminals also seek to exploit vulnerabilities in telecommunications provider networks. For example, late last year, a threat actor with the username "desugun" offered to sell an SQL injection (SQLi) vulnerability in the infrastructure of a telecommunications company.

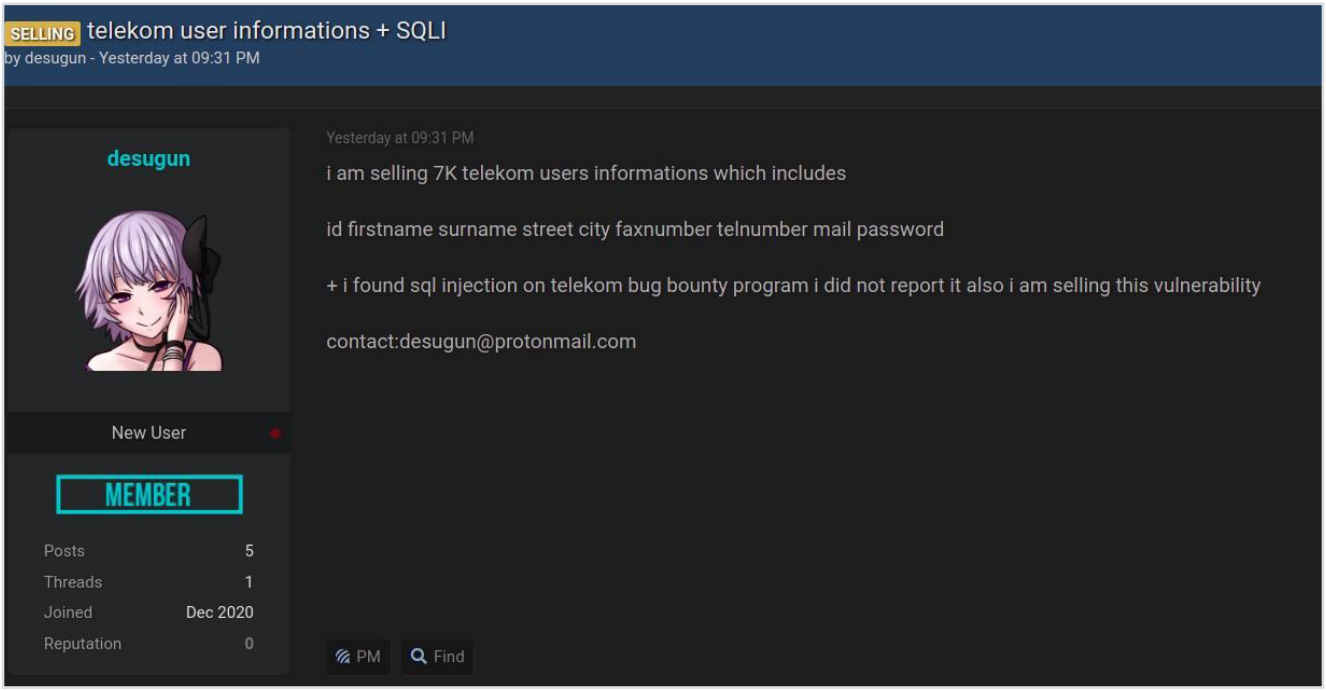

Figure 4: A threat actor offers an SQL injection (SQLi) vulnerability in the infrastructure of a telecommunications company for sale

SIM swapping attacks are the most important use case for unauthorized access to the networks of mobile service providers. These attacks enable criminals to defeat the SMS-based 2FA that defends so many accounts, particularly online banking accounts. These attacks reroute SMS-based 2FA messages containing codes meant for victims to SIM cards in the possession of attackers. The attackers can thus use those 2FA codes to gain unauthorized access to online banking or other accounts in order to conduct fraudulent transactions, or for other malicious purposes.

Tutorials for SIM swapping attack techniques are readily available on criminal forums. For example, IntSights discovered that username "salammoleikum1" posted a tutorial on various technical methods for cloning SIM cards. Similarly, username "19911" offered to sell a tutorial on SIM swapping attacks for $37 in October 2020. He specifically emphasized the value of SIM swapping as a way to defeat 2FA, particularly for online bank accounts.

