R E D S H I F T
N E T W O R K S

RSN Security Advisory – May 21st, 2020

RISE IN VOICE CONFERENCE JOIN ATTACKS DUE TO COVID-19

EXECUTIVE SUMMARY

As employees of enterprises started to work from home due to mandates from their employers and government orders since late February, 2020, there is a huge rise in communications via video and voice conferencing. With this rise in work habits, cyber criminals have also adapted to this new reality with glee as home users are easier to hack into due to typically weak security practices on the home front. Many of the attacks have been specifically on these voice and video communications and conferencing systems which inherently have weak security implementations as they were never meant for mass market global use.

This SECURITY ADVISORY discusses the new threats that enterprises face as their employees use their voice and video conferencing systems from remote locations. Many of the attacks center around illegal join of conferences which is easily possible due to weaknesses in these conferencing and collaboration systems. The most recent well-known attack was the "Zoom Bombing" incidents facing the users of Zoom.

This demonstrated the real-world weaknesses of these collaboration systems.

TECHNICAL ANALYSIS OF ILLEGAL JOIN CONFERENCING ATTACKS

This is a method of attack by which the hacker takes advantage of SIP messaging to join a conference call illegally. This can have detrimental effect on the enterprise as an unknown party or hacker can be listening in to very sensitive and confidential conferences where the CEO or CFO may be discussing very important information about the company.

In SIP, the anyone can join a call with the right credentials by using the SIP JOIN method. The JOIN method defines a 'User Agent' field which the customer uses to join the call. The hacker can put in ANY User Agent to JOIN the conference call. If the hacker was sitting on a soft client in another part of the world, he could join a legitimate company conference call without anyone knowing about this.

Therefore, RedShift Network's UCTM, checks to ensure that the User Agent used and the person trying to join the conference is legitimate. If someone registered with a Polycom phone into the enterprise network, and if he tries to enter a conference with a different phone type (User Agent), the RedShift UCTM would flag this and can block the entry into the conference, among other checks & verifications.

In that way only legitimate parties can enter into voice and video conferences.