The Surging Threat of Telephony Denial of Service Attacks

October 21, 2014

13750 San Pedro, Suite 820 San Antonio, Texas 78232 • PH 210.402.9669 • FAX 210.402.6996
Telephony Denial of Service (TDoS) attacks are on the rise. The U.S. Department of Homeland Security (DHS), along with several other federal and state agencies, have issued very recent warnings that cite a growing number of TDoS attacks.

TDoS attacks generally follow the same model as the more traditional data network denial of service (DoS)—unauthorized users flood the system with too many access requests and prevent legitimate users from accessing the system. With TDoS, the objective is to make a significant number of phone calls and to keep those calls up for long durations in order to overwhelm an agent or circuit capacity. By keeping long duration calls active, the attacker prevents voice network resources from being used by legitimate callers such as customers, partners and suppliers. This not only impairs voice network availability in general, but can also be selectively focused to impede specific types of calls, for example, calls from a financial institution to an account holder to verify funds transfers. That is, TDoS can not only be used as an outright means to disable a company’s communications network, but it can also be used as a means to enable other forms of fraud and misuse.

The impact to an organization when attackers tie up every available voice circuit, or a significant enough subset to impact voice services, can be a catastrophic loss of the ability to conduct business at even the most basic level; the subsequent loss of business and revenue can be devastating.

Voice network security in the enterprise has been an issue for years, with voice application threats such as toll fraud, social engineering-based account takeover, robocalling fraud schemes (vishing), harassing calls, and modem abuse posing the largest threats. However, with the proliferation of VoIP in both the service provider and enterprise networks, the threats to voice networks have dramatically increased.

This increase is not because IP voice network itself is being attacked due to packet vulnerabilities, but rather that the IP voice network makes it easier to create attacks at the application level, and thus makes the overall voice network, whether that is IP or legacy TDM, vulnerable. Attackers leverage VoIP to perform the same voice-application attacks they have been perpetrating for years. Therefore, even the Public Switched Telephone Network (PSTN), which used to be primarily a closed network, has become much more vulnerable due to the proliferation of VoIP call origination, causing it to increasingly experience the security threats common to the Internet. This is compounded by social networking sites such as Facebook and Twitter being used to organize mass calling campaigns, creating a new method of generating harassing calls or even TDoS attacks.

*Increased Threats From The PSTN*

The primary way in which VoIP is increasing the threat to enterprise voice networks lies in the simple and inexpensive ability for attackers to originate SIP calls onto the PSTN.

As the PSTN continues to migrate to IP, with SIP being the dominant protocol, it has become easy and inexpensive to originate large numbers of concurrent calls (or floods) into this network. While the trunking entry point into enterprises remains primarily TDM, the call origination point is often
SIP. On the call origination side, the PSTN looks more like the Internet every day, and this change is accelerating and is out of the control of the enterprise. Service providers are in the business of delivering calls and are neither incented nor equipped to address attacks based on call floods. These automatically generated calls are often referred to as "robocalls," and are occurring independently of how the enterprise chooses to adopt IP for voice services. This transition represents the most significant threat to enterprise networks.

SIP trunks, consumer/cable SIP offerings, Internet-based SIP services, softphones, and smart phones all combine to make call origination with spoofed/anonymous calling numbers easy and commonplace. Moreover, now a call generation capability can be set up in a manner of hours or days to enable voice attack campaigns, which include TDoS, vishing, and voice SPAM. These tools make it possible to generate thousands of concurrent calls. These attacks can be accomplished with free software, such as an Asterisk IP PBX, SIP call generator, and other tools, to automatically generate robocalls. An IP-aware botnet can fire up and generate tens of thousands of simultaneous calls, and there are even commercial services available to generate robocalls.

**Malicious Calls are the Real Threat**

As discussed, attacks are increasing not because of packet vulnerability, but rather that the IP voice network makes it easier to create attacks at the application level, and thus makes the overall voice network, whether IP or legacy TDM, more vulnerable. While packet-based, VoIP-specific attacks garner much discussion regarding potential vulnerabilities, the real active threat lies with voice-application attacks. The means of attack is often not an IP scan, malformed packet, or flood of packets, but rather, it is a malicious call exchanged between the PSTN and the enterprise.

