REDSHIFT NETWORKS

Unified Communication Threat Management

The Growing Threat of Robocalls in the U.S.

CARRIERS TURN TO UNIFIED COMMUNICATION THREAT MANAGEMENT TO KEEP CUSTOMERS SAFE FROM SCAMS

Your phone rings. You see it's a local number, so you answer. But it is not one of your friends or neighbors on the other end. Instead, you hear a mechanical voice telling you about a contest you supposedly won or trying to sell you something you don't need. It is a robocall – a problem that has aggressively spread across the U.S. in recent years.

Robocalls are automated messages delivered via a computer system. They automatically play a message whenever the person being contacted answers their phone. These messages can be about anything from telemarketing scams to political campaigns to appointment reminders.

The FTC said that in 2018 it received about 400,000 complaints about robocalls every single day. Some of these are "legitimate" calls like reminders from pharmacies and messages from libraries and schools, but a growing number of them are scams aimed at defrauding unassuming people of their hard-earned money.

AN EXPLODING EPIDEMIC

To say this phenomenon is growing would be a gross understatement. Its exponential surge has reached epidemic proportions due to the ease and low cost of deployment.

With robocalls hitting more and more carrier and enterprise customers and consumers by the day, carriers are scrambling to stay ahead of the problem. However, the technology is cheap and easy to use due to Voice over Internet Protocol (VoIP), which allows scammers to make billions of automated calls. Out of those billions of calls, only a small percentage of people need to respond for the deception to pay off. According to the FTC, scammers made an average $430 per successful phone call in 2018.

Criminals have latched on to the profitable world of robocalling, so much so that an ecosystem has developed in which people will pay top dollar for phone lists that can generate the best results in a robocall campaign. Robocallers from other countries are also now tapping into U.S. telephone networks to reach their victims.

ASSESSING THE IMPACT

Based on industry reports, it is estimated that in 2018 the average American was inundated with more than 20 spam phone calls per month. And that number is growing exponentially. What's worse, Consumer Reports states that robocalls often target vulnerable populations such as the elderly, who are "harassed into buying worthless products and services they did not want or need."

To limit the damage, most wireless carriers have adopted a security protocol called SHAKEN/STIR, which limits the number of robocalls hitting their networks and verifies that the number displayed on caller ID is the same number that initiated the call. When a call does not actually come from the (often local) number displayed on caller ID, it is referred to as "spoofing," a common practice among robocalling scammers.

SHAKEN (Secure Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited) work to ensure that calls traveling through interconnected phone networks have their caller ID established as legitimate by originating carriers and validated by other carriers before reaching consumers. The Federal Communications Commission (FCC) has worked to make progress in call authentication through the implementation of SHAKEN/STIR to strengthen call-blocking and unmask spoofed calls. In November of 2018, FCC Chairman Ajit Pai instructed carriers who had not yet done so to protect their consumers by using SHAKEN/STIR "without delay," and most have committed to an accelerated timeline to meet that directive.

REDSHIFT NETWORKS

CARRIERS KEEP CALLS LEGITIMATE WITH REDSHIFT

RedShift Networks has worked tirelessly to stay ahead of the robocall curve and protect carrier and enterprise customers and consumers from spoofed calls and other scams. The company uniquely implements SHAKEN/STIR standards with SBCs, and promises to both block the majority of current scam robocalls and stem the tide of likely robocall mutations.

RedShift UCTM RoboCall Protection with STIR/SHAKEN

However, RedShift Networks fundamentally believes that SHAKEN/STIR doesn't go far enough. There is no verification mechanism within the protocol to ensure that the call passed to the downstream/upstream carrier is a "GOOD Caller." Therefore, in addition to implementing SHAKEN/STIR, RedShift Networks validates the caller by integrating its unique Unified Communications Threat Management (UCTM) patented technology to guarantee that the caller is legitimate.

RedShift's UCTM platform establishes a baseline for normal voice traffic deep at the SIP/VoIP protocol level, and applies unique algorithms to verify and authenticate legitimate users and traffic flows. Once established, anomalous VoIP/SIP traffic levels or call attempts from unregistered users are dynamically blocked.

UCTM FEATURES OFFERED BY REDSHIFT

User Fingerprinting: Each user has unique SIP characteristics and is "fingerprinted" by the system (by calling number).

User Behavioral Analysis: UCTM learns the calling patterns for each user.

Individual Reputational User Scoring System: UCTM assigns a "score" to each user based on their reputation. Has the user account been hijacked before? Has the user account caused any robocalls before? Has the user account had any type of alarms or failures before? UCTM's scoring system answers these questions. RedShift Networks also uses Machine Learning and AI algorithms on the network traffic data sets collected. Overall, the UCTM Robocall solution can identify robocalls in real time with 99.99% accuracy.

RedShift Networks Cloud: The robocall database is continuously updated with banned phone numbers. The Global SIP BotNet Updates blocks millions of Automated Botnets (compromised servers) sitting in networks around the world that target Carriers and Enterprises and generate these robocall attacks.

RedShift offers many other unique and patented algorithms to detect robocalls and SPAM through a solution that curbs these malicious calls, protects consumers, and keeps criminal robocallers at bay.

The UCTM platform intelligently correlates SIP Security, Threat Intelligence Analytics and Fraud Detection to give operators real-time, context-driven visibility into unauthorized activities and mitigate threats including Denial of Service (DoS), botnet attacks and robocalls throughout their VoIP network.

REDSHIFT STOPS ROBOCALLERS AND SAVES CARRIERS MONEY

RedShift's VoIP security module protects against more than 40,000 different threats and attacks, with real-time monitoring, detection and mitigation of robocall activity. The result is 80 million daily robocalls eliminated from the network – saving customers vast amounts of both time and money.

Based on projected growth percentages, robocalls are not going anywhere anytime soon. In fact, the problem will likely get much worse before it gets better. RedShift offers a solution that curbs these malicious calls, protects consumers, and keeps criminal robocallers at bay.

Please visit www.redshiftnetworks.com for additional information.