Contractor Using Security Cameras to Spy

Industry: Energy

Attacker Objective

Corporate espionage

Background

Surveillance cameras are common devices in any large enterprise, especially those in critical infrastructure industries. An Arista NDR customer in the energy industry had thousands of these cameras on its network and learned that a contractor was using them to spy on employees in sensitive locations.

Arista NDR detected this threat by:

- Automatically profiling all devices on the network including the thousands of IP cameras.
- Detecting a single camera that was communicating with a destination network that none of the other cameras were interacting with.
- Identifying one other device that had accessed the same destination in question—a device in use by an IT contractor.

Why Arista NDR?

The security team found multiple cameras that were impacted by the malicious activity, including some in data centers and secure facilities for managing critical infrastructure. The team determined nearly all of their cameras were badly configured, giving the attacker easy access to any of them. This customer is an ongoing nation-state target, so identifying this part of their attack surface was critical.

While a detailed investigation like this could typically take days, it was completed in minutes with Arista NDR. And ultimately, Arista NDR turned intelligence generated during the investigation into actionable protection for the organization.

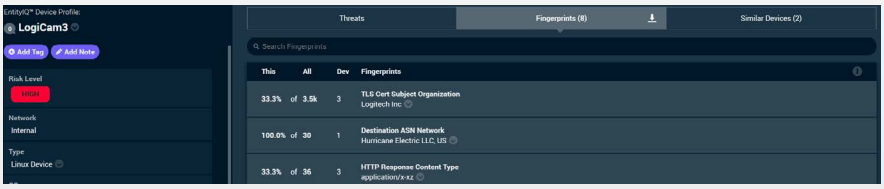

Figure 1: After clicking on a link, users were directed to this page which looked like a Microsoft SharePoint login but was harvesting credentials and sending them to the attacker.

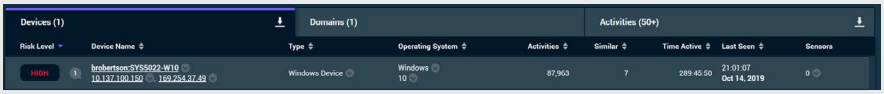

Figure 2: The look-alike Microsoft SharePoint login page had an embedded password-stealing script.

Identifying what is on the network is a critical first step to securing it, especially as people bring their own devices to work and the number of Internet of Things (IoT) devices steadily increases. The Arista NDR platform automatically identifies and creates profiles of all devices on a network – which in this case, included thousands of IP cameras.

Importantly, these cameras had been compromised before the organization began using the Arista NDR platform. For other security solutions that baseline "normal" activity, this would be a challenge because they wouldn't see anything anomalous about activity that was present before they got there. However, the method of profiling each entity and comparing the activity of entities most similar to each other made a significant difference.

Specifically, the solution identified one camera that was communicating with a destination network that none of the other cameras were communicating with. Additionally, this led to the identification of malicious communication occurring over FTP. The security team was able to retrieve the FTP credentials and find only one system on the network that had accessed the same FTP server in question—a device in use by an IT contractor.