TransNexus®

VOIP THEFT OF SERVICE: PROTECTING YOUR NETWORK

Table of Contents

Introduction to VoIP Theft of Service

The truth is you just aren't a phone company until you've had a run-in with telecom fraud. VoIP fraud is a significant and growing problem in the telecommunications industry. Because fraudsters often attack during weekends, fraud events often go undetected for many hours. A single fraud event can easily cost a company between three and fifty thousand dollars. In many cases, this number can be even larger.

This is a problem that is only increasing. According to the CFCA report, phone fraud is growing at a rate of 29% per year. As the popularity of VoIP continues to grow, the problem of VoIP fraud will become an increasing threat to the industry.

Understanding the threat is the first step in preventing fraud. The more an organization learns about the many ways that criminals can compromise a vulnerable network, the easier it will be to put measure in place to prevent criminal access.

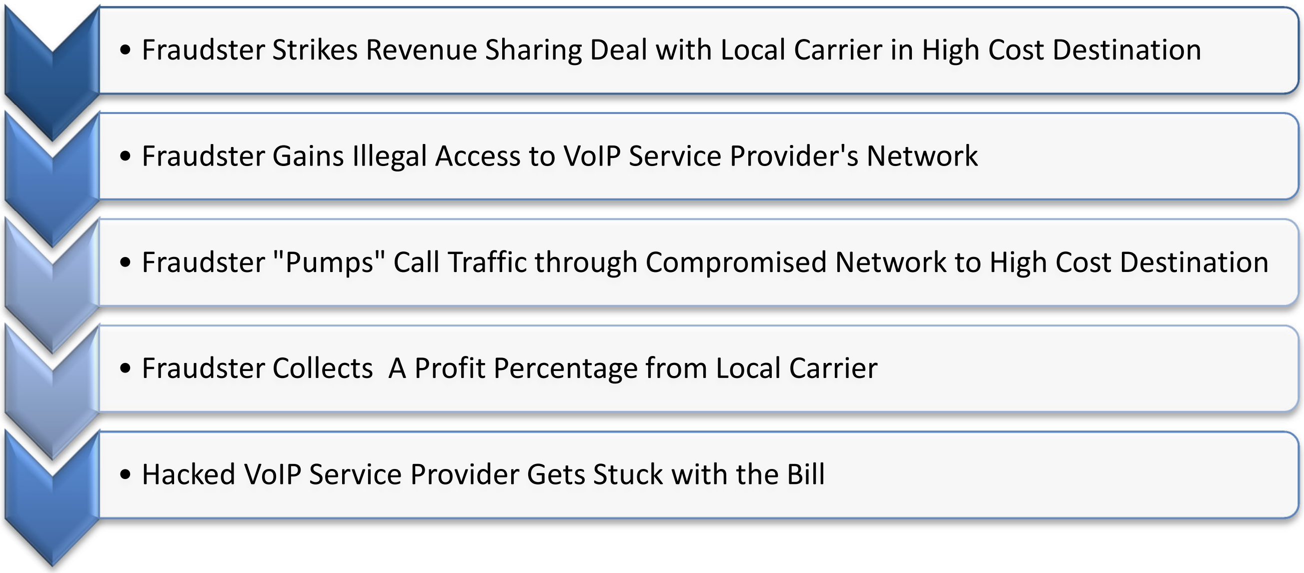
Meet Our Expert – Phone Power

At TransNexus, we want to help our customers prepare their best defense against the VoIP security threats. For help, we turned to an expert in enterprise communications security, Ryan Delgrosso, CTO at Phone Power. Ryan is the CTO and chief network architect at Phone Power and is responsible for the design and construction of their nation-wide telecommunications network. Prior to joining Phone Power, Ryan had extensive experience in both the network security and finance industries.

The Anatomy of International Revenue Sharing Fraud

International Revenue Sharing Fraud (IRSF) is, without a doubt, both the most damaging and the most prevalent VoIP fraud scenario. Revenue share fraudulent activities are those which abuse carrier interconnect agreements. The fraudster partners with a local carrier that charges high rates for call termination and agreement to share revenue for any traffic generated by the fraudster. Common destinations for these calls include West African countries, UK mobile numbers, and satellite phones.

IRSF is characterized by large amounts of calls, often with long duration, to a single destination. While it is not difficult to detect IRSF by examining Call Detail Records (CDRs), by the time you collect the CDRs, the damage has been done.



