Contractor Using Security Cameras to Spy

Industry
Energy

Attacker Objective
Corporate espionage

Awake detected this threat by:

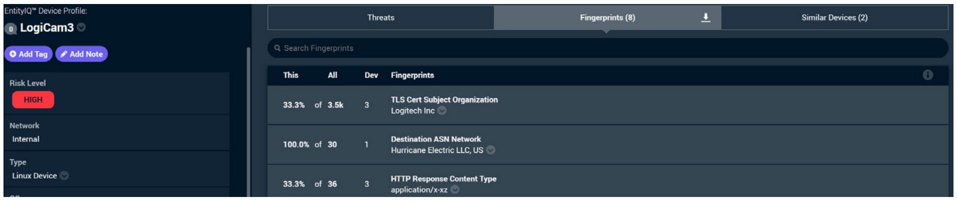
- ✓ Automatically profiling all devices on the network including the thousands of IP cameras.
- ✓ Detecting a single camera that was communicating with a destination network that none of the other cameras were interacting with.
- ✓ Identifying one other device that had accessed the same destination in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

Surveillance cameras are common devices in any large enterprise, especially those in critical infrastructure industries. One Awake 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.

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 Awake Security 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 Awake 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, Awake's method of profiling each entity and comparing the activity of entities most similar to each other made a significant difference.

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



EntityIQ™ Device Profile:
0 LogiCam3

Risk Level
HIGH

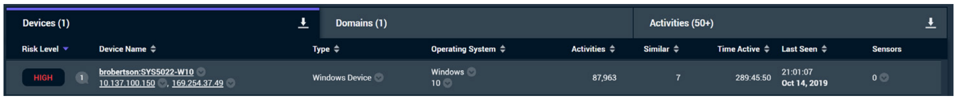
Network
Internal

Type
Linux Device

This		All	Dev	Fingerprints
33.3%	of	3.5k	3	TLS Cert Subject Organization Logitech Inc
100.0%	of	30	1	Destination ASN Network Hurricane Electric LLC, US
33.3%	of	36	3	HTTP Response Content Type application/x-xz

Awake identified an unexpected network connection from an IP camera.

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.



Risk Level		Device Name	Type	Operating System	Activities	Similar	Time Active	Last Seen	Sensors
HIGH	1	brobertson:SYS5022-W10 10.137.100.150, 169.254.37.49	Windows Device	Windows 10	87,963	7	289:45:50	21:01:07 Oct 14, 2019	0

Identifying the malicious contractor by isolating devices that connected to the FTP location.

For additional information about Awake please visit awakesecurity.com

AWAKE