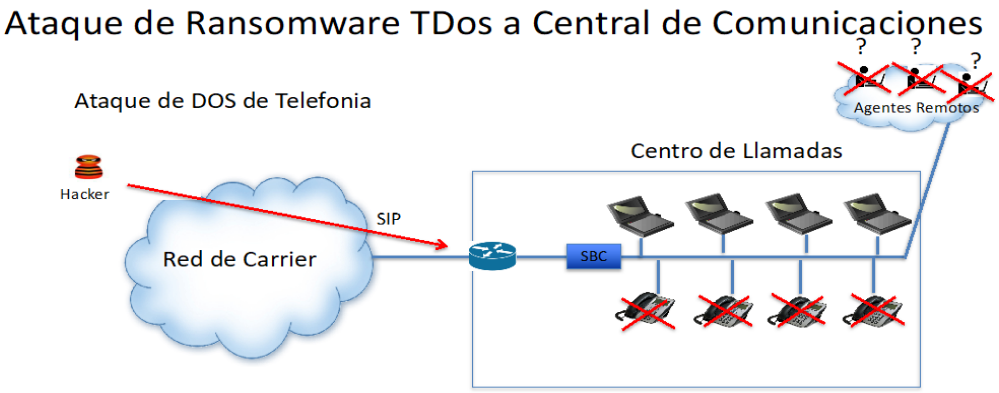
RSN Security Advisory – Agosto 3rd, 2020

Ataques de Ramsomware en Centrales de llamadas

Recientemente nos dimos cuenta de un ataque de Ransomware a la Central de llamadas de un cliente empresarial de un importante operador de próxima generación en Estados Unidos. El atacante exigió un pago de 15 bitcoins (aproximadamente US$150.000) o de lo contrario, el atacante llevaría a cabo un ataque de denegación de servicios de telefonía (TDoS) en la central de llamadas y la cerraría.

Las operaciones de una Central de Comunicaciones son una parte esencial de las grandes empresas de negocios. Si la Central de Comunicaciones se cerrara, ellos potencialmente perderían millones de dólares en ingresos. Una vez consciente de la situación, el Carrier se comunicó con Redshift Networks con los detalles del ataque en busca de ayuda para solucionar la situación.



El Software de Redshift Networks Unified Comunications Threat Management (UCTM) Manejo de Comunicaciones unificadas protege a las redes contra más de 40.000 diferentes tipos de VoIP y ataques de video incluyendo los ataques TDos . Hay diferentes tipos de ataques DoS y el protocolo SIP permite a los atacantes manipular fácilmente paquetes para generar diferentes vectores de ataques. Los ejemplos son ataques DDoS basados en calificaciones y ataques DDoS basados en sigilo. Las pistas DDoS basadas en sigilo son más difíciles de rastrear ya que son ataques de baja frecuencia que pueden derribar segmentos específicos de la red sin afectar otras partes de la red. Redshift Networks ha patentado algoritmos granulados que pueden detectar y frustrar una gran cantidad de vectores de seguimiento DoS únicos basados en SIP. SIP es un protocolo aceptado y ampliamente utilizado basado en más de 43 IETF RFCs. Los métodos de mensajería SIP que se pueden utilizar para generar ataques TDoS o DDoS. Estos tipos de ataques TDoS pueden derribar rápidamente un centro de llamadas y causar estragos y pérdidas de ingresos para una empresa cuyo negocio depende de que su Central de llamadas funcione al máximo rendimiento.

Para resolver este problema, Redshift Networks instaló su software de Comunicaciones Unificadas en el operador y en las redes de sus clientes empresariales para protegerlos de futuros ataques TDoS y las otras 40.000 amenazas y ataques potenciales de VoIP.