The Robocall Threat

An Analysis of the Robocall Threat in Voice Network Security

A Whitepaper From
SecureLogix Corporation

Introduction

Robocalls are the most recognized voice security issue. We use the term “robocall” to refer to a broad class of nuisance and malicious calls, which include automated telemarketing/voice SPAM, impersonation scams, voice phishing (vishing), social engineering, and harassing calls. Some calls in these categories are still manual and some are hybrid, involving an automated and a human component, but we group them into a class of robocalls for this discussion.

Robocalls affect all voice users and types of voice systems. Robocalls most commonly target consumers, including those who are the most vulnerable, but also target employees at businesses and enterprises. Landline consumers have been inundated with robocalls for years. Coupled with an increase in robocall volume and gradual reduction in the use of landlines, robocalls have become increasingly common on consumer mobile phones. Robocalls are also an increasing issue for businesses and enterprises, especially those with public-facing numbers and verticals such as hospitals, which house many vulnerable consumers.

The technical reason for this increase is that the Public Switched Telephone Network (PSTN) is no longer a closed network. It heavily uses Voice over Internet Protocol (VoIP) and increasingly connects to the Internet through the Session Initiation Protocol (SIP). It is very inexpensive, easy, and safe to generate robocall campaigns. All you need is SIP access to the network, free PBX software such as Asterisk, a call generator, and the message you want to deliver. It is also trivial to spoof the calling number, to trick the victim into answering calls that they should not.

It has become more difficult to use email phishing and other forms of fraud. Better email filters, more educated users, chip cards, better online security, mobile authentication, etc., have made other forms of fraud more difficult, driving attackers to the weakest link, which is the PSTN and voice systems. In addition, the voice network still has an unfounded level of trust with many consumers. Users have been somewhat trained not to trust an email, but many still trust the phone network and information such as the calling number/caller ID, which again, is trivially spoofed.

Types of Robocalls

Calls such as telemarketing, surveys, political ads, pranks, and scams have been around for a long time. The same is true for threatening and harassing calls. What has changed is that the ability to cheaply and anonymously generate robocalls, has made telemarketing and other nuisance calls much more common and has made threatening calls such as bomb threats and SWATing worse because they can be delivered to many more victims, and the ability to spoof the calling number makes impersonation scams and phishing more dangerous. We summarize these different types of robocalls in the following taxonomy:

Category	Types	Target	Frequency	Severity
Voice SPAM	Telemarketing/Survey/Debt Collector/Political/ Non-Profit	Consumers	Constant	Nuisance
Scams	Impersonation Scams/IRS Scams/Tech Support Scam/Other Scams	Consumer/ Employee	Very Common	Costly
Phishing	Dead-Air/Answer-Yes/ 1-800 Callbacks	Consumer/ Employee	Very Common	Costly
Harassing Calls	Bomb Threats/SWATing Threatening Calls	Employee	Uncommon	High

These types of robocalls are described as follows:

- Voice SPAM—A broad class of very common calls, which at a minimum includes telemarketers (someone selling something), debt collectors, political calls, surveys, non-profit requests, and other nuisance calls. These calls are a constant issue and are interrupting, annoying, and very much a nuisance. These calls primarily target consumers, while at home, on their mobile devices, and at their place of business.

- Scams—Another broad class of very common calls, where the caller is attempting to defraud the victim, usually by stealing money. There are many types of scams, including those where the caller fraudulently claims they are representing an organization such as the Internal Revenue Service (IRS), other government office, or a technical firm (Microsoft tech support scam). There are also credit card scams, vacation scams, contest winner scams, extortion scams, etc. These scams are truly malicious and defraud consumers out of billions of dollars a year. These calls primarily target consumers, while at home, on their mobile devices, and at their place of business.

- Voice phishing/vishing calls—Vishing calls are a common form of a scam, but the goal is to get the victim to provide some sort of information that is used for a later attack. Some examples are “dead air” or “can you hear me” calls that trick the victim into saying “yes” or something that provides information to the attacker (gender, age, accent, etc.). Other forms of vishing impersonate a victim’s bank and attempt to get them to call back a 1-800 or other number. The attacker answers the call from a fake Interactive Voice Response (IVR) or human that attempts to gather information from the victim. Still other calls are social engineering into

enterprises, attempting to gather information such as passwords. These calls primarily target both consumers and employees at businesses and enterprises.

