Employee Selling Corporate Secrets

In early 2018, an employee at a large media and entertainment company was caught selling extremely sensitive intellectual property to a third-party. This type of activity would be 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 being 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 an any given email. They were selective and only sent very specific files, making their actions unlikely to trigger alarms that typically look for large or continuous uploads.

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

This is the type of "low and slow" activity that most other solutions miss. However, Awake allowed this organization to identify the activity because of its deep analysis of all traffic crossing the organization's network. Ultimately, the evidence presented by Awake allowed the organization to pursue legal action.

Industry

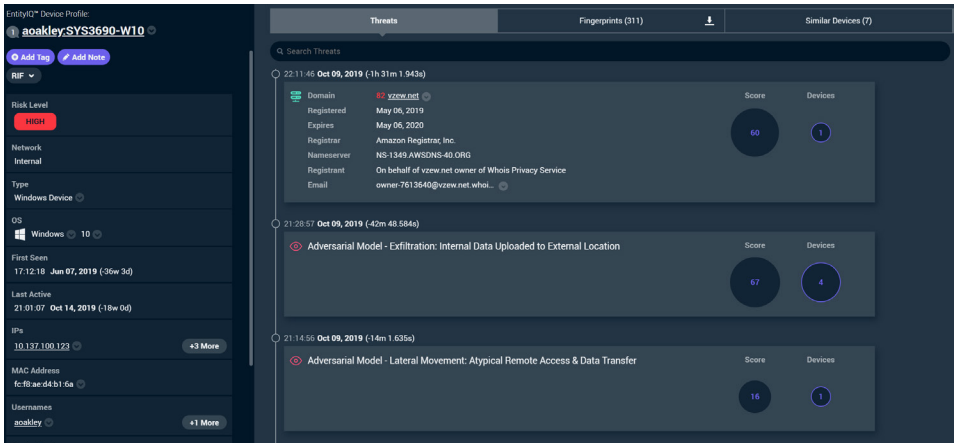
Media and Entertainment

Attacker Objective

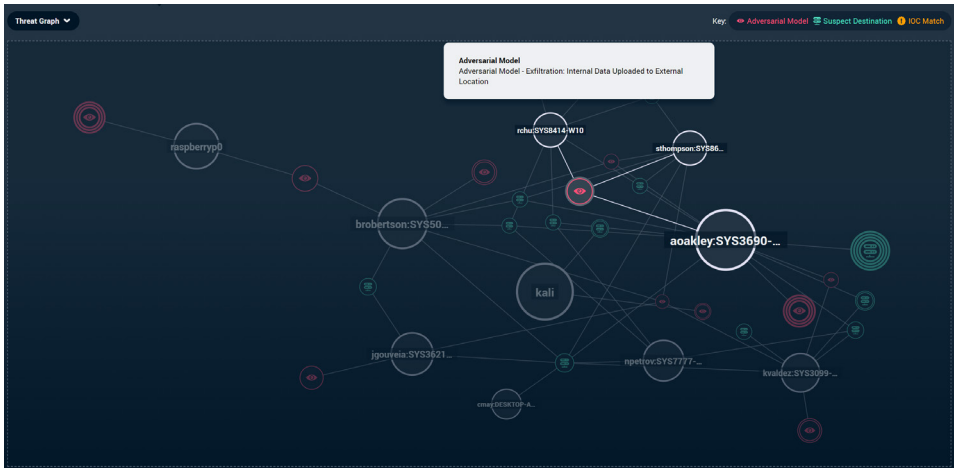
Profit from selling intellectual property

Awake detected this threat as:

- Rare when compared to any other device in the enterprise that interacts 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 functions.



The device detail page on Awake's platform shows a timeline with lateral movement, internal data transfer and finally data exfiltration.



The dashboard highlights the risk based on the adversarial models triggered by the perpetrator's device.

For additional information about Awake please visit awakesecurity.com

AWAKE