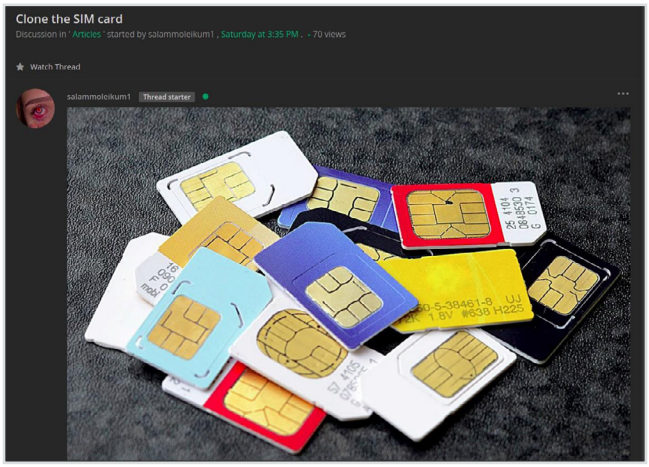

Figure 5: A hacker offers tutorials on cloning SIM cards

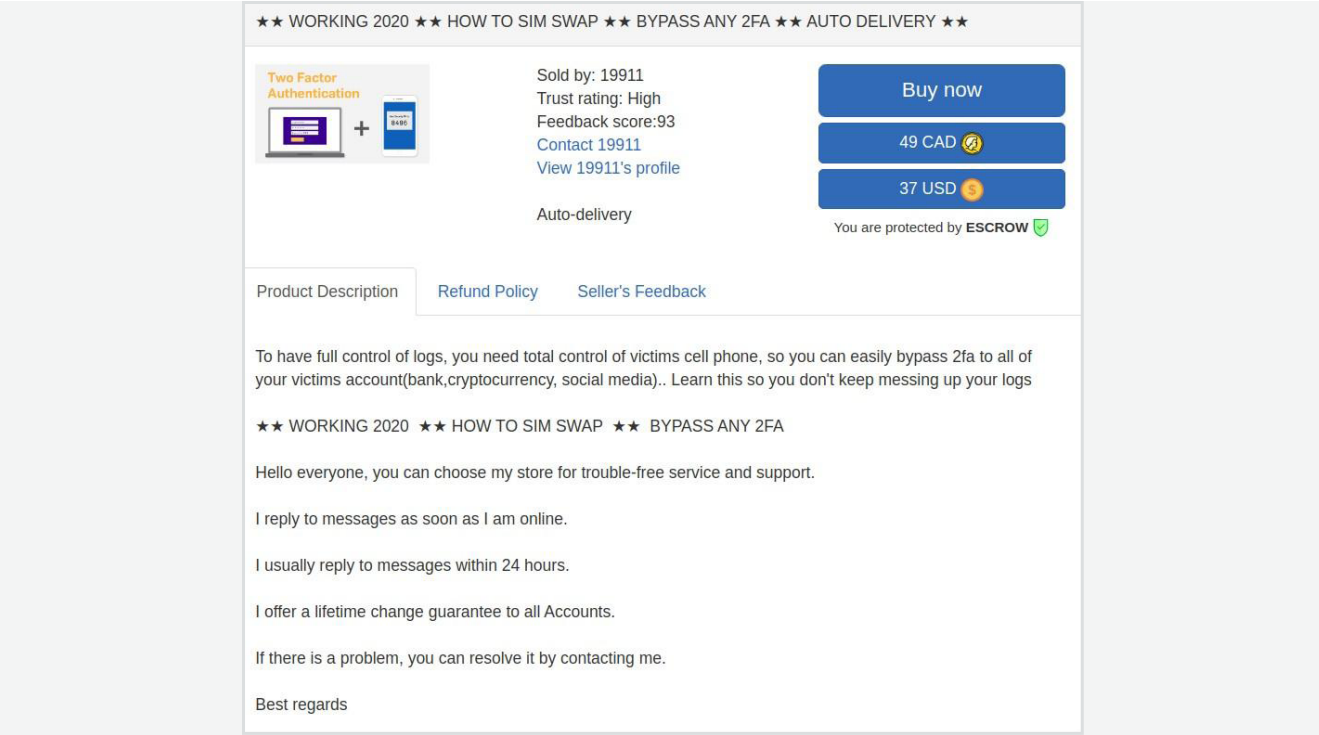

Figure 6: A cybercriminal lists a tutorial on SIM swapping attacks for $37

The intended purpose of many of the above-mentioned sales of unauthorized network access to telecommunications providers is probably to enable SIM swapping attacks, although the criminal vendors may not explicitly advertise this particular use case. However, username "r41s3r" specifically mentioned SIM swapping attacks last October as the intended application of his sale of access to a Fortune 500 telecommunications company. His asking price for web shell access to one machine at this company was $2,500.

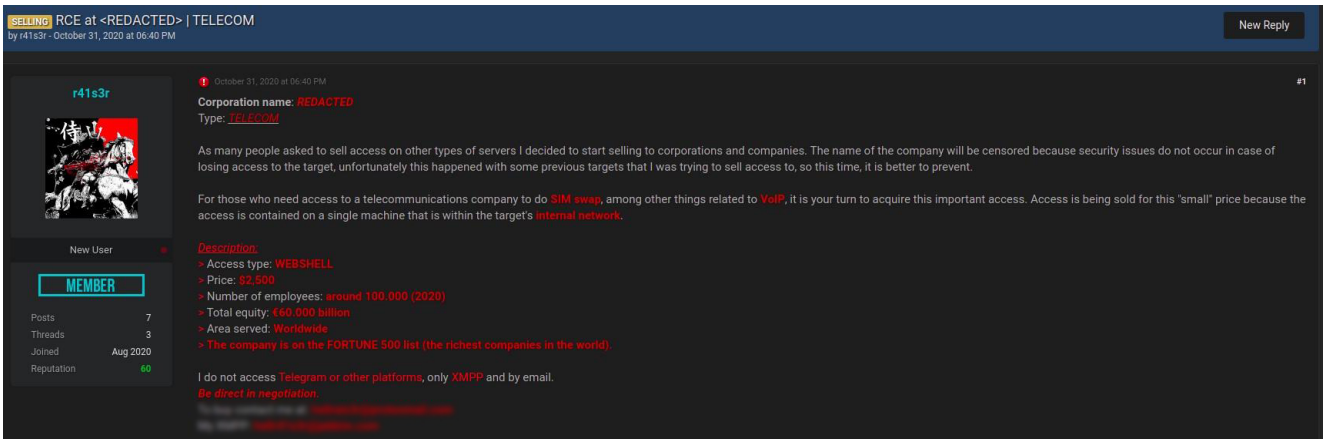

Figure 7: A threat actor sells access to a Fortune 500 telecom company's network for the purpose of carrying out a SIM swapping attack

SIM swapping attacks are lucrative enough that some criminals have established dedicated SIM swapping businesses that charge other criminals for their services. For example, a Russian-speaking criminal named "Panther" who provided SIM swapping services at significant prices, ranging from $190 to $230 per target.