- Harassing calls—A class of calls intended to threaten or otherwise harass the victim. These include dangerous calls such as bomb threats, SWATing calls, or calls intended just to harass the victim. Traditionally, these calls have been manual, but the ability to deliver them via robocalls makes them that much more disruptive. These calls most often affect employees and businesses.

The Current Robocall Threat

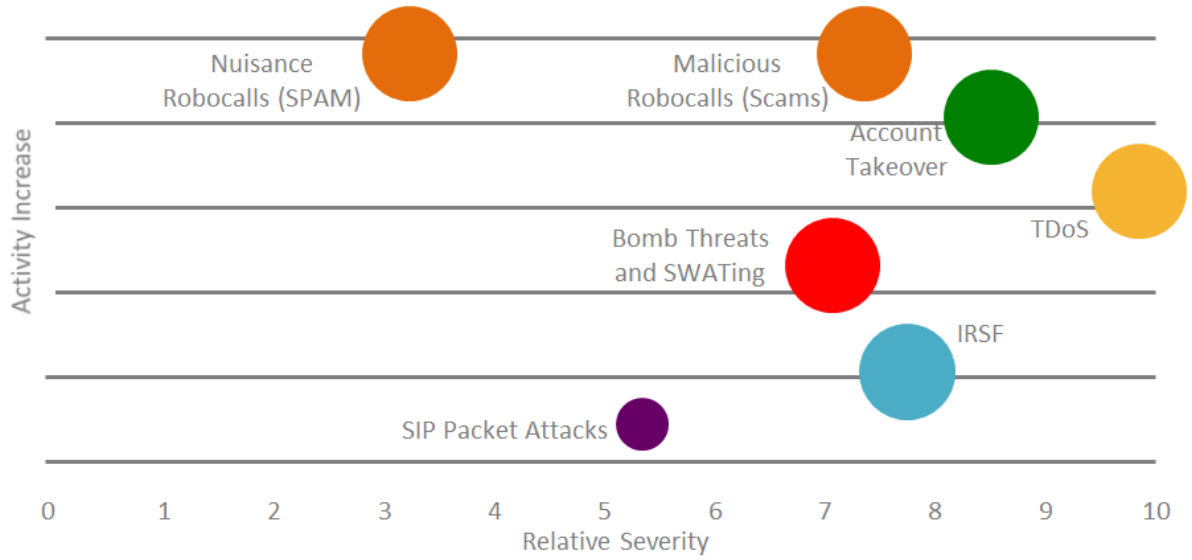
Estimates place the number of robocalls in the billions per month. YouMail reports a peak of 2.61 billion robocalls in September 2016. A 2015 Harris Poll estimates that 27 million U.S. consumers lost approximately $7.4 billion to phone scams. These numbers will only increase as the number of robocalls rises, threatening to reach the levels we see with email SPAM.

The Federal Trade Commission (FTC), which tracks consumer complaints, collects on average more than 250,000 robocall/scam call complaints every two weeks, about 50,000-60,000 unique numbers each period, about 35,000 of which are new numbers. Aside from volume, this shows that while some attackers still use the same numbers, they now more often use random calling numbers. In the IRS scam, for example, attackers use random numbers from the 202 area code, the local area, or other IRS locations.

The most damaging robocalls are scams and vishing attacks. The goals of attackers are to directly steal money, gather Personal Information (PI), or obtain other sensitive information. While SPAM calls are a nuisance, the most damaging calls are those that directly result in financial losses or the gathering of information, which also often leads to financial loss. The IRS scam is one well-known example of an effective and damaging vishing attack. IT scams, “dead air” calls, credit card scams, etc., are other well-known examples of scams designed to collect PI. This PI is also used for later attacks such as Account Take Over (ATO) in financial contact centers. Other damaging calls include those that target specific users by using “spear vishing” techniques to target executives, Human Resources (HR), IT personnel, or users to obtain sensitive information.

