Tapping IP Phones In Sensitive Locations

Industry: Financial Services

Attacker Objective

Blackmail and ransom

Background

A major consumer finance institution in the U.S. with more than 17,000 IP phones on its network used the Arista NDR platform to determine that four of its phones were being electronically tapped.

The organization's large security team struggled with visibility into the IP phones since existing security controls were blind to these devices. They also exist for the sole purpose of communicating with destinations outside the company, so large volumes of traffic being exchanged with external sources is not unusual. However, it was unusual that only a small number of phones were uploading data to a particular suspect destination every so often.

Arista NDR detected this threat by:

- Identifying the phones and comparing their behaviors to the cohort of phones over time.
- Analyzing behaviors of IP phones in the environment to spot outliers.
- Using encrypted traffic analysis to profile the source and destination of the communication.

Why Arista NDR?

Arista NDR detected 4 IP phones (out of more than 17,000) that were uploading data to a suspect destination. Using Arista NDR, the security team determined that an IT employee was responsible for this attack. He was attempting to obtain information to be used in blackmail and ransom operations. The detailed information gained from the NDR platform enabled the company to immediately stop the activity and gain evidence for legal action.

The analysis enabled the security team to quickly find the compromised phones. The phones in question were stationed in executive conference rooms and other sensitive locations that were frequently the site of high-level and sensitive company discussions.

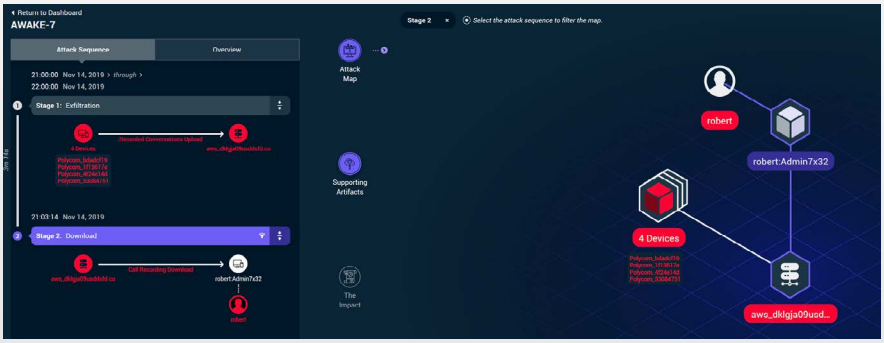

Figure 1: Threat correlation and visualization Attack Map.

To find this activity, Arista NDR's analytics did not simply compare the current behavior of these devices to what it observed in the past. In this case, the devices were compromised long before Arista NDR was deployed in the environment. A more basic anomaly analysis offered by a traditional security solution would have considered the malicious activity to look "normal" compared to what had been previously observed.

Arista NDR first identified all of the devices with similar behavioral fingerprints and then compared these devices to each other. This allowed it to spot four devices that deviated from the norm.