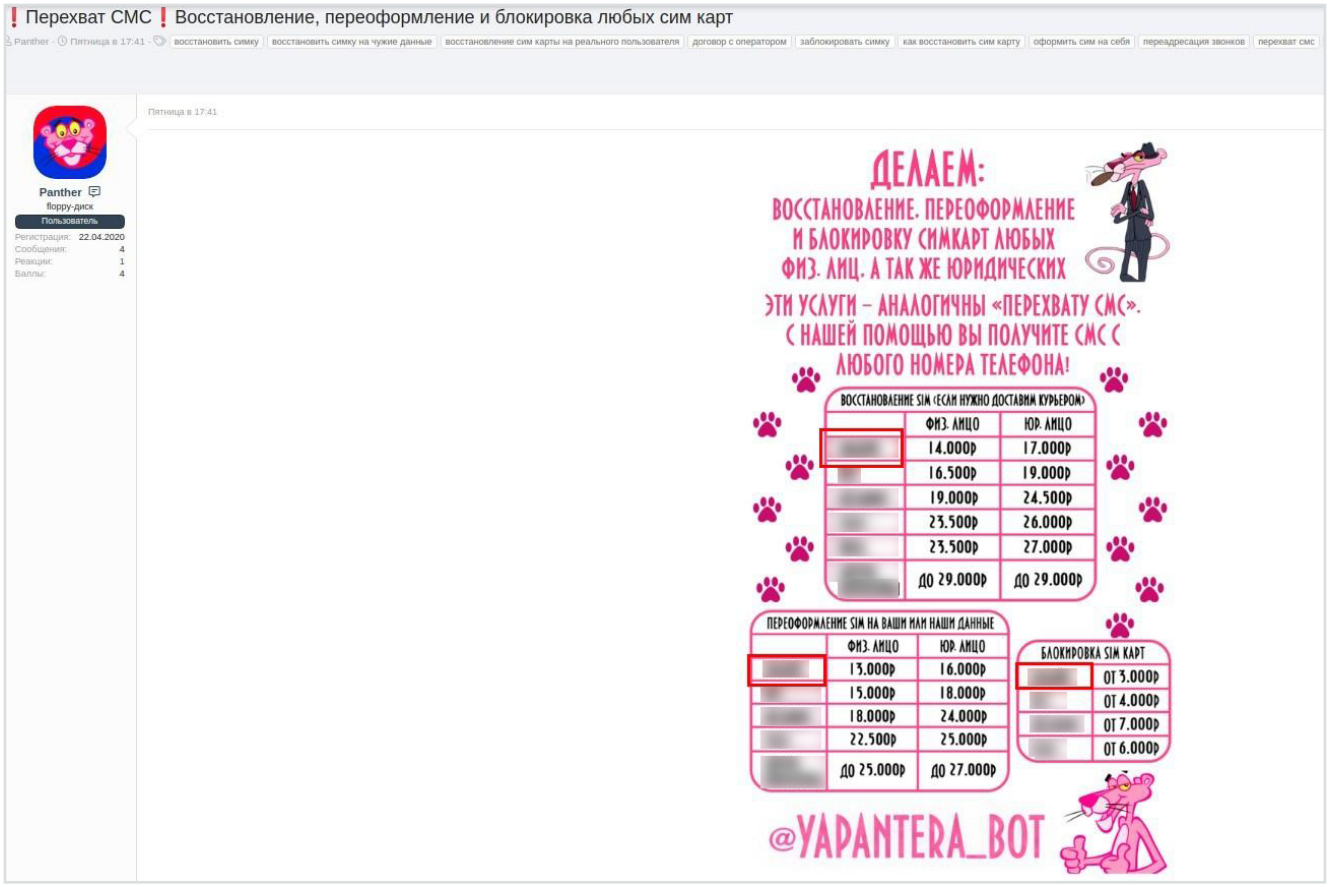

Figure 8: A Russian threat actor offers SIM swapping services ranging from $190-$230 depending on the target

Insider threats are another way for criminals to conduct SIM swapping attacks. Malicious employees of telecommunications companies with the appropriate access can reassign targeted phone numbers to attackers' SIM cards, enabling them to receive SMS-based 2FA codes meant for victims. This insider access is valuable enough that underground criminal forum user "Gonemist" has developed a specialized insider threat service, enabling SIM swapping attacks on the customers of Canadian mobile service providers via malicious employees at those companies. Gonemist and his network of malicious insiders work for a certain percentage of what their customers earn from these attacks.

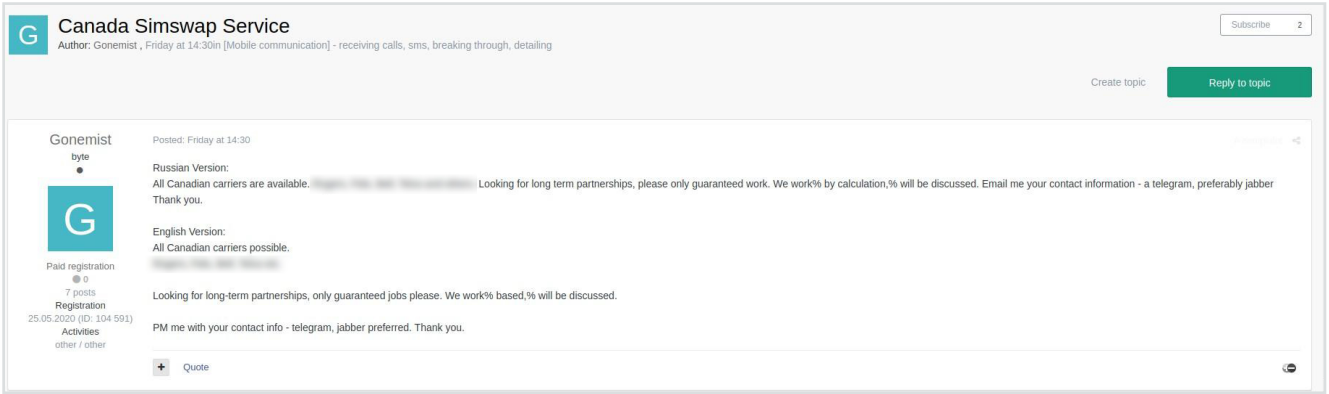

Figure 9: A cybercriminal offers SIM swapping services for a percentage of what the customers earn from their subsequent attacks

While many SIM swapping operators charge on a per-target basis, Gonemist and many others, such as username "scanproof," collect a certain percentage of the proceeds of whatever attacks they enable for their customers via SIM swapping. For example, scanproof, who targets Ukrainian mobile numbers, negotiates a share of 10-30 percent of the revenue that these SIM swapping attacks generate.

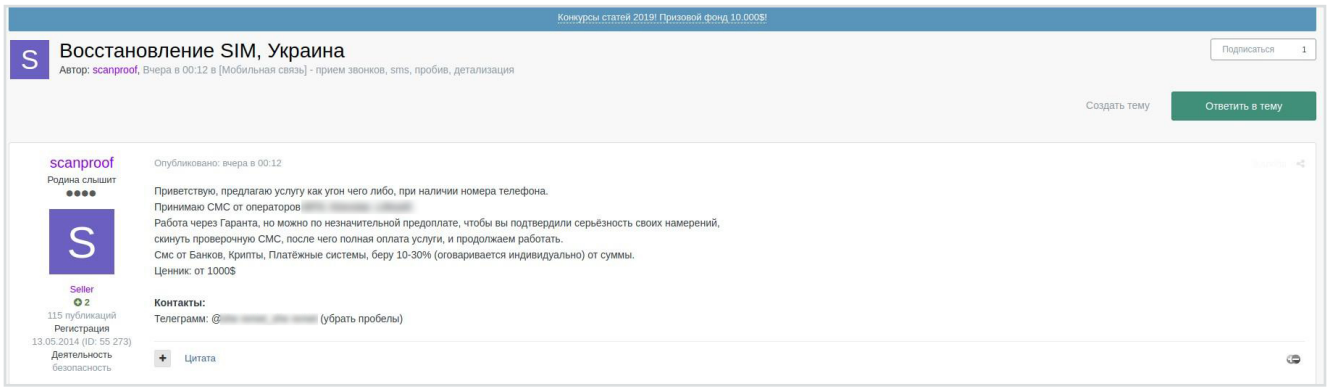

Figure 10: One threat actor negotiates his share of the revenue generated by SIM swapping attacks

IntSights security researchers also identified an English-speaking Telegram user (@Whitecollarb) targeting US mobile service providers. This user charges $300 per phone number for SIM swapping attacks, which take approximately 30-45 minutes to complete. IntSights researchers tested this individual's access and confirmed that he can successfully enable SIM swapping attacks.

