Reactive Measures: Informing Threat Intelligence Team

In some cases, it is necessary for the investigating analyst to inform the threat intelligence team, if the organization has one in-house. This is typically conducted when there is an on-going and sustained phishing campaign against the organization, the phishing emails are extremely targeted towards the organization, or the attack is complex and the sharing of intelligence could benefit other organizations and help them to defend themselves. We will cover all three of these scenarios below.

SUSTAINED CAMPAIGN

If an organization is being bombarded by a continuous stream of phishing emails, there is an increased risk that an employee will open one and potentially compromise the company. Depending on the maturity of the threat intelligence team and the tools they have at their disposal, they may be able to predict how the campaign will continue and take actions to outsmart the attacks. If a pattern emerges based on the sending addresses used to push the malicious emails to employees, or with the domain names used to host malicious content, proactive blocking actions can be taken to stop future phishing emails before they're even sent.

TARGETED ATTACK

If a phishing attack or campaign is specifically targeted towards the organization, or even worse, spear-phishing specific employees, it is definitely time to let the threat intelligence team know. They can work with the victim(s) to provide specific support regarding being targeted, and can also conduct public exposure assessments to determine how much information is available publicly online about the target(s).

SOPHISTICATED ATTACK

If an attack is extremely sophisticated, gathering and sharing indicators of compromise (IOCs) with intelligence sharing partners, government, and even publicly can be a great move to help other organizations protect themselves and have the organization earn a good reputation amongst others for their approach.

CONCLUSION

Whilst it's not always beneficial to inform the threat intelligence team about phishing emails, in certain circumstances, they are able to provide more context, perform threat exposure checks, and share intelligence with

other organizations to help other network defenders prepare for, or take proactive measures to protect themselves.

Previous Topic
Mark Complete
Back to Lesson