ARISTA

Case Study

Employee Selling Corporate Secrets

Industry: Media and Entertainment

Attacker Objective

Profit from selling intellectual property

Background

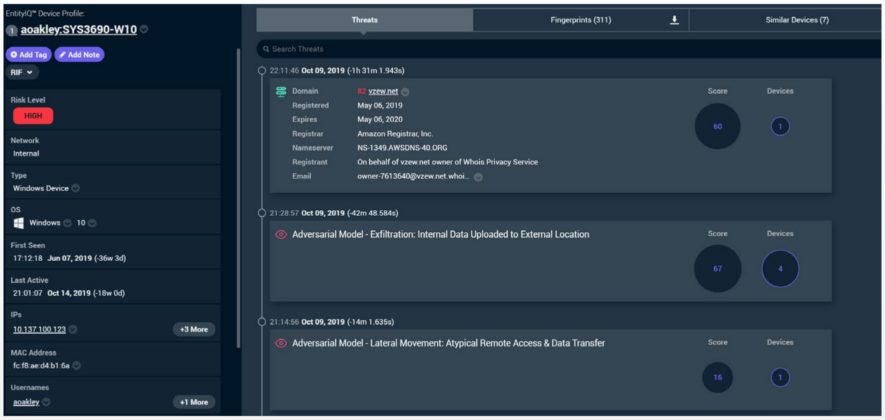
An employee at a large media and entertainment company was caught selling extremely sensitive intellectual property to a third party.This type of activity is especially hard to detect using traditional tools such as threshold-based solutions that look for large or anomalous uploads. In this case, the files were sent infrequently, and when they were sent, the amount of data traversing the network was very small.

In addition, this was a case where the perpetrator was authorized to access the information he was sharing. The files in question were sent to this person's corporate email account from others within the organization. And the person did not forward or send all of the attachments contained in any given email. The files sent were selective and very specific, making the perpetrator's actions unlikely to trigger alarms that typically look for periodic or continuous uploads.

While the amount of data being uploaded was small and usually only occurred a handful of times per week, Arista NDR identified the activity as "persistent" and "unique," worthy of a closer look.

Why Arista NDR?

This is the type of "low and slow" activity that most other solutions miss. However, Arista NDR allowed this organization to identify the activity because of its ability to compare this user's behavior to those most similar to it. Ultimately, the evidence presented by Arista NDR allowed the organization to pursue legal action.



EntityIQ™ Device Profile:

aoakley:SYS3690-W10

Risk Level: HIGH

Network: Internal

Type: Windows Device

OS: Windows 10

First Seen: 17:12:18 Jun 07, 2019 (-36w 3d)

Last Active: 21:01:07 Oct 14, 2019 (-18w 0d)

IPs: 10.137.100.123 +3 More

MAC Address: fc:f8:ae:d4:b1:6a

Usernames: aoakley +1 More

Threats | Fingerprints (311) | Similar Devices (7)

22:11:46 Oct 09, 2019 (-1h 31m 1.943s)

Domain: 82 vzew.net

Registered: May 06, 2019

Expires: May 06, 2020

Registrar: Amazon Registrar, Inc.

Nameserver: NS-1349.AWSDNS-40.ORG

Registrant: On behalf of vzew.net owner of Whois Privacy Service

Email: owner-7613640@vzew.net.whoi...

Score: 60 Devices: 1

21:28:57 Oct 09, 2019 (-42m 48.584s)

Adversarial Model - Exfiltration: Internal Data Uploaded to External Location

Score: 67 Devices: 4

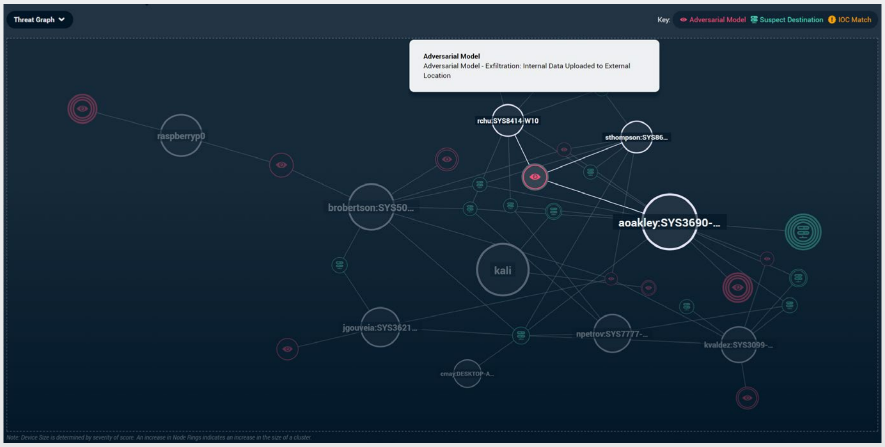
21:14:56 Oct 09, 2019 (-14m 1.635s)

Adversarial Model - Lateral Movement: Atypical Remote Access & Data Transfer

Score: 16 Devices: 1

Figure 1: Suspicious Activity Timeline

The device detail page in the Arista NDR platform shows a timeline with lateral movement, internal data transfer, and finally, data exfiltration. This enables threat hunters to understand the entire scope of the attack and trigger appropriate remediation measures.



Adversarial Model

Adversarial Model - Exfiltration: Internal Data Uploaded to External Location

Note: Device Size is determined by severity of score. An increase in Node Rings indicates an increase in the size of a cluster.

Figure 2: Dashboard highlights the risk based on the adversarial models triggered by the perpetrator's device.

Arista NDR detected this behavior as:

- It behaved differently as compared to any other device in the enterprise that interacted with the same destination domains.
- Persistent in that it occurred multiple times over a few weeks.
- Unique to a particular device or person when compared to other similar devices or people, such as those in similar job

arista.com

May 31, 2022