Toll Fraud, International Revenue Share Fraud and More:

How Criminals Monetise Hacked Cellphones and IoT Devices for Telecom Fraud

Written by:

Craig Gibson, Principal Threat Defense Architect of Trend Micro's Forward-Looking Threat Research (FTR) Team, and Europol

EUROPOL DISCLAIMER

More information on Europol is available on the internet:

Website: www.europol.europa.eu
Facebook: www.facebook.com/Europol
Twitter: @Europol
YouTube: www.youtube/EUROPOLtube

TREND MICRO LEGAL DISCLAIMER

Introduction

Telecommunications fraud is by no means a new crime. It encompasses a wide range of modi operandi, each of which takes multiple forms and many of which have existed for over a decade. Until recently, many of these crimes had not featured significantly on the radar of law enforcement. However, developments in technology, the industry, and criminal capabilities have turned telecommunications fraud into a multi-billion euro criminal industry.

Two major types of telecommunications fraud can be identified: subscription fraud and toll fraud. Subscription fraud is the use of carrier business process compromise (BPC) by an attacker to pose as a legitimate customer and gain access to one or more customer accounts that can be abused. Toll fraud, which is the more damaging, involves exploiting how money moves within the global telecom network. Typically, the amount of money stolen in each event is much higher, often going beyond EUR 1 million. Prosecuting this kind of event is usually more difficult given the cross-border nature of the crime.

These crimes have a significant impact on customers, including the loss of all connectivity due to being blocked at the carrier (or telecom infrastructure provider) level. Customers can also receive enormous bills, be mistakenly blocked by their own carriers, or be blocked globally by all carriers. During these crimes, the criminals pose as real customers and carriers. The customers may, in some cases, experience prolonged outages because they're unable to persuade the carriers involved that they are actually the victims and not the perpetrators.

Inter-carrier trust and how it gives rise to fraud

International revenue share fraud (IRSF) is a type of crime relying on the "gentleman's agreement" between telecom carriers, in which they have an unspoken pact not to hack or attack one another. This global agreement is called *inter-carrier trust*, similar to the relationship banks have with one another. When a miscreant entity exploits that trust, it can manipulate the flow of traffic — money in the case of banks, expensive calls in the case of telecom carriers — to perform activities such as fraud and money laundering. As for miscreant carriers who have joined the inter-carrier trust community, they can commit traffic redirection abuses, including wiretapping (to record conversations and search for credit card numbers and passwords, for example) and injection of malware. These often include IRSF methods.

IRSF is attractive to criminals because of the inherently low risk of the attack: it can be performed at a distance and the received money comes from redirecting the inter-carrier billing for expensive telecom traffic. This redirected money moves from the victim's carrier to the attacker's carrier in such a way that it can be "withdrawn" quickly in the form of payment from a complicit carrier.

Since these frauds can be executed against the internet of things (IoT), the sheer number of devices that can be possibly involved has to be considered. Many fraud cases may be more profitable and more difficult to detect when performed against, say, refrigerators or traffic lights. If fraud originates from IoT-critical infrastructures, such as in smart cities, and are consequently blocked as fraud, the IoT-enabled deployments would go silent. Therefore, cities and organisations that are using telecoms in operations should improve their security and fraud prevention posture to ensure the continuity of services.

The popularity of IRSF in particular and telecom fraud in general has been steadily growing. According to the Communications Fraud Control Association (CFCA), some telecom carriers believe that as much as 18% of their revenue may be composed of traffic generated by organised crime. The CFCA also quantifies the current impact of telecom fraud, including premium-rate service and theft, to have reached nearly USD 27 billion. However, many carriers do not report fraud losses for fear of being regulated, with the subsequent inconvenience and costs often passed on to the customer. For this reason, many carriers suffer in relative silence and the actual impact of this type of crime is likely to be much higher than the figure quoted above.

While fraud primarily poses financial damage, the secondary impact, such as the use of the crime's proceeds to pay for activities like terrorism, can't be ignored.