- Fraudster Strikes Revenue Sharing Deal with Local Carrier in High Cost Destination
- Fraudster Gains Illegal Access to VoIP Service Provider's Network
- Fraudster "Pumps" Call Traffic through Compromised Network to High Cost Destination
- Fraudster Collects A Profit Percentage from Local Carrier
- Hacked VoIP Service Provider Gets Stuck with the Bill

"IRSF is the most common form of fraud we see," said Ryan Delgrosso, CTO of Phone Power. "The international carrier that delivers the last mile is obligated for paying the final destination telco. They charge the carrier that sent them the call, and the cost flows downhill until you get to the access point that was compromised. Further complicating matters, these schemes always cross international boundaries making pursuing it from a criminal perspective almost impossible. Access or retail service providers usually end up eating the costs."

Common International Revenue Sharing Fraud Scenarios

The first step for a potential VoIP fraudster is gaining illegal access to your network. As with any large network, it is nearly impossible to protect every access point to a VoIP network. This is especially true for retail service providers whose customers access the service provider's network over the Internet using a wide range of different access devices. Residential or small business customers access the service provider network using analog telephone adaptors (ATAs) that may be easily compromised. Larger enterprises may access the service provider's network via a SIP trunk connected to a Private Branch eXchange (PBX) which aggregates traffic from hundreds of SIP phones. Many of the SIP phones may be on the public Internet and completely removed from any security precautions that could be enforced the enterprise or service provider. In addition, lax PBX security precautions can make PBX hacking a simple task.

FCC Guidelines: Avoiding Voice Mail Fraud

Always change the default password

Choose a complex voice mail password of at least six digits

Change your voice mail password frequently

Don't use obvious passwords such as a birth date, phone number, or repeating or successive numbers

Check your recorded announcement regularly to ensure the greeting is indeed yours.

Consider blocking international calls, if possible

Consider disabling the remote notification, auto-attendant, call-forwarding, and out-paging capabilities of voice mail if these features are not used.

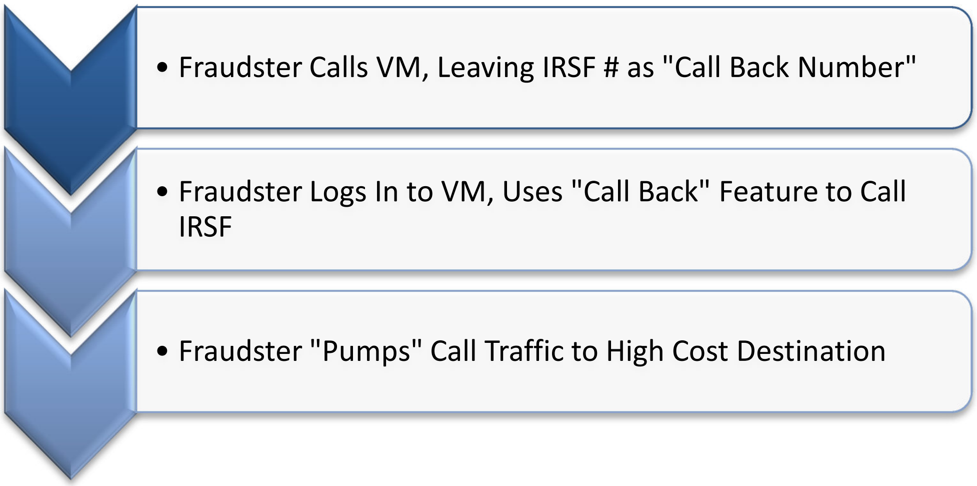
Source: http://www.fcc.gov/guides/voice-mail-fraud

Following are three examples that illustrate how fraud techniques have progressed from hacks over the telephone network using dial tones, to hacks of the web interfaces of PBXs to more sophisticated hacks of customer premise equipment on the Internet.

Voice Mail Hacking

Voice Mail hacking was an early form of communications fraud. It can happen simply and easily through the telephone network. It is a problem rampant enough that even the FCC has recently issued guidelines on how to avoid becoming a victim. Here, a hacker need only find a device with an easy to break password. Some voice mail systems have static or easily guessed default passwords, and users often do not change the default. Recent studies have shown that the password 1-2-3-4 constitutes nearly 5% of Voice Mail passwords – 7x the frequency of the next most common password (0-0-0-0).