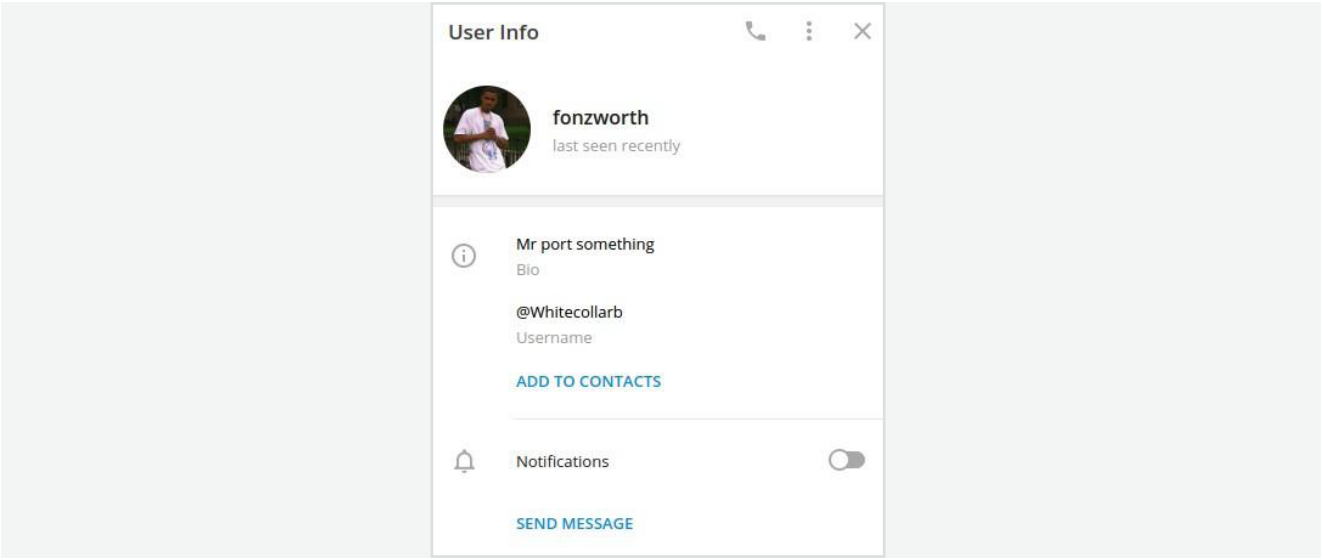

Figure 11: A Telegram user who charges $300 per phone number for a SIM swapping attack. IntSights confirmed that his access is legitimate.

The criminals who use these forums to advertise their SIM swapping services also use them to recruit malicious employees of telecommunications companies. For example, IntSights coverage of underground forums revealed that, in February 2020, the Russian-speaking criminal "KHAN service" sought to recruit malicious insiders at telecommunications providers in Russia and other former Soviet republics, offering them high levels of compensation.

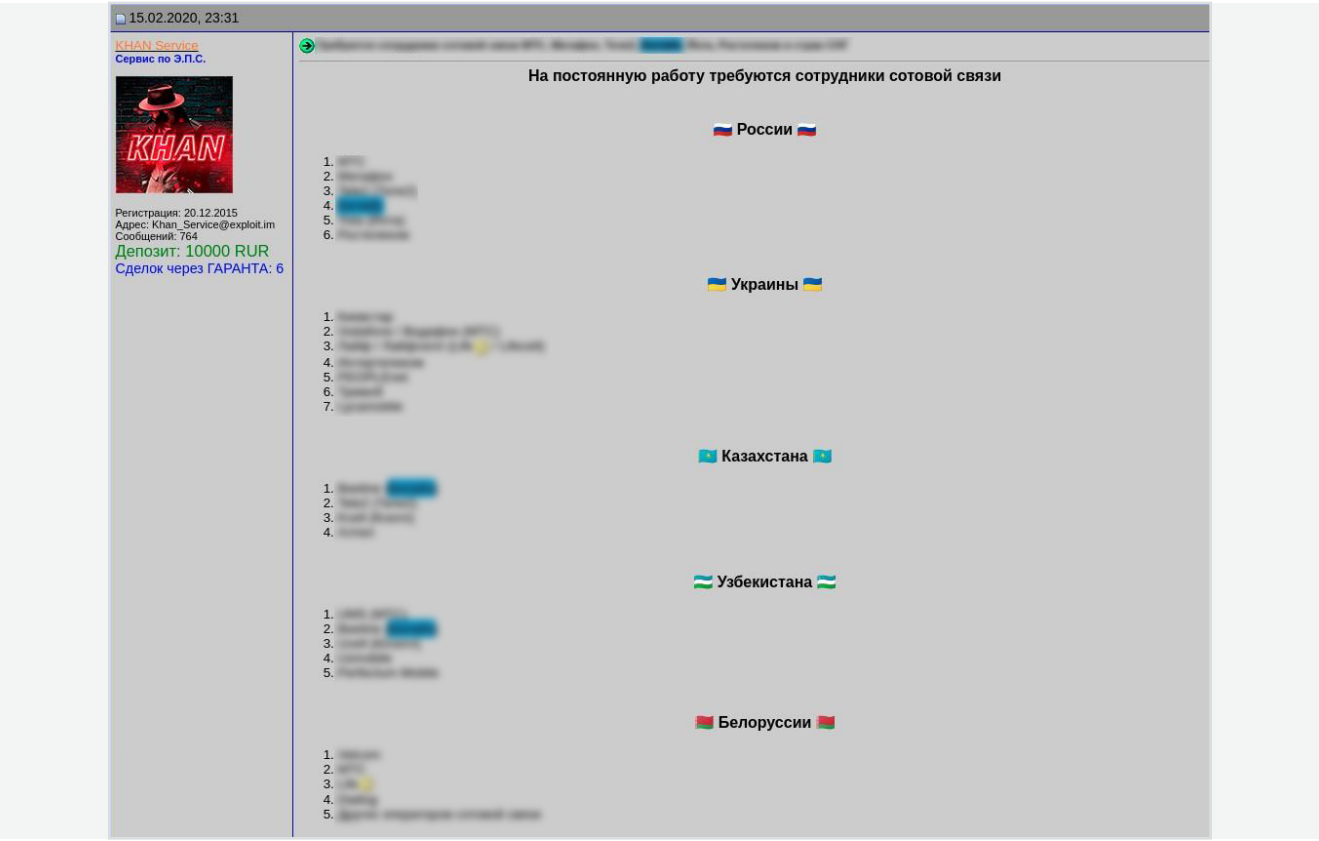

Figure 12: A threat actor recruits insiders at telecom providers in Russia and other former Soviet states

Criminals and State-Sponsored Actors Collect Customer PII

Telecommunications subscriber records are one of many sources of consumer PII that criminals can use for identity theft, other forms of fraud, or social engineering attacks. For example, telecommunications providers may collect PII data points, such as dates of birth and US Social Security numbers, that criminals can use to apply for fraudulent lines of credit in victims' names, or in other forms of identity theft. The combination of customer contact information with other personal details can also facilitate social engineering attacks on customers. The attackers can contact victims at their now-exposed phone numbers or email addresses and use those other PII details to give themselves credibility as fake customer service representatives.

Telecommunications customer PII is also useful to state-sponsored threat actors for a variety of intelligence purposes. They can use it to identify the phone numbers and email addresses of persons of interest. They can then: collect SIGINT by targeting those phone numbers and email addresses for technical monitoring of their communications; target victims at those phone numbers or email addresses in social engineering attacks to install malware on their phones or computers; or contact targets directly for potential development or recruitment as HUMINT sources. Government intelligence agencies can also ingest bulk PII into searchable databases for future queries for a variety of purposes, such as background checks, screenings of visa applicants and foreign travelers, and the identification of prospective targets for development and recruitment as HUMINT sources.

