LABYRINTH

CASE STUDY

Summary

During the Russian full-scale invasion, the Client, one of Ukrainian law enforcement agencies, faced unprecedented cybersecurity challenges. With heightened tensions and the increased likelihood of cyber attacks, the Client's infrastructure was under the highest risk of being targeted by sophisticated hacking attempts aimed at disrupting their operations, stealing sensitive information, and spreading misinformation. Ensuring the security of their digital infrastructure became paramount, requiring robust defense mechanisms and constant vigilance to safeguard against potential breaches and cyber espionage orchestrated by adversarial actors.

Client's Infrastructure:

- Up to 350 LAN hosts
- Up to 10 VLANs

Challenge

The Client's infrastructure contained a lot of data related to information of highly restricted access. It was necessary to strengthen the following areas of IS infrastructure: detection of potentially unwanted activity in the LAN, attempts of unauthorized access to internal systems, and detection and control of lateral movement in the killchain.

Realization

During the day, a stand of Labyrinth AdminVMs and one WorkerVM were deployed, to which all necessary VLANs in TRUNK were served. The file baits were placed only on servers in the infrastructure.

Solution

At the first stage, the types of decoys were deployed that maximally "fit" into the existing set of network systems/services and were most similar to the existing configurations in the network. After that, a variety of different test attacks were conducted, data on the detections/alerts created by Labyrinth was collected, and additional information related to the use of the existing Deception system in incident response was added to the overall infrastructure incident response plan.

The second phase significantly increased the number of decoy types, configured multiple custom decoy types and, based on the Moving Target Defense methodology, the set of network decoys was periodically regenerated. This gave additional dynamics to the infrastructure and increased the complexity of its exploration by the attacker.

Results

After covering a significant portion of the Client's infrastructure and utilizing a wide variety of different types of network decoys, an intruder of internal security policies was identified and began conducting blatant attack activities on SCADA decoys.

About LABYRINTH

Labyrinth is a team of experienced cybersecurity engineers and penetration testers, which specializes in the development of solutions for early cyber threat detection and prevention.

Deception techniques provide adversaries with an essential advantage over defenders, who cannot predict attackers' next move.

OUR VISION is to shift the balance of power in favor of defenders.

OUR MISSION is to provide all kinds of organizations with a simple and efficient tool for the earliest possible detection of attackers inside the corporate network.