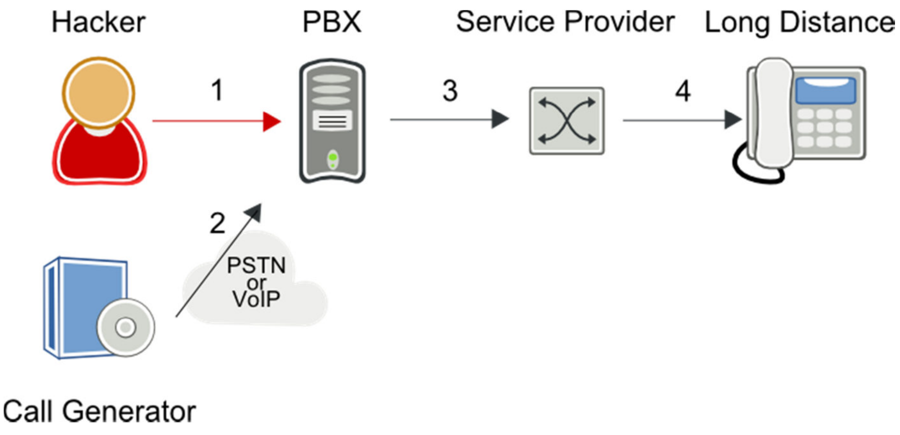
Criminals can easily use this straightforward technique for International Revenue Sharing Fraud (IRSF). Once they have the password to an account, it is a simple matter in many Voice Mail systems to exploit the "Call Back" feature – that feature that allows a user to immediately return a missed call. The criminal calls the phone number, leaving their IRSF number as the "call back" number. Then, they login to the account, find their missed call, and return it, signaling the Voice Mail to initiate a call to their IRSF number. Once the call is connected, a criminal can attempt to leave it up as long as possible, often hours or days.



- Fraudster Calls VM, Leaving IRSF # as "Call Back Number"
- Fraudster Logs In to VM, Uses "Call Back" Feature to Call IRSF
- Fraudster "Pumps" Call Traffic to High Cost Destination

Call Forwarding Hack

The Call Forwarding hack is a more sophisticated form of VoIP fraud. In this case, fraudsters are hacking through the user access web portal of an enterprise PBX. By guessing a user's password, they can login to a PBX, and configure call forwarding to an expensive long distance destination to profit from IRSF. Then the hacker will call the telephone number of the hacked account which forwards the call for IRSF.



1. Hacker accesses the web interface of the PBX and configures call forwarding to international long distance destination
2. Hacker calls the compromised number over either the PSTN or VoIP.
3. Hacked PBX forwards the call to the service provider's softswitch.
4. The service provider switch forwards the call to the IRSF destination.

Buffer Overflow ATA Attack

Certain Analog Telephone Adapters (ATAs) with web interfaces are notoriously vulnerable to attack. VoIP fraud expert, Ryan Delgrosso , from Phone Power, describes credential theft from customer premise devices, such as ATAs or SIP phones, as a potential worst case scenario. "If you blow this up to a global scale, all across the industry, there is a really big dollar figure attached," said Delgrosso. Buffer overflow vulnerabilities occur when an ATA has a web login screen, something Delgrosso describes as "exceptionally common." Customers use their ATA as router with a public IP address so the Service Provider's technical support can access the device when needed. In this case, the vulnerable device is an ATA from a vendor with very high market share, so the potential for widespread fraud is huge.

Adding to the mess, Delgrosso adds that one attack signature he has seen with this scenario is that hackers will delete the configuration URLs from compromised devices. This prevents the administrative password from being updated again. The device will continue to function, leaving the compromised customer completely unaware of the attack, but the device will stop talking to the carrier's configuration server. When (and if) the security breach is discovered, a carrier cannot make a global change that is pushed out to all devices at once. Rather, the service provider must contact each individual device owner to perform a factory reset.

Step 1 Find target devices to hack.

- Use a network mapping tool, such as the open source Nmap utility (Nmap.org), to scan the Internet for devices listening on port 80 (the HTTP port used by web browsers). The target device can be identified by its HTTP response.

Step 2 Rewrite Administrative Password.

- Send an HTTP Post message to the target device. The message is designed to overflow the device's memory buffer and rewrite the administrative password.

Step 3 Steal device credentials.

- Log into the compromised device using the new administrative password and download the user name and password which are stored in plain text.