Compromised telecommunications customer data routinely appears for sale in underground criminal forums. For example, last October, IntSights found username "GoldApple" offering to sell 7 million subscriber records from a Turkish ISP. The records included names, phone numbers, email addresses, and street addresses.

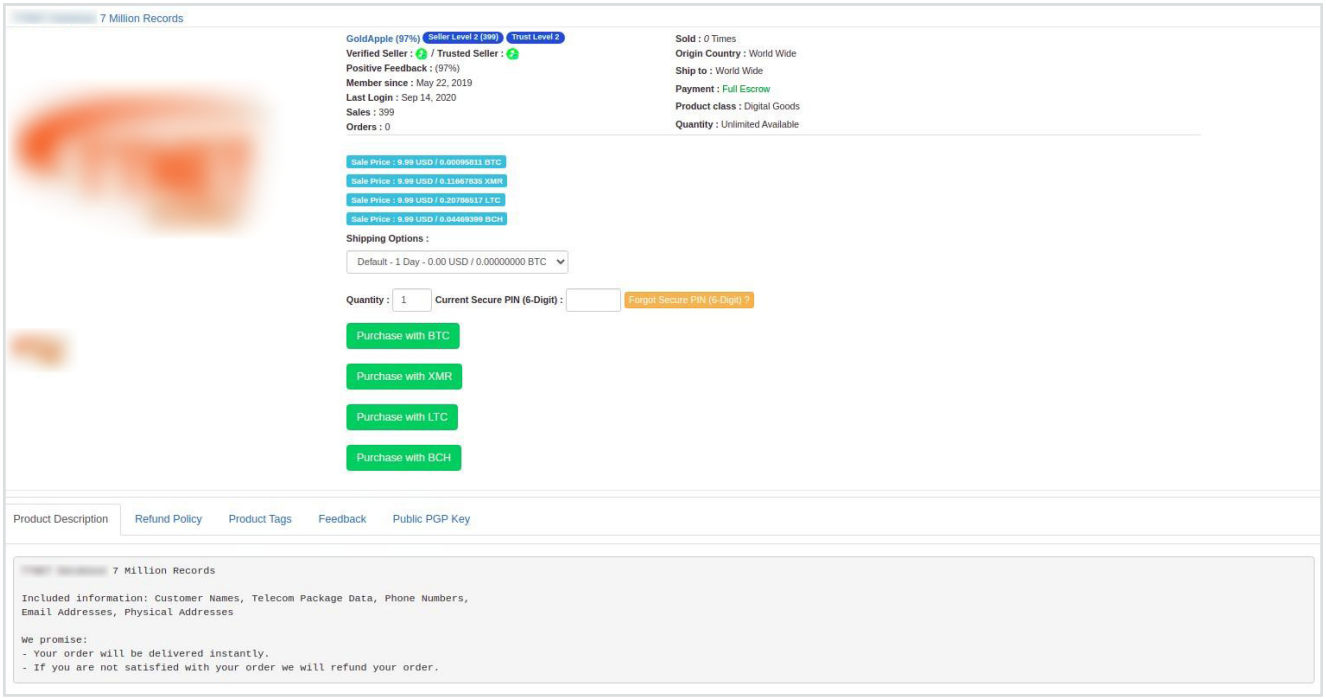

Figure 13: Over 7 million subscriber records from a Turkish ISP for sale

Other PII data points in telecommunications customer data may include national ID card numbers. For example, earlier this year username "t3rra" offered to sell a 2020 Pakistani telecommunications database of 176 million subscriber records that included national ID numbers, along with names, street addresses, SIM card numbers, and other details.

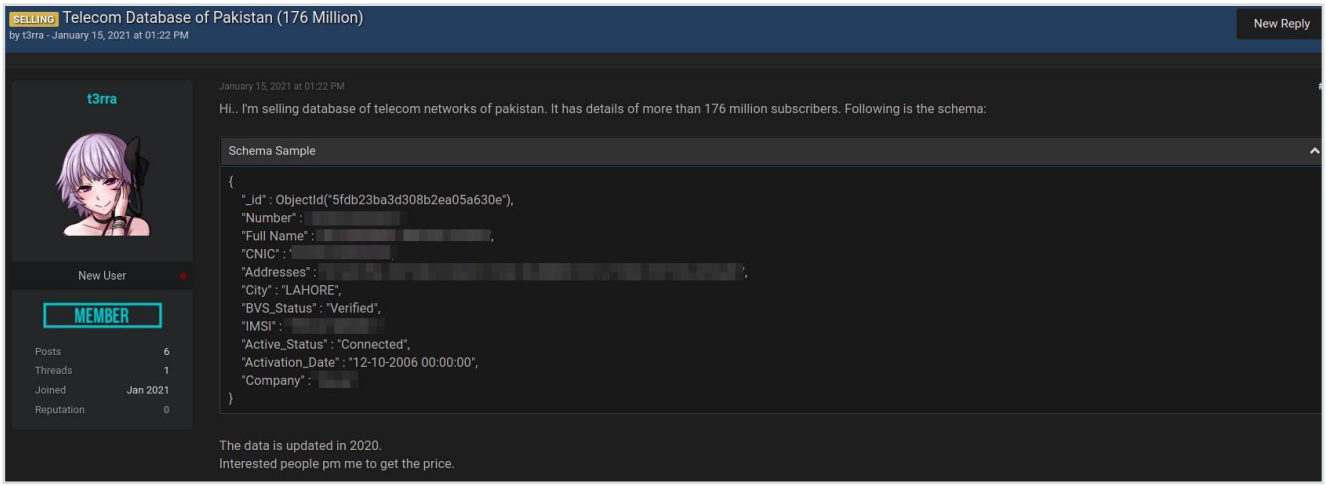

Figure 14: A threat actor sells a Pakistani telecom database of 176 million subscriber records that included national ID numbers

The billing details of telecommunications customers can also be useful for fraud. For example, in January 2021, IntSights coverage of criminal forums revealed that username "Leningrad" was selling a database from a Spanish telecommunications company. The database included international bank account numbers (IBANs) and photos or scans of customer identity documents, which could facilitate fraudulent bank transfers or identity theft, respectively, as well as documents about money transfers.