Inter-carrier trust involves multiple methods that can be abused to bring about toll fraud. One of these is the use of international premium rate numbers (IPRNs), which incur charges beyond those made on regular calls, and could leave users with hefty bills. Within the family of toll fraud is IRSF, within IRSF is IPRN fraud, and within IPRN fraud is another observable technique called short stopping (or call hijacking). Each of these categories has dozens of fraud types with different traits, profiles and risks. Additionally, IPRN and many other toll fraud types such as IRSF may include internal carrier collusion, depending on the specific implementation and on whether the carrier incentivises its sales staff to increase sales volume but does not incentivise the selection of non-criminal clients. This is an attribution problem centering on carrier customer onboarding security and supply chain security — the two ends of the carrier business "pipe."

If, for instance, a telecom carrier colludes with criminals to make a profit, cell towers (and all mobile phones nearby them) will have very little in the way of anti-fraud controls. Some criminals even go out of their way to set up their own cell towers (also called rogue femtocells) that can affect devices, including wireless IoT devices, within a 100-metre radius or more.

These risks can originate from a wide range of technologies, including 5G, traditional trunking, long-distance networks and satellite. They may be aimed at phones (hacking, for example), networks, carriers or the IoT.

While the fraudulent activity of toll traffic compromise is very profitable, it can be detected although often only after the fraud has occurred. If the victim carrier detects the fraud, it can report the source carrier to the global telecom authorities, which effectively "block" the perceived source of the crime. However, the perceived source of crime is not always the actual source of the crime. Criminals can originate their attack from another source and have it appear as the most profitable victim. It is then the victim, not the attacker, who is consequently blocked or subjected to a denial-of-service (DoS), which may have been the intent in the first place. In some cases, such as in island nations, on cruise ships and at other similar locations, they are even blocked entirely.

How the fraud can be carried out

When a miscreant adds itself to the circle of inter-carrier trust as a supplier to a carrier, a vendor of carrier equipment, a "grey" carrier covertly partnering with criminals, or a "black" carrier reselling hacked carrier services, the technical sophistication of an attack is moderate. However, when a miscreant creates its own "war rig" carrier infrastructure (as represented in Figure 1 below), which could be both financially cheap and physically small, the attack becomes more sophisticated. From the perspective of an attacker with a functional war rig, the attack becomes more flexible, more profitable, and less risky.

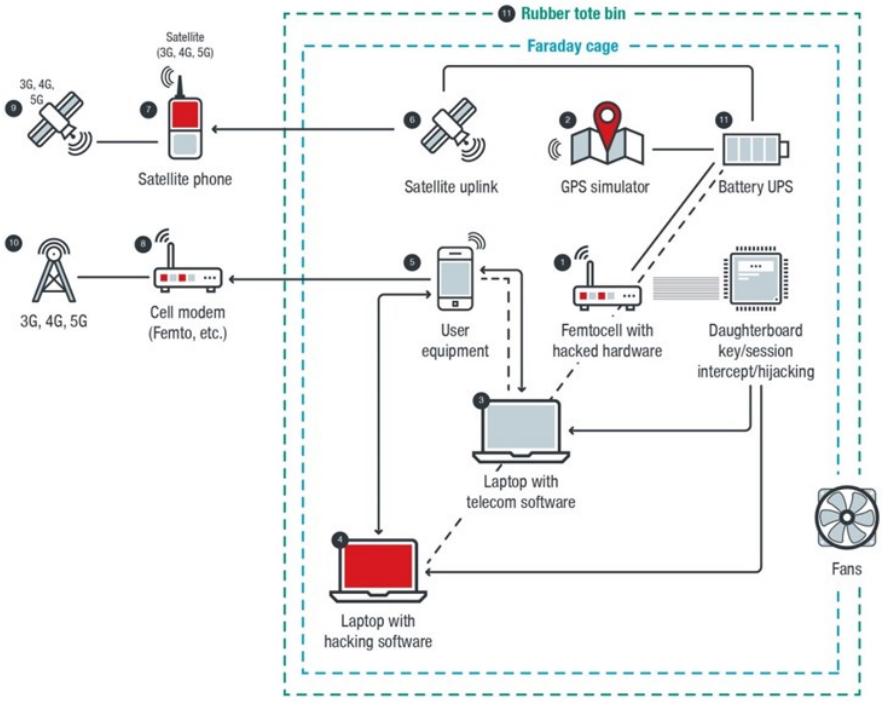

Figure 1. Telecom war rig, where individual war boxes work together to automate telecom fraud.
Note: Low-power IoT targets reduce attack power and hence battery size and total rig weight or size.

