REDSHIFT NETWORKS

UCTM AND THE VoIP THREAT INTELLIGENCE NETWORK

National Cable Operator Uses RedShift Networks to Proactively Block Attacks

ABOUT THE CUSTOMER

This National Cable Operator operating as a MSO (Multi Service Operator) offers diverse network capabilities to tens of millions of subscribers throughout more than 500,000 square miles in one of the larger countries in the world. The MSOs multiple divisions and network operations make it a leading player in the market. This Operator aggressively pursues new customer acquisitions offering promotions, special pricing, and invests heavily in new infrastructure to build a world-class multi-channel network..

THE PROBLEM

The Operator's network offers are increasingly exposed to network security issues related to fraud and cyber attacks due to its rapid expansion and new network deployments. Fraud loses run into the millions of dollars annually and as the network migrates to an all IP core and specifically Session Initiation Protocol (SIP) for their call flows. Using SIP, the attacks became more frequent and costly. Initially, the Operator acquired a CDR (Call Detail Record) based reactive fraud solution to stem security issues. This was ineffective and the MSO founds itself still hemorrhaging revenue due to the fraud losses since the CDR system was simply reactive and only provided alerts after the call theft of service was complete.

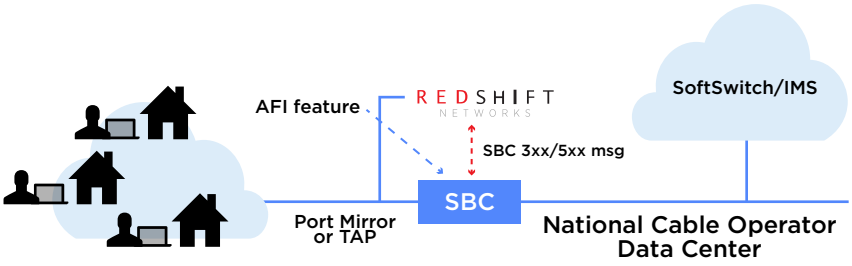
They were also concerned about suspected insider attacks and threats by malicious employees. CDR-based solutions only provide rear-view mirror insight, lack real-time detection and blocking to prevent costly attacks. This MSO's operations teams realized a CDR system did not meet their needs for real-time alerting and mitigation. The MSO also realized that it needed a more IP and SIP centric view of the attack flows to build a broader profile of the attacks and attackers, and more effectively block the threats. The MSO had also built an expensive fraud response team to manually block fraud and attacks. Attacks occur every hour of the day or night including the weekend and cause strain on the network resources needed to manually monitor the network.

RedShift Network's software, AFI intelligence and SIP Botnet Threat Intelligence feed helps this MSO proactively block attacks coming from known SIP Bots from around the world.

THE SOLUTION

In the midst of its search for a world-class solution to quickly arrest its revenue loss due to the fraud and cyber security VoIP/SIP attacks, the Operator contacted RedShift Networks. RedShift Network's Unified Communications Threat Management (UCTM) software proactively detects and thwarts more than 40,000 SIP/VoIP attack vectors to prevent MSO service fraud. After a successful UCTM evaluation, the product was immediately deployed in their production network. The UCTM software was installed across a large national footprint and corresponding service areas.

The MSO enabled RedShift's UCTM auto mitigation and remediation to reduce eyes-on-the-glass and overhead. This automation element frees up their Network Operations Teams engineering resources and fraud teams by relieving them from constantly having to monitor and manually block fraud and cyber attacks saving hundreds of thousands of dollars.



RedShift Networks UCTM Technology with Advanced Fraud Interdiction (AFI)

RedShift Network's team works closely with the Operator to implement RedShift's AFI (Advanced Fraud Interdiction). Under normal SIP call processing flows, AFI ensures bad calls or fraudulent calls are blocked. AFI intelligence allows the RedShift UCTM to communicate directly with the SBC (Session Border Controller) and proactively block bad callers and fraudulent callers in real-time while the call is in process.

RedShift Network's patented UCTM technology and algorithms block SIP/VoIP Cyber attacks and fraud with near zero false positives protection. The MSO annually saves hundreds of thousands of dollars in blocking theft of service and malicious attacks automatically without human intervention.

Other SIP/VoIP attack vectors identified and blocked using RedShift Networks software and AFI intelligence in the National Cable Operators network include:

- Illegal User Agent Attacks
- SIP Botnet Attacks
- Robocalls (STIR/SHAKEN Compliant)
- Call Spoofing Attacks
- Call Hijacking Attacks
- SIP Attacks from inside and outside the network
- War Dialing Attacks
- Telephony DOS Attacks (TDoS)
- Illegal calls made to international destinations
- SIP Fuzzing Attacks
- Registration Attacks
- and hundreds of other SIP Attacks

RedShift Network's software, AFI intelligence and SIP Botnet Threat Intelligence feed helps this MSO proactively block attacks coming from known SIP Bots from around the world.

THE NATIONAL CABLE OPERATOR NEXT STEPS

Reviewing RedShift's UCTM Threat Intelligence Analytics module to perform forensics, troubleshooting, and debugging functions, and detect bottlenecks on SIP traffic flows.