Step 4 Pump Traffic

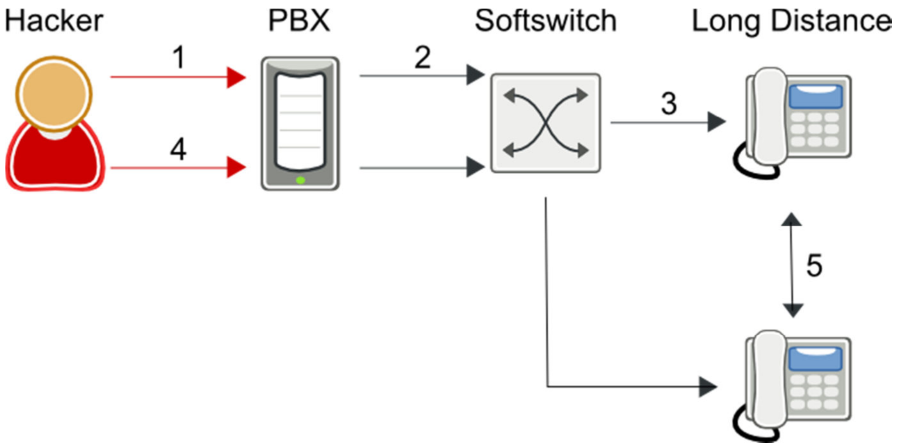
- Using device credentials, login and begin pumping traffic to your IRSF Number.

"Once we discovered this particular vulnerability, we were able to get ahead of it pretty quickly," said Delgrosso. "We know of another company that found thousands of compromised accounts. We have since shared our findings with many other carriers, and have validated that this is happening across the industry, on a global scale. For many carriers, this can be a nightmare scenario."

In scenarios like this it is important to note that the carriers have an urgent vested interest in detecting and securing devices that show these kinds of vulnerabilities, and often times a response to threats of this type cannot wait for the hardware vendor to write a patch, and in many cases they do not want to announce the vulnerability or the patch for PR reasons.

Blind Call Transfers

Blind call transfers are a sophisticated technique for doubling International Revenue Sharing Fraud while making the fraud more difficult to detect. See the chart below for a detailed explanation.



1. Hacker phone service hacks unsuspecting PBX to make a call to make international calls
2. PBX sends SIP INVITE to service provider's soft switch
3. Softswitch routes call to international number for IRSF
4. Hacker instructs PBX to blind transfer call to another international number for IRSF
5. The hacker hangs up. The call between the two international destinations remains in place. This is double IRSF with one phone call.

"We saw a lot of these happening several years ago," said Delgrosso. "Once the calls are transferred, they stay up until the carrier shuts it down. We've seen calls stay up for over 24 hours. On many platforms transferred calls don't count against concurrent calls, and most switches won't cut a call record until the call is over. If the criminal is clever, he will transfer dozens or hundreds of calls concurrently. They are pinned in the network, and can go unnoticed until it is too late."

Wholesale Trunking

Fraudulent wholesale trunking is a relatively new phenomenon, but one that is growing in popularity and difficult to detect. In this scenario, the fraudster is actually making money by selling wholesale trunking services, using stolen credentials to terminate the calls.

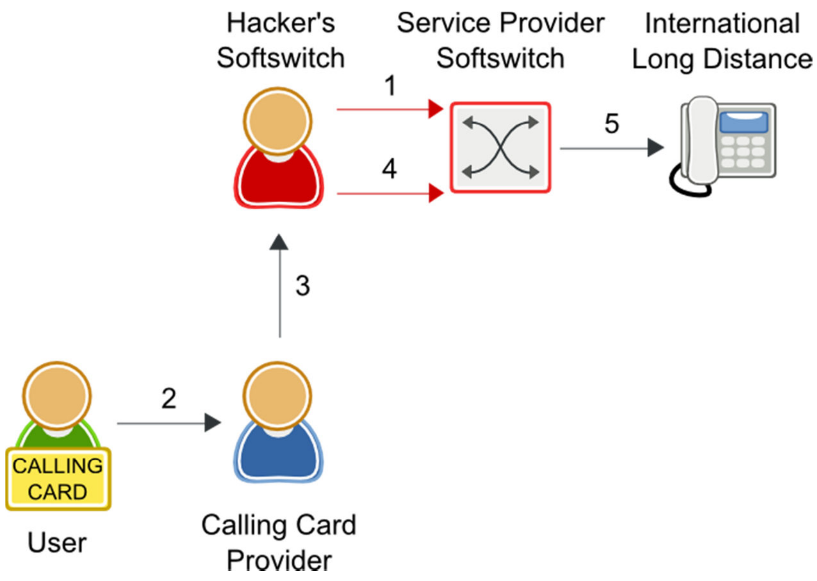
The key calling signature for this type of fraud is a huge number of apparently random calls. The destinations are not particularly high cost, but neither are they cheap. Countries like Vietnam, Laos, and other middle-priced Asian countries show up often. The traffic often appears to be to residential numbers.

Online Black Markets: The Final Frontier

The Internet is no stranger to crime. From illegal drugs to hacked VoIP network IDs and passwords, nearly anything can be purchased online with a few clicks of the mouse. The entire process of ordering illicit goods and services is alarmingly easy and anonymous.