These malicious calls may cause the enterprise:

- Financial loss through long distance abuse and toll fraud
- Theft of money and loss of brand luster by manipulation of financial contact center representatives through social engineering
- Problems by harassing key personnel or just taking up bandwidth and agent time in contact centers
- An overwhelmed contact center or other enterprise resource if the calls are numerous and a long duration
- Security issues through illicit modem access, either to a key computing resource or outbound to an ISP, creating a backdoor into the enterprise data network

**A Visual Summary of Recent Voice Security Trends**

Based on voice threat monitoring data acquired from hundreds of real-world, enterprise operational networks over many years, SecureLogix has developed a threat-risk trending model to provide an all-at-once visual summary of the voice security risk environments enterprises face. It represents recent relative trending and illustrates the severity of well-known and new-risks areas.

The chart shows the primary threats to enterprises. Each threat is represented by a "bubble", the size of which is a measure of the impact to the enterprise, coupled with the difficulty of detection
and mitigation. The x-axis shows the relative severity, while the y-axis shows the rate of incident increase (threats towards the top are increasing in occurrence). This chart is based on real-world data assembled from hundreds of SecureLogix’s assessments and managed service efforts.

Trends relating specifically to TDoS Attacks include:

- **Socially Organized TDoS** – With its legality and ease of mass-organization through social networking, this method of TDoS has been adopted as a mainstream tool for organized dissent. It has severe impact due to the density of calls and the ability of human callers to engage target staff for extended periods of time, but is also a threat which can be detected and mitigated with real-time detection technologies and voice-intrusion prevention.

- **Automated TDoS**—Trending up. Detectable via cutting-edge technology that has limited availability. Very few organizations realize they are victims of this and perpetrators tend to target financial areas of companies and high-volume contact centers. This is on the high severity watch list.

**Anatomy of Socially Organized TDoS**

Socially organized harassing call attacks leverage social networking sites such as Facebook and Twitter. In this case, an attacker who may be a disgruntled individual “organizes” a large group of people, all of whom call at one time, or in a single or small set of numbers. A Facebook page for example, can be quickly set up to coordinate a large group of people to flood an organization with calls by publicizing the reason, the phone numbers, and the time of the attack on the page itself. A similar attack can be organized through Twitter by an individual with a large group of followers. The individual needs simply to generate a tweet that encourages followers to all call a selected number at a designated time. The same attack is also possible by hacking into a celebrity’s Twitter account. They would simply then generate a tweet and request the celebrity’s million+ followers call a specific number at a given time.
2011 was the year in which social networking became widely used as a way to organize vast numbers of participants in protest activities, such as the Occupy movements and London riots. Protest groups have discovered that leveraging social networking technologies to organize or “crowdsourced” callers for targeted telephone disruption campaigns is a very effective and legal means of protest.

So-called “organized complaint” groups have long used call flooding as a means to affect their issues. However, new trends such as social networking, the availability of free VoIP calling, and low cost mobile minutes all serve to drastically increase the effectiveness and impact of this form of protest. In fact, online services are now available to mass-call politicians, and social media groups have been organized around topics such as “occupy the phones” making social engineering a mainstream tool of organized protest.

**Anatomy of Automated TDoS**

TDoS refers to automatically generated call floods received by enterprises, primarily their contact centers or other public facing support numbers. Attackers flood the contact center IVR or agents with hundreds or thousands of concurrent calls for the purpose of traffic generation/pumping or outright TDoS. Some of these attacks are designed to generate calls for revenue and target large contact centers because the attacker hopes that the extra traffic will not be quickly detected.

Well-designed call pumping attacks are designed to dwell in IVRs and never reach an agent where they will be detected. These attacks are designed to stay in the IVR as long as possible but not intentionally overwhelm a resource or draw attention from agents. However, as call pumping attackers get greedy or sloppy, these attacks are noticed and affect IVR bandwidth and agents.

TDoS attacks can use simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns, which attempt to cause calls to dwell in IVRs. These are simple techniques, with future attacks likely using other types of mutating audio.

TDoS attacks are sometimes difficult to detect because the attacker may change the caller ID frequently. Often the easiest way to determine non-legitimate calls is to trace back each call to the originating carrier. If that call center typically does not receive calls from that area or carrier, it
can quickly be assumed that they are non-legitimate. Unfortunately this method is difficult to use as the attacks can move through multiple service providers, making them time consuming to trace back to the source. And because service providers are not allowed to examine the audio, they are forced to look for attacks based the limited information they do have available.