A telecom war rig is a network of interconnected hacker war boxes composed of different controlling telecom equipment types. Recently, the cost of telecom equipment has decreased to the point that individuals can launch such attacks. War rig elements and war box components include:

1. Radio war box – Femtocell with hacked hardware, which allows arbitrary information to be fed to and from the user equipment (UE).
2. GPS war box – GPS simulator, which allows arbitrary information to be fed to the UE and provokes a change of state such as roaming and falsification of the apparent location that the attack is originating from (hiding the location of the attacker).
3. Telecom war box – Laptop with telecom software, which provides a sense of "reality" and technical consistency to the changed state of the mobile device.
4. Traditional information technology (IT) war box – Laptop with hacking software, which collects, sorts and manages data generated by the attack.
5. Victim ("user equipment") – One or more mobile devices such as those connected to the IoT (note that the victim UE can be outside the shield represented by the dotted line to perform bulk attacks against people or devices within range.)
6. Satellite war box – Satellite uplink, which routes the attack across satellite infrastructure to provoke a telecom billing response from the telecom network on the other side of the satellite.
7. Satellite phone – A point to launder data as it goes back to the telecom network.
8. Cell modem, femto, etc. – These allow arbitrary information to be fed to the telecom network.

9. Typical telecom satellite with common attributes.
10. Cell tower or other base stations (5G, 4G, 3G, LPWAN, etc.) – These allow arbitrary information to be fed to the telecom network.
11. Rubber tote bin and Faraday shield combined with battery and fan – These allow the entire rig to be mobile (in a car, for instance) and function for an indefinite period, if charged by a car inverter. (Note that if the target devices are low-power IoT devices, the overall size of the rig and its power requirements decreases significantly. The entire rig can fit in a backpack or the back of a motorbike and still function for a prolonged period. The rig may still fit in a backpack for cellular attacks, but its power demand will limit its operational effectiveness.)

It is also important to note that telecom fraud grows substantially in impact each year. However, the necessary cost and sophistication to execute it decreases. Attacks have also recently gained attention in the cybercriminal underground in anticipation of the widespread use of 5G technology. The nature of 5G amplifies the financial impact of frauds such as IRSF due to the dynamic scalability and openness of billing of the technology.

Defending against telecom fraud

The fight against fraud should not be something that either private industry or law enforcement should shoulder alone. Forming public-private partnerships based on trust and information sharing is a fundamental strategy for success. Europol has already demonstrated how such initiatives can work effectively, with hugely successful industry-spanning actions targeting a number of areas of fraud, including e-commerce, airline ticket fraud and money mules. To this end, in 2017 Europol established the Cyber Telecoms (Cytel) Fraud Working Group, with its initial focus being on the largest class of cyber telecom fraud: IRSF. The group consists of law enforcement officers from 18 countries from around the world, the GSM Association (GSMA), the Pacific Island Telecommunication Association (PITA), the International Telecommunication Union (ITU), Trend Micro and more than 35 global telecom companies.

In April 2018, during a two-week action by the Working Group, 250 000 fraudulent transactions were reported, and over 100 cases were reported to law enforcement, resulting in 25 new investigations. Additionally, over EUR 13.13 million in fraudulent payments was blocked. While the focus of the action was IRSF, the activity also captured a wide variety of other telecom frauds, with Wangiri fraud and PBX hacking also prominent in the reporting. Wangiri fraud involves an automated criminal dialer calling many people once each, and when they call the attacker back they are billed excessively, for as many minutes as possible.