Online black markets, such as Silk Road and Black Market Reloaded, use Hidden Tor Servers to mask a user's tracks on the site. The level of protection provided by Tor makes law enforcement's job tracking such activities next to impossible.

Adding to the confusion, these markets deal in anonymous "Bitcoin" currency. Bitcoins are a peer-to-peer currency, not issued by banks or governments, but created and regulated by a network of other bitcoin holders' computers. They are purportedly untraceable and have been championed by cyberpunks, libertarians and anarchists who dream of a distributed digital economy outside the law, one where money flows across borders as free as bits.



1. Hacker's softswitch registers with service provider's softswitch using stolen user name and password
2. Calling card user places a call
3. Calling card provider routes call to lowest advertised route (hacker)
4. Hacker sends INVITE to service provider's softswitch
5. Softswitch routes call to international long distance destination

Delgrosso explains that he has traced this type of fraudulent traffic coming from prepaid calling card companies operating a VoIP platform in an offshore colocation facility. Prepaid calling services are well suited to exploit this type of fraud since there are no calling numbers linked to customers. The IP address of the prepaid calling platform is the only link to trace the fraudster. Unfortunately, geolocation cannot always be used to identify the fraudster. These services can be offered via a tunnel through the Internet that hides the true IP address of the fraudster. The public IP address of the fraudster's calling platform could be the IP address of a hosted Virtual Private Network (VPN) service while the actual prepaid calling platform is located in a different part of the world.

The Future of VoIP Theft of Service

Delgrosso believes that the rapid growth of VoIP related fraud techniques is creating its own eco-system. His observations lead him to believe that some hackers specialize in stealing network access credentials. This is their specialty, not VoIP fraud. He theorizes that a black market exists for selling telecom credentials (see sidebar), and many hackers simply sell stolen credentials to as many criminals as possible. For this reason, service providers may see call signatures from a variety of types of VoIP fraud. A single account, once compromised, can be sold over and over again to any criminal who wishes to perpetuate IRSF or start a fraudulent wholesale trunking company.

Preventing VoIP Theft of Service

Secure Your Network

The first layer of defense against VoIP Theft of Service is to secure your network. It may seem simple, but ensuring that your network passwords are strong can be one of the best ways to avoid security threats. We recommend increasing your networks password strength requirements, and well as improving your default password strength. For maximum protection, passwords should not be sequential or repeated numbers, or your own extension. To limit the impact of any compromised passwords, disable voice portal dialing.

Unfortunately, for many carriers, it is difficult, if not impossible, to control customer's password choices. This is especially true in SIP trunking scenarios, where there carrier may have no control over the types of devices and passwords used behind the PBX. The less direct control a carrier has over their network endpoints and devices, the greater the risk.

Fraud Detection Software

Though a secure network can help to prevent fraud, attacks are almost inevitable today. Constantly changing technologies and savvy criminals ensure that there is always a new way to hack into a network. It is absolutely essential to have some sort of fraud detection software in place, to catch instances of fraud before it hits your bottom line.

It is not enough to analyze CDRs for evidence of fraud. By the time calls are completed, or cut off by the carrier, the damage has been done, and tens of thousands of dollars lost. Instead, effective fraud detection software will look at call routing requests. This allows alarms to go off before the calls are set up, and before you find 300 calls to the Ivory Coast that have been connected for 48 hours.

TransNexus has developed a number of solutions to detect and prevent fraud in VoIP networks. TransNexus solutions integrate fraud detection with an already world class least cost routing (LCR) platform. TransNexus software can block fraudulent calls before they are routed, including calls that have been transferred from their original source.

Summary

Fraudulent activity across VoIP networks is increasing, and will continue to be a major problem for service providers in the coming years. However, with proper planning and maintenance, as well as the proper monitoring tools, this threat can be successfully managed

About TransNexus

TransNexus is a software development company specializing in applications for managing wholesale VoIP networks. TransNexus provides its Operations and Billing Support System (OSS/BSS) software platform to major VoIP carriers worldwide. Important carrier features offered by TransNexus are least cost routing, number portability, fraud detection, profitability analysis and QoS controls. For more information, online demonstrations, and free downloads, please visit www.transnexus.com.

About Phone Power

Phone Power is a next-generation telecommunications company, headquartered in Los Angeles, California. A privately-owned company founded in 2005, they provide telecommunications service to the continental US, and Canada. All customer service is based in the USA. Phone Power customers range from single-line residential service all the way to corporate call centers. For more information about Phone Power, visit www.PhonePower.com.