Attacks can come from one source, multiple sources, compromised enterprises, or even a botnet where each piece of malware makes a single call to the target. The following diagram illustrates this type of attack.

In the future, these attacks will be much more severe. By simply generating more calls or using more entry points to the IP network, many more calls can be generated, resulting in a severe business-impacting attack including one that can degrade the performance of a contact center, rendering access unavailable to legitimate callers and potentially negatively impacting brand image. This can be especially damaging at sites with limited trunk capacity. These attacks will get harder to detect, be more common, and create a greater impact. These attacks will also expand and affect other parts of an enterprise.

**Real Life Examples – Socially Organized TDoS**

One popular example of socially organized TDoS involves a rapper called The Game. He put a request on Twitter for followers to call the Los Angeles County Sherriff’s Office. More than 500,000 people received the message and created a call volume that shut down emergency services.

Similarly, Facebook has been used to coordinate TDoS attacks on bond rating agencies relating to national credit ratings and Twitter searches show “Occupy” movements requesting followers to call banks, lobbyists, and so forth.

Socially organized TDoS is favored for two reasons: 1) calling an organization or individual is legal and inexpensive and 2) organizers have realized that they do not need a participation rate so massive as to overwhelm circuits (or a web server in an IP DoS case) but that they only need to overwhelm a single individual or a relatively small number of agents in a contact center. So, it is an inexpensive, legal and effective method.

In 2012, we began to see those same social media portals used to inadvertently produce a TDoS condition. In a recent example, a minor teen celebrity and his management team used various social media portals including YouTube, Twitter and Facebook to encourage his fans to call him. Of course, due to the large number of followers, most celebrities, like this one do not take direct calls from fans. Instead, they use a set of telephone numbers that go to a series of voicemail systems that play a short message.
This simple promotion became an inadvertent TDoS condition when a simple typographic error was made in posting one of the telephone numbers. The phone number in error happened to belong to a single employee at a government agency. That one employee was flooded with calls from the teen celebrity’s fans. This further refines the definition of a TDoS condition: a TDoS condition can affect an entire organization, a sub-group within that organization, such as a call center or help desk, or even a single user when they are overwhelmed with calls to the point where they can no longer conduct business.

Fortunately, this government agency had the SecureLogix and Cisco solution to monitor and analyze calls and we alerted them to the huge spike in calls to that single number. Since calls from those fans could originate from virtually any telephone number anywhere, the agency adopted a different strategy for defense. Since this number belonged to a single user at that government agency rather than a main number or a group number, we were able to identify a "whitelist" of telephone numbers that the employee regularly used for business purposes; only calls from numbers on that whitelist were allowed and all other inbound calls to that number were blocked. In the graph below, the vast majority of all inbound calls to that user had to be terminated as the fans repeatedly called in expecting to hear from their teen celebrity.

The power of social media can be magnified depending on the reach of the celebrity in question. In this particular instance, this “minor celebrity” had almost 400,000 followers on Twitter, of which only a fraction had participated. If the same thing had happened with a major celebrity with millions of followers, the result would have been even more devastating for the employee and the business.

**Real Life Examples – Automated TDoS**

Another method being employed to create a TDoS attack is call automation and the possible use of recorded audio to supplant the need for people to do the calling.

In this example, the victim asked us to analyze several circuits supporting an advertised contact center. The circuits showed much higher peak utilization than was anticipated or expected and they were concerned that customer traffic was being affected. The left hand side of the graph shows an example of the traffic on these circuits, and it can be seen that peak utilization regularly exceeded 90%. We determined that four callers were automatically generating calls which matched our TDoS profile logic, all of which were also found to be presenting spoofed caller ID.
information. We designed a blocking policy and implemented it on the customer lines. The right portion of the graph shows the post-policy implementation peak usage.

Thousands of calls per day were being blocked by our solution, resulting in a noticeable reduction in peak trunk utilization, as can be seen on the graph. Overall, available circuit capacity was increased 60% eliminating the need to purchase extra circuits. Furthermore, as can be seen on the right-hand side of the graph, the contact center still had days where legitimate-caller peak utilization was above 80%. Without our voice policy solution in place, the additional illegitimate robo-traffic generated by the TDoS perpetrators would have resulted in legitimate customers not being able to reach or do business that company.