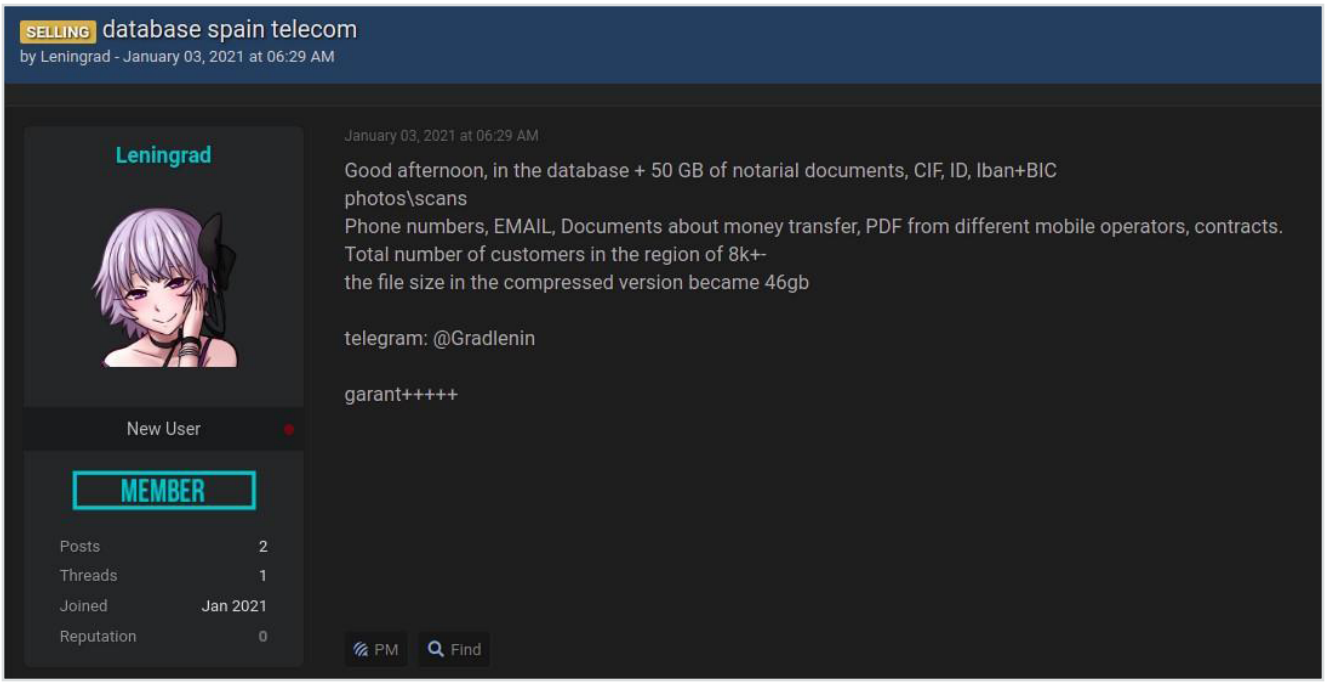

Figure 15: Database from a Spanish telecom company for sale, including bank account numbers and images of customer documents

The web applications telecommunications companies offer to customers for bill payment can also become targets for criminals. IntSights coverage of criminal forums revealed that, in October 2020, username "Medusa23" offered to sell a zero-day vulnerability in the web applications of a Kuwaiti telecommunications service provider with a presence in multiple Middle Eastern markets, as well as five other telecommunications providers in the region. The actor was also offering to sell web shell access to Zain's domain and a database of information on 450,000 customers, including credentials.

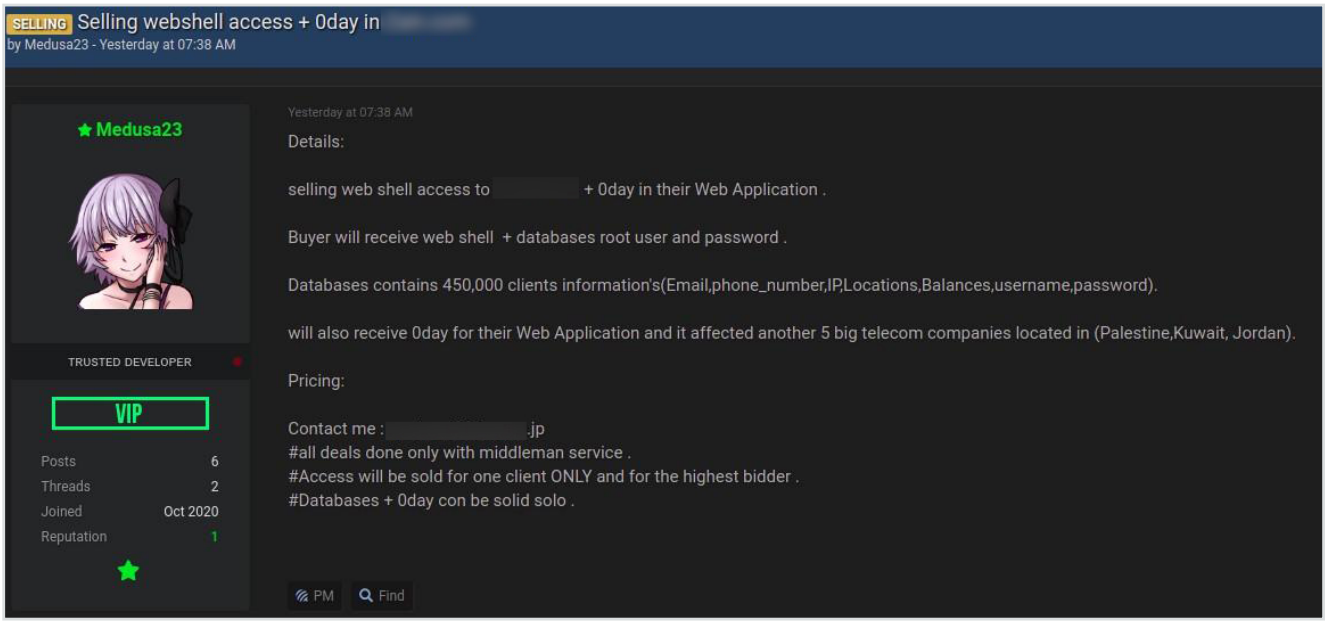

Figure 16: A threat actor sells a zero-day vulnerability to a Kuwaiti telecom company, among others