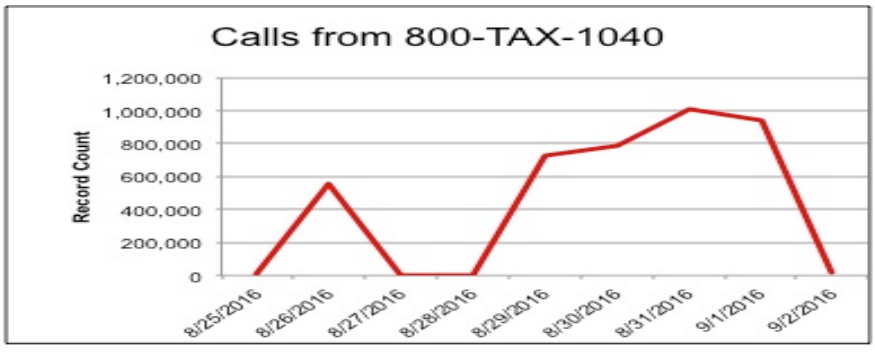
The chart below provides an illustration summarizing the current threats we see in real-world enterprise voice networks and how they relate to one another in likelihood and relative severity/impact.

As you can see from this illustration, both nuisance and malicious robocall activity is increasing rapidly in relation to other voice network threats, likely because of their ease of execution.



These attacks affect virtually all users of the PSTN, including consumers using mobile devices and landlines, consumers at their places of business, small business users, and enterprise users. Attackers often target the most vulnerable users with the least security, such as the elderly who are often using older mobile phones or landlines, which are very difficult to protect (and no one is incented to protect them). Attackers obtain various number lists and use robocalls and other techniques to reach their victims.

The IRS scam is just one example of a robocall scam. The U.S. Treasury Inspector General for Tax Administration (TIGTA) has communicated to us that this issue alone cost users more than $50M in 2016. Addressing this scam, not to mention others, will have a significant financial benefit to consumers. In our work with Verizon, we have seen attackers commonly use the 1-800-TAX-1040 number, because it results in a caller ID of "IRS" being presented to the consumer. Verizon recorded traffic spikes of up to 1,000,000 calls per day in August 2016. The chart below shows data on actual traffic entering the Verizon network (which is just one of many networks):



Expect attackers to come up with more scams over time. Attackers will also use spear vishing techniques to target specific users, similar to the "whaling" attacks occurring over email. The attacker will use calling number spoofing.

We are already seeing this to some degree with bomb threats, where the attacker uses robocalls to find a source number from which the victim will answer a call (to defeat whitelists) and then uses text-to-speech software to interact with the victim.

Generating Robocalls

There are several ways to generate robocalls attacks. There are commercial auto-dialing products, robocall dialing services such as Call-Em-All, and free software. It is easy to use tools such as the Asterisk IP PBX, the sipp call generator, and other freeware tools to automatically generate calls. These tools make it possible to generate millions of calls. These tools also make it trivial to spoof the calling number to any value the attacker wants. A brief summary of how to generate robocalls is as follows:

- Select the phone numbers to dial. These numbers can be purchased, guessed at, or even based on a public resource such as the Do-Not-Call-List.
- Install and configure the Asterisk or other open source/free IP PBX software. These systems require nothing more than a capable Linux server. There are many resources on the Internet that describe how to set them up.
- Set up a call generator, which uses the underlying Asterisk software to make the calls. During this process, the attacker can set victim numbers, chose how to spoof the calling number, decide what audio to play, choose the call rate, etc. Asterisk can also be used to detect when a human answers the call, such as when they select DTMF to transfer the call to a human.
- Determine a calling number spoofing strategy, which may be to spoof to a recognized number, such as 1-800-TAX-1040, local numbers, familiar numbers, or just random numbers in a particular area code or exchange.
- Make the calls when they will be the most effective, such as during the early evening on consumer land lines, any time of the day on mobile devices, or during business hours for employees.

Existing Countermeasures

The current state of the art in robocall mitigation is primarily managed blacklists, available primarily for VoIP-based landlines and common smartphones from vendors such as Apple and Google.

Managed Blacklists

Most of the vendors providing these lists use a similar process, that being to maintain an active blacklist and block arriving calls on that list. The vendors update these lists as a function of the traffic they monitor and based upon comments from their users. These solutions work pretty well when they are available, but are not widely available to some POTS landline users, less popular mobile devices, and businesses and enterprises.