![Resource Utilization Chart](image)

**The Solution: Policy-Enhanced Gateways and Session Border Control from Cisco and SecureLogix**

SecureLogix® voice policy and security solution is integrated with Cisco’s session border controller (Cisco Unified Border Element (CUBE)) and Cisco TDM Gateways, enabling highly flexible and granular voice-policy solution to identify security threats and issues like TDoS.

By leveraging the network edge through its integration with CUBE and TDM Gateways, SecureLogix Voice Policy fights these abuses before they hit the voice enterprise network. To detect TDoS attacks, for example, you can define a rule to look for a certain number of calls from the same telephone number or extension within a certain time period. The solution can mitigate the attack in any number of ways including recording the call, dropping or forwarding the call, or alerting someone to take action. SecureLogix supports a large number of use cases beyond TDoS including:

- Voice fraud and toll theft
- Phone-based social engineering schemes
- Harassing and threatening calls
- Unauthorized voice-line access to data network resources
- Voice service misuse, abuse, and data leakage
- Voice protocol intrusion into data resources
- Other voice network threats and restricted traffic
By using the Cisco UC Gateway Services API, SecureLogix has integrated its voice-policy enforcement applications with CUBE and TDM gateways, complementing and extending their benefits. With the SecureLogix voice-policy application deployed on a Cisco UCS™ Express server blade, the application can sit directly on the Cisco router alongside CUBE or the TDM Gateway and eliminates the need for external voice-policy appliances. This tight integration provides customers with a truly unified policy enforcement solution across their entire unified communications environment from a single management interface.

To find out more about the Cisco and SecureLogix solutions, please go to these websites:
- Cisco Unified Border Element
- Cisco TDM Gateways
- SecureLogix
DHS Warns of ‘TDos’ Extortion Attacks on Public Emergency Networks

APRIL 1, 2013

As if emergency responders weren’t already overloaded: Increasingly, extortionists are launching debilitating attacks designed to overwhelm the telephone networks of emergency communications centers and personnel, according to a confidential alert jointly issued by the Department of Homeland Security and the FBI.

The alert, a copy of which was obtained by KrebsOnSecurity, warns public safety answering points (PSAPs) and emergency communications centers and personnel about a recent spike in so-called “telephony denial-of-service” (TDoS) attacks:

“Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.”

According to the alert, these recent TDoS attacks are part of a bizarre extortion scheme that apparently starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time.

DHS notes that the attacks can prevent both incoming and/or outgoing calls from being completed, and the alert speculates that government offices/emergency services are being “targeted” because of the necessity of functional phone lines. The alert says that the attacks usually follow a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did. The full alert is reposted here (PDF).

A much shorter version of this alert appeared in January 2013 on the Web site of the Internet Crime Complaint Center (IC3), which warned of another twist in these TDoS attacks: “The other tactic the subjects are now using in order to convince the victim that a warrant for their arrest exists is by spoofing a police department’s telephone number when calling the victim. The subject claims there is a warrant issued for the victim’s arrest for failure to pay off the loan. In order to have the police actually respond to the victim’s residence, the subject places repeated, harassing calls to the local police department while spoofing the victim’s telephone number.”

Neither alert specifies how these call floods are being carried out, but KrebsOnSecurity has featured several stories about commercial services in the underground that can be hired to launch TDoS attacks.

Image: SecureLogix

According to a recent report from SecureLogix, a company that sells security services to call centers, free IP-PBX software such as Asterisk, as well as computer-based call generation tools and easy-to-access SIP services, are greatly lowering the barrier-to-entry for voice network attackers.

The company says TDoS attacks can be difficult to detect, because the attacker typically changes the caller ID on every call. From their report: “This makes it very difficult even for service providers to detect the attacks. Unless these attacks can be quickly traced back to an originating carrier that typically does not generate many calls to the contact center, they are very difficult to differentiate from legitimate calls. The attacks also typically move through multiple service providers, making them time consuming to trace back to the source.”

SecureLogix said TDoS attacks can employ simple audio content, including white noise or silence (which could be dismissed as a technical problem), foreign language audio (representing a confused user), or repeated DTMF patterns.

“These are simple techniques, with future attacks likely using other types of mutating audio. In the future, these attacks will be much more severe. By simply generating more calls or using more entry points to the [target] network, many more calls can be generated, resulting in a very expensive attack or one which degrades the performance of a contact center, rendering access unavailable to legitimate callers and potentially impairing brand image.”

courtesy of krebssecurity.com