Customers may be the primary target of interest for most criminal attacks on telecommunications companies, but employees and their data may become targets as well. For example, IntSights found that username "3lv4n" offered to sell a database of a major US mobile phone provider's employee information. This database could facilitate social engineering attacks on the company by revealing employee contact information and responsibilities.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Email Address	Display Name	Given Name	Surname	Middle Na	Title	Company	Business Street Address	Business Postal Co	Business	Business	Business	Cellular N	Office Nu	Office Nu	Primary P	Business	Business
[redacted]	[redacted]	[redacted]	[redacted]		Sr Engine	[redacted]	[redacted]	98021	WA	Bothell	USA	[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Expert, T	[redacted]	[redacted]	83642	ID	Meridian		[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		General C	[redacted]									Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Develope	[redacted]	[redacted]	98006	WA	Bellevue	USA		[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Retail Sal	[redacted]	[redacted]	7012	NJ	Clifton					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Analyst, F	[redacted]	[redacted]	98006	WA	Bellevue		[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		TPRi - Reb	[redacted]			TX						Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		CW - Con	[redacted]	[redacted]	98006	WA	Bellevue					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		TPRi - Prir	[redacted]									111-111-1111		
[redacted]	[redacted]	[redacted]	[redacted]		Customer	[redacted]	[redacted]	98006	WA	Bellevue	USA	[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Expert, A	[redacted]	[redacted]	65803	MO	Springfield					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		General C	[redacted]									Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]			[redacted]					Ireland						
[redacted]	[redacted]	[redacted]	[redacted]		Retail Sal	[redacted]	[redacted]	60639	IL	Chicago					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]			[redacted]											
[redacted]	[redacted]	[redacted]	[redacted]		Director,	[redacted]	[redacted]	30346	GA	Atlanta	USA		[redacted]	[redacted]	813-351-4178		
[redacted]	[redacted]	[redacted]	[redacted]		Retail Sal	[redacted]	[redacted]	89102	NV	Las Vegas					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Expert, A	[redacted]	[redacted]	98226	WA	Bellingham					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		TPRi - Reb	[redacted]			CA						Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		TPRi - Mar	[redacted]			NY						Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Group Pro	[redacted]	[redacted]	98006	WA	Bellevue		[redacted]			Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		M-Manag	[redacted]	[redacted]	80246	CO	Glendale		[redacted]			Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Account M	[redacted]	[redacted]	7054	NJ	Parsippany					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Analyst, B	[redacted]	[redacted]	98006	WA	Bellevue					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Retail Ass	[redacted]	[redacted]	15222	PA	Pittsburgh			[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Solution A	[redacted]									Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Intern, Un	[redacted]	[redacted]	98006	WA	Bellevue					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Manager,	[redacted]	[redacted]	98006	WA	Bellevue					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Sr Analyst	[redacted]	[redacted]	98021	WA	Bothell					Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Assoc Tec	[redacted]	[redacted]	77032	TX	Houston		[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		District Sa	[redacted]	[redacted]	77046	TX	Houston	USA	[redacted]	[redacted]	[redacted]	813-348-3118		
[redacted]	[redacted]	[redacted]	[redacted]		Sr Manag	[redacted]	[redacted]	98006	WA	Bellevue		[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Manager,	[redacted]	[redacted]	98065	WA	Snoqualmie		[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		Service Pa	[redacted]	[redacted]	99999	GA	Various	USA	[redacted]	[redacted]	[redacted]	Reserved	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]		TPRi - Reb	[redacted]			WA						Reserved	[redacted]	

Figure 17: A threat actor sells a major mobile provider's employee database, which could facilitate social engineering attacks on the company

Similarly, in November 2019, IntSights security researchers identified a Russian-speaking criminal known as "Olegik," who offered to sell a partial database of information on the employees of the Russian telecommunications company Beeline. The database included the employees' personal phone numbers and social media accounts.

State-Sponsored Threat Actors Target Telecommunications Providers for Cyber Espionage

SIGINT is one of the primary forms of intelligence that government intelligence services collect in order to inform political, military, economic, and other decision-making processes in their governments, and otherwise uphold and defend their countries' interests. The state-sponsored actors that have been most active in targeting telecommunications service providers are also the most active state sponsors of cyber espionage in general, such as Russia, China, and Iran.

Digital copies of phone and internet communications are the most common and typical forms of SIGINT. Breaches of telecommunications service providers are one of several ways for intelligence services to collect this SIGINT. In such incidents, state-sponsored threat actors breach telecommunications provider networks and move laterally until they have unauthorized access to infrastructure that enables them to record voice calls, collect copies of SMS, or gather PCAPs of customer network traffic.

For example, the Chinese APT41 developed and deployed the proprietary malware MESSAGETAP to collect SMS traffic from specific phone and SIM card numbers, or text messages containing specific keywords. In 2019, APT41 deployed this malware during a breach of a mobile service provider at a cluster of Linux servers functioning as Short Message Service Centers (SMSCs) for SMS traffic. The list of keywords targeted for SMS collection reflected the collection requirements of Chinese intelligence services, as they indicated an interest in groups and individuals hostile to or otherwise of interest to the Chinese government. During this same breach, APT41 also targeted the call detail records (CDRs) of high-ranking individuals of interest to the Chinese government. CDRs document the date, time, duration, source, and destination of voice calls, as well as cell towers that the callers used. Cell tower details can enable geolocation of callers.

The Chinese Operation Soft Cell has targeted telecommunications providers in particular, including their CDRs. This campaign's tactics, techniques, and procedures (TTPs) were consistent with those of the Chinese APT10. The actors gained initial access by exploiting a vulnerable, public-facing server and installing the China Chopper web shell, from which they expanded their access. China Chopper is a common hallmark of Chinese attacks. They moved laterally by using the Mimikatz credential harvesting tool and abusing Windows Management Instrumentation (WMI). They eventually gained access to the Domain Controller and created their own accounts with high privileges. They used the Trojan PoisonIvy, which is also a hallmark of Chinese attacks. They compressed compromised data, such as CDRs, into encrypted archives for exfiltration via separate web shells.

In 2020, The Chinese cyber espionage group Mikroceen also targeted a telecommunications service provider in Central Asia, along with organizations in other industries. As in Operation Soft Cell, the attackers used the credential harvesting tool Mimikatz to expand their access and abused WMI to move laterally within the compromised network. They sometimes demonstrated weak operational security, including the use of Chinese infrastructure in their attacks. They used the Gh0st RAT Trojan, which Chinese cyber espionage groups have used in the past, and other aspects of the attack bore code similarities to the previously identified Vicious Panda campaign from China. Central Asia is of high importance to the Chinese government for a variety of reasons, including oil and gas reserves for the Chinese economy, infrastructure connecting China to the Middle East and Europe, and tensions with the Uighur minority in Xinjiang, an autonomous region of China.

Chinese SIGINT and CDR collection likely cover many different types of political, military, and economic targets. Ethnic tensions with the Uighurs are primarily a domestic issue but have nonetheless become so important to Chinese officials that they drive Chinese cyber espionage attacks against telecommunications providers in foreign countries where Uighurs are likely to travel.

The ability to monitor travelers, including one's own citizens traveling overseas, is likely one of multiple reasons for the Iranian APT39's targeting of foreign telecommunications providers, along with foreign airlines, hotels, and other travel businesses. APT39 has targeted primarily other Middle Eastern countries, along with the US. The US is a top target of Iranian cyber espionage due to long-standing tensions between the two countries, including US support for Iranian dissidents seeking regime change. Many Iranian dissidents live in the US or elsewhere outside Iran. APT39 uses malicious email links and attachments, often in conjunction with domains that spoof legitimate organizations and services, to infect recipients with its POWBAT backdoor. APT39 has also targeted Outlook Web Access (OWA) servers and exploited vulnerable web servers, possibly via SQL injection (SQLi) attacks, to install its own web shells. APT39 often abuses the RDP protocol for persistence and lateral movement.

