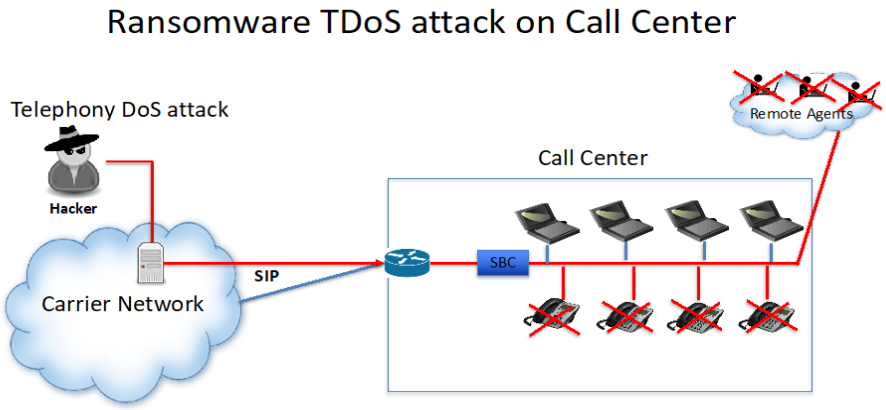
RSN Security Advisory – August 3rd, 2020

RANSOMWARE ATTACKS ON CALL CENTERS

Recently we were made aware of a Ransomware attack on a major US next generation carrier's enterprise customer's Call Center. The attacker demanded a payment of 15 bitcoins (approximately US$150,000) otherwise the attacker would conduct a Telephony Denial of Service (TDoS) attack on the Call Center and shut it down.

The Call Center operations are an essential part of this large enterprise's business. If their Call Center were shutdown, they would potentially lose millions of dollars in revenue. Once aware of the situation the carrier contacted RedShift Networks with the details of the attack seeking help to resolve the situation.



RedShift Network's unique Unified Communications Threat Management (UCTM) software protects networks against over 40,000 different types of VoIP and Video attacks, including TDoS attacks. There are different types of DoS attacks and the SIP protocol allows attackers to easily manipulate packets to generate different attack vectors. Examples are rate based DDoS attacks and Stealth based DDoS attacks. Stealth based DDoS attacks are harder to track as they are low frequency attacks that can bring down specific segments of the network without affecting other parts of the network. RedShift Networks has patented granular algorithms that can detect and thwart a host of unique SIP based DoS attack vectors. SIP is an accepted and widely used protocol based on over 43 IETF RFCs. SIP messaging methods can be used to generate a TDoS or DDoS attack. These types of TDoS attacks can quickly bring down a call center and can cause havoc and loss revenue to an enterprise whose business depends on their call center operating at peak performance.

To resolve the issue, RedShift Networks installed their UCTM software in the carrier and enterprise customer networks to protect them from future TDoS attacks and the other potential 40,000 VoIP threats and attacks that may be next.