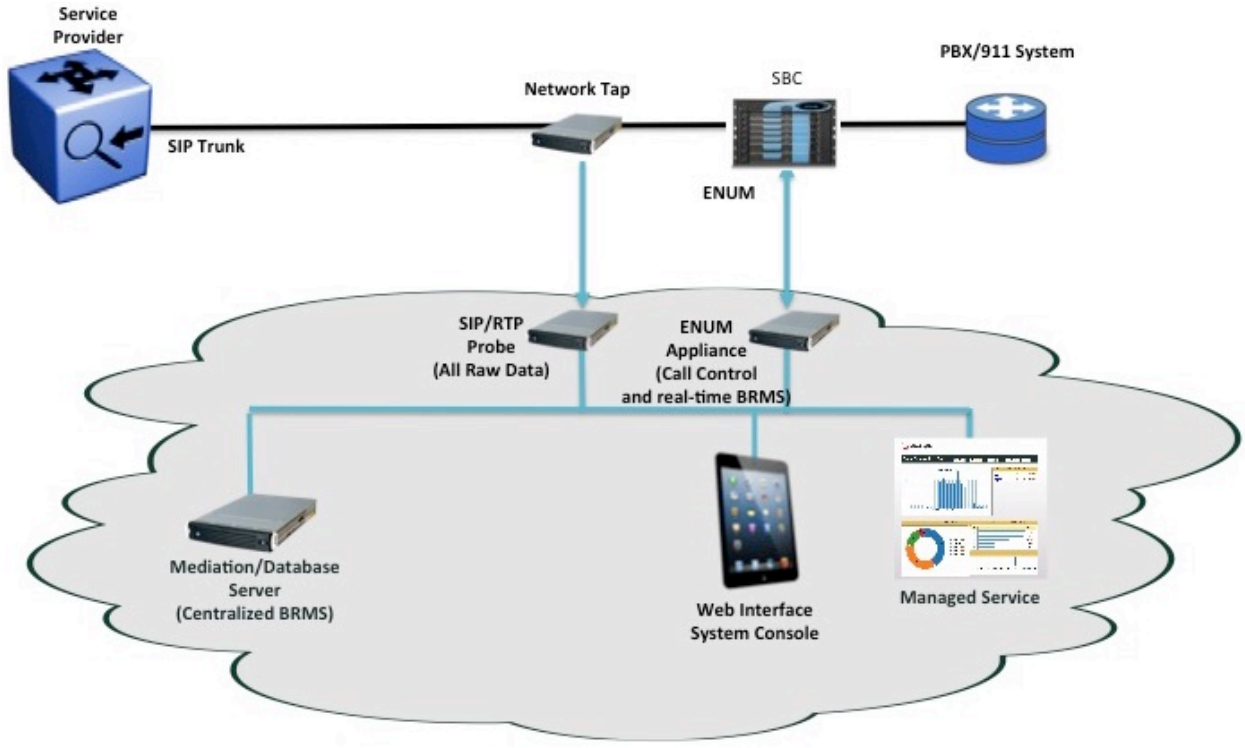
The biggest challenge with blacklist approaches is that they do not work for new calls that are not on the list and also calls which use randomly spoofed calling numbers. The robocallers know about the blacklists and if they really want to deliver a call, they either know what numbers are on the blacklist or can easily probe to find out.

Service Providers

Service providers are working on solutions such as the Internet Engineering Task Force (IETF) Secure Telephony Identity Revisited (STIR) Request for Comment (RFC), do-not-originate approaches, and Alliance for Telecommunications Industry Solutions (ATIS) SHAKEN. However, it is our opinion that these solutions will take years to be broadly implemented.

Solutions

SecureLogix offers solutions to mitigate robocalls. Our enterprise-focused solutions address the various forms of robocalls. In addition, we are working with service providers and with the Department of Homeland Security (DHS) to improve our solutions to address calling number spoofing. Our solutions can be deployed in SIP and TDM networks, support large and small sites, and have very flexible polices that are used to detect and mitigate robocalls. Our solutions integrate with common network infrastructures such as Cisco routers and SBCs through network interfaces, also allowing for a cloud-based deployment. A high-level architectural diagram of our high-capacity SIP solution is shown below.



Our solutions allow new business rules and policies to be built without impacting the underlying software. All of the call attributes and, in the case of VoIP, SIP signaling attributes are available to feed new business rules. The solutions offer call control options and support for semi-static and dynamic white and black lists. A set of network queries, to include source phone number checks, number type checks, and queries to call authentication services are also available. This allows any combination of business rules for different signatures, vertical requirements (such as health care, emergency services, or financial services), or specific customers to be built without changing software.

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 (210) 402-9669 • www.securelogix.com