As discussed, toll fraud is a financial crime executed in the telecom domain. As such, it can be tracked at a financial level through the correlation of financial and telecom evidence. As a multijurisdictional technology crime, it can be predicted through intelligence fusion, where more intelligence means faster detection and more credible prediction.

As a financial telecom cybercrime, it can be detected well in advance through predictive analytics such as those employed by new technologies. One example is the virtual security architecture called security orchestration, a rules-based network management strategy that can easily adopt financial and anti-fraud rules as part of its native network management approach. Through the correlation of telecom events (such as calls, radio communications and messages) and available threat information (such as IP addresses and reputation data), security orchestrators will be able to combat increasing telecom fraud incidents.

The prevalence of old and new frauds that use emerging technologies such as the IoT and 5G warrants the integration of 5G machine learning and artificial intelligence to create new models capable of being orchestrated. This way, enterprises' security posture will evolve in pace with attackers' techniques. Moreover, this will help organisations prepare against the different types of fraud that can put them in a bad light and negatively affect legitimate customers. This approach is also especially critical in regard to organised crimes and their use of criminal artificial intelligence (CAI).

Conclusion

Telecommunications fraud represents a serious threat to the telecommunication industry, resulting in loss of revenue, which is undoubtedly passed onto customers. It also represents a significant source of criminal revenue, which could potentially be reinvested in other serious criminal activities.

Experience in other areas of fraud has shown us that collaborative public-private partnerships are a prerequisite for effectively tackling this threat. Unfortunately, relationships between law enforcement and the telecommunication industry have in most cases not reached the level of trust and cooperation as those seen in, for example, the financial sector. The Cyber Telecoms (Cytel) Fraud Working Group is the first step toward addressing this.

More work is needed to determine how criminals can obtain the telecommunication equipment needed to carry out such attacks and how they can become part of the circle of inter-carrier trust. Solutions to these problems, and other aspects related to cytel fraud, will likely need to be addressed jointly by law enforcement, the industry and regulators.

References

1. Trend Micro. *Trend Micro.* "Business Process Compromise (BPC)." Last accessed on 15 August 2018 at https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise.

2. Basset. (2012). *GSM Association.* "Following the money – the drivers of fraud." Last accessed on 15 August 2018 at https://www.gsma.com/membership/wp-content/uploads/2012/03 Following_the_money_the_drivers_of_fraud.pdf.

3. Craig Gibson. (31 May 2018). *TrendLabs Security Intelligence Blog.* "Emerging 5G Technology Could Compromise SIM Card-Dependent IoT Devices on Massive Scale." Last accessed on 15 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/emerging-5g-technology-could-compromise-sim-card-dependent-iot-devices/.

4. GDPR Report. (29 May 2017). *GDPR.Report.* "Telecommunications: the battle against fraud." Last accessed on 15 August 2018 at https://gdpr.report/news/2017/05/29/telecommunications-battle-fraud/.

5. United Nations Office of Counter-Terrorism. (n.d.). *United Nations.* "UN Global Counter-Terrorism Strategy." Last accessed on 15 August 2018 at https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy.

6. Craig Gibson. (11 June 2018). *TrendLabs Security Intelligence Blog.* "Attack Vectors in Orbit: The Need for IoT and Satellite Security in the Age of 5G." Last accessed on 15 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/.

7. Europol. (19 June 2018). *Europol.* "95 E-Commerce Fraudsters Arrested in International Operation." Last accessed on 15 August 2018 at https://www.europol.europa.eu/newsroom/news/95-e-commerce-fraudsters-arrested-in-international-operation.

8. Europol. (26 June 2018). *Europol.* "141 Arrested in Worldwide Crackdown on Airline Fraud." Last accessed on 15 August 2018 at https://www.europol.europa.eu/newsroom/news/141-arrested-in-worldwide-crackdown-airline-fraud.

9. Europol. (28 November 2017). *Europol.* "159 Arrests and 766 Money Mules Identified in Global Action Week Against Money Muling." Last accessed on 15 August 2018 at https://www.europol.europa.eu/newsroom/news/159-arrests-and-766-money-mules-identified-in-global-action-week-against-money-muling.