In another example of the Iranian targeting of telecommunications providers, the Iranian cyber espionage group Greenbug targeted South Asian telecommunications providers in South Asia in 2019 and 2020. The group used email messages with malicious links to gain initial access. It may have abused multiple legitimate red team or penetration testing tools, such as Covenant, Cobalt Strike, and Metasploit, as well as the legitimate administrative tools Plink and Bitvise, in order to reduce the likelihood of detection. It repeatedly used PowerShell commands to download and execute payloads and otherwise expand its access. Filenames from these attacks suggest the targeting of Pakistan, which has a border with Iran and nuclear weapons status that Iran also seeks.

State-sponsored Russian cyber espionage groups and their attacks are generally less transparent and obvious than those of their Chinese and Iranian counterparts. State-sponsored Russian attacks are typically harder to detect and harder to attribute to state-sponsored Russian actors, as they typically make much greater efforts to reduce the likelihood of detection, cover their tracks, and conceal their identities, locations, and affiliations. It is thus harder to gain insights into the state-sponsored Russian targeting of telecommunications service providers for cyber espionage purposes.

Indeed, one state-sponsored Russian attack on telecommunications service providers was specifically for the purpose of obscuring attacks from security researchers and foreign governments. The Russian cyber espionage group Turla specifically targeted satellite internet service providers (ISPs) in order to provide cover and protection behind which to hide its own command & control (C2) infrastructure.

The SolarWinds supply chain breaches of the US Government and other US organizations, which US Government officials attributed to the Russian APT29, raised the prospect of widespread compromises within the US telecommunications industry. All of the top 10 US telecommunications providers were SolarWinds customers. The National Telecommunications and Information Administration, which is part of the US Department of Commerce, was one of the many federal government victims of this supply chain attack. Its compromise could indicate more specific interest in the targeting of the US telecommunications industry and US telecommunications policy.

State-sponsored threat actors may dominate the market for geopolitical and other high-value targets, but criminals can target such individuals as well. Late last year, IntSights found username "Ahmose" offering to sell mobile subscriber databases from more than a dozen Arab countries. The criminal vendor claimed that these databases included information on members of royal families, government ministers, military leaders, petroleum engineers, and terrorists.

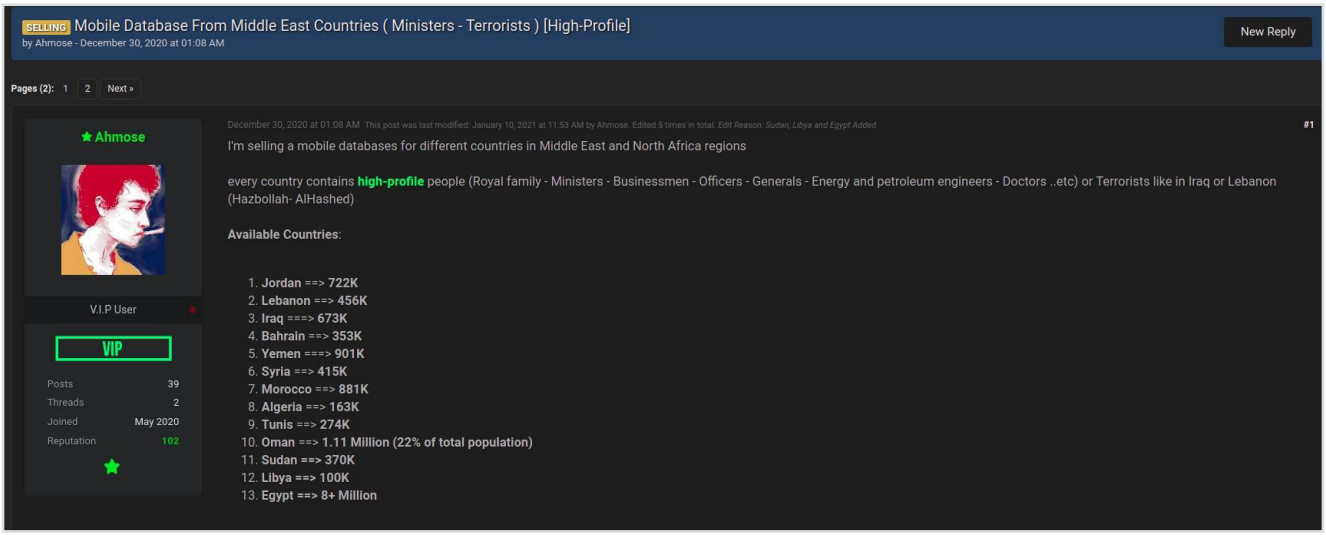

Figure 18: A cybercriminal offers mobile subscriber databases for sale from over a dozen Arab countries, including information on royal families, government officials, and other high-profile targets

Conclusion and Recommendations

Breaches at telecommunications companies can have a significant impact on their retail and enterprise customers, such as the compromise of phone and internet traffic. End-to-end encryption and the use of VPNs can mitigate the risks of exposure to state-sponsored SIGINT collection via compromised ISPs. The reliance on mobile service providers for SMS-based 2FA leaves it exposed to the risk of criminal SIM swapping attacks that can defeat this key line of defense. If and when feasible, enterprise and individual users should adopt mobile authentication apps for 2FA in order to avoid this risk.

Telecommunications companies can take steps to mitigate the top risks to their industry. Mobile service providers should establish and maintain insider threat programs, as malicious insiders are a leading way for criminals to gain the access that they need to conduct SIM swapping attacks. Telecommunications companies should also invest in advanced threat detection and prioritize threat intelligence coverage of state-sponsored cyber espionage, as the attacks of foreign intelligence services may be harder for their security teams to detect. The value of telecommunications subscriber PII to both criminals and cyber espionage groups warrants special measures to protect it, such as encryption or network segmentation.

External threat intelligence can help security teams identify and validate emerging cyber threats targeting their organizations before they evolve into attacks. Proactive threat detection enables practitioners to react more quickly to threats and take measures necessary to ensure the security of their organization's network and digital assets. Telecommunications providers in particular can benefit from a comprehensive external threat intelligence solution, as they face an onslaught of rapidly evolving cyberattacks that threaten their employees, end users, partners, and business reputation.

About IntSights

IntSights enables organizations of any type or size to gain the full benefits of external threat intelligence, no matter the size or sophistication of their threat intelligence programs. Unlike any other solution on the market, IntSights takes the complexity out of threat intelligence and delivers instant value without the heavy lift or sizable resource allocation that traditional threat intelligence solutions require. Designed to scale, IntSights is for any company, and frictionless integration of our real-time cyber threat intelligence with existing security infrastructure allows enterprises to maximize return on investment.

IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit intsights.com or connect with us on LinkedIn, Twitter, and Facebook.