Spear Phishing Detection and Intelligent Response

Industry: Petroleum Refining

Attacker Objective

Access critical applications

Background

A small group of employees at a petroleum refining giant were targeted by a sophisticated spear-phishing campaign to steal credentials to access critical information and applications.

The targeted nature of spear phishing makes it especially dangerous because, most often, an organization does not become aware of compromised credentials until bad actors are already using them. This is because the people being "phished" willfully click on malicious links or provide credentials to attackers who have become exceedingly adept at spoofing emails to look legitimate. With so much information about a person's professional and personal lives available online publicly, it's increasingly easy for attackers to deceive their targets.

However, while spear phishing attacks vary based on the attacker and the target, certain tactics, techniques, and procedures (TTPs) are common in most attacks. For example, even targeted campaigns are rarely isolated to a single user, so once an email is delivered, a small number of users will typically "take the bait" and click on a link.

Why Arista NDR?

The security team was then able to take additional steps to further secure the organization. For example, the team was able to detect the use of compromised credentials on systems where they had not been previously used. Similarly, the team created a mechanism to automatically look for attacker attempts to use typosquatting, which typically requires complex manual efforts of forensic detection. With Arista NDR, this complexity is invisible to the analyst who simply invokes a function.

Ultimately, the organization stopped the phishing attack while taking proactive measures to ensure that stolen credentials could not be maliciously used while simultaneously teaching the system to look for similar techniques.

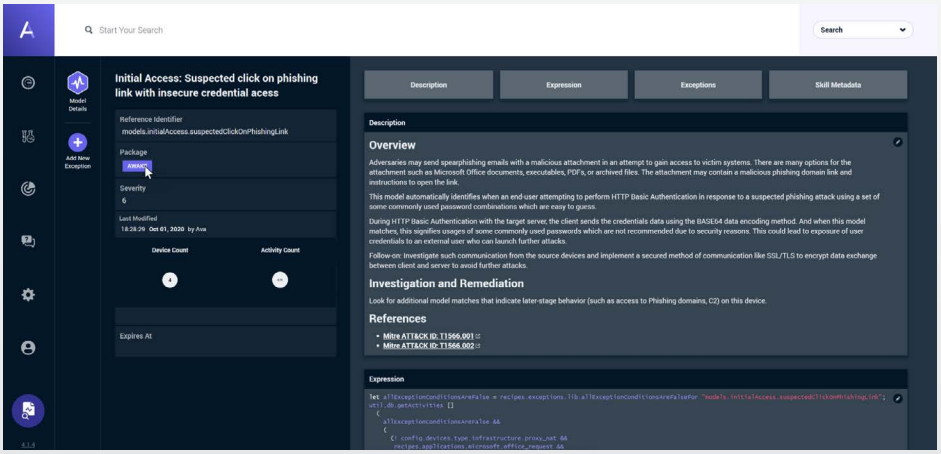

Fig 1: The solution allows analysts to quickly and easily create new detections to stop compromised credentials from being used in the future.

Arista NDR detected this threat by:

- Determining which users clicked on the link versus those who simply received the message but did not click on it.
- Identifying all the devices that communicated with the destination in question and jeopardized the users' credentials by using an insecure access mechanism.
- Generating a list of all the potentially compromised systems and required remediation.

The Arista NDR platform notified the security team as soon as it discovered the potential breach. The platform recognized that a small number of devices in the organization were visiting a destination domain identified as a suspected phishing site.