RSN Security Advisory – March 21st, 2020

RISE IN VOICE ATTACKS ON A GLOBAL LEVEL DURING COVID-19 PANDEMIC

Towards the end of the month of January and into February in 2020, RedShift Networks saw a heightened increase in Voice/VoIP/SIP attacks on a global scale around the world. As the world and companies were rapidly moving towards a remote workers environment, the hackers were very busy in targeting enterprises around the world. This increase in attacks was also seen in general cyber security world, as most cyber security companies around the world noted a heightened level of threats and attacks on their customers networks and services. This is very typical in the Cyber Security world, were hackers take advantage of the chaos and mayhem that this pandemic has caused to seek vulnerabilities and weaknesses in enterprise and carrier networks.

In this particular case, enterprises were left to the 'security levels' in their employees personal or work PCs to protect their networks and thwart against these attacks. Enterprises typically have robust security postures to protect their core data enterprise services but it's difficult for them to provide the same level of security to their remote workers.

Specifically, in the voice and real time applications aspects, RedShift Network's Condor Labs has found:

1) **Increase in telecom fraud attacks on a global scale,**
   - We are seeing a heightened level of telecom fraud attacks to our customers with more frequent and sustained attacks from around the world.

2) **Increase in SIP BotNet attacks from around the world,**
   - RedShift Networks has a SIP Botnet threat intelligence feed and we've seen a heightened level of activity from these SIP Botnets from around the world. Botnets are hijacked servers in enterprises or hosting services– We're seeing primarily these attacks coming from the US, Canada, France, United Kingdom, Netherlands, Russia, China, Vietnam, Lithuania, Iceland and Laos.

3) **Increase in the types and variances of voice/real time application attacks,**
   - RedShift Networks protects against more than 40,000 attacks - RedShift is seeing more and more different types of attacks exploiting the SIP and VoIP protocol. This shows the enhanced sophistication of the voice/real time attackers as they look to exploit weaknesses in enterprise and carrier customers.

4) **Increase in domestic traffic call patterns for voice/real time networks that merit better threat intelligence analytics tools (& performance management) due to the sudden increase in traffic patterns.**

However, enterprises have reacted rapidly and have accelerated the deployment of data security measures to their remote assets and their remote employees. The concept of a mobile worker has come to full force and will continue to be so for the foreseeable near-term future until the medical community can come with a vaccine where everyone feels safe.

In the same way that enterprises and carriers have beefed up their data security postures, they need to rapidly enhance their voice and video security postures. Voice and video applications are prone to a huge set of attacks that are not prevalent in today's traditional data security centric products in the marketplace.

RECOMMENDATION

RedShift Network's recommends that enterprises and carriers move quickly to enhance their security postures for voice and video applications/networks today as these voice/real time attacks are getting more sophisticated and are global in nature. RedShift Network's UCTM (Unified Communications Threat Management) technology specifically targets the voice and real-time aspect of an enterprise and carrier network, and thwarts/protects against more than 40,000 different types of voice/real-time application threats and attacks.