Spear Phishing Detection and Intelligent Response

Industry
Petroleum Refining

Attacker Objective
Access critical applications

Awake detected this threat by:

- Determining which users clicked on the link and submitted credentials, versus those who simply clicked the link and then closed the page.
- Identifying all the devices that communicated with the destination in question.
- Generating a list of all the systems where credentials that were now compromised had been used prior to the phishing incident.

A small group of employees at a petroleum refining giant were targeted by a sophisticated spear phishing campaign aimed at stealing credentials to access important 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 they're already being used by bad actors. This is because the people being "phished" willfully click on malicious links or provide credentials to attackers who have become extremely 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, there are certain tactics, techniques and procedures (TTPs) common in almost all attacks of this nature. 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.

At this customer, the Awake Security 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 that had not been previously seen on this network but also had other signs of being a suspect destination..

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 Awake, 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.

Awake allowed analysts to quickly and easily create new detections to stop compromised credentials from being used in the future.

For additional information about Awake please visit awakesecurity.com

AWAKE