CASE STUDY

Summary

The Client is a financial institution that performs special functions in guaranteeing individuals' deposits and removing insolvent banks from the market. Legal status - a legal entity under public law. The Client is an economically independent institution that does not seek to make a profit. The main task of the Client is to ensure the deposit guarantee system's functioning, remove insolvent banks from the market, and liquidate them.

Clients's main functions

- maintains a register of the participants;
- accumulates funds and monitors the completeness and timeliness of the transfer of fees by each member of the Company;
- takes measures to organize the payment of deposit compensation in case of a decision to revoke a banking license and liquidate a bank;
- regulates the participation of banks in the deposit guarantee system;

- takes measures to inform the public about the functioning of the deposit

  guarantee system, protect the rights and legally protected interests of depositors, and increase the level of financial literacy of the population.

Challenge

Since the Company has large amounts of data relating to the financial information of many banks and legal entities, it is an alluring target for an attack, especially during a full-scale war.

The client had a large number of servers running MS Windows. Most of the workstations also used Windows OS of various versions.

The network used specific software developed specifically for this Company. The first one is among the key infrastructure elements

for providing electronic services to citizens and businesses, providing convenient, unified access to data from state registers. This software has many interaction interfaces, including various Web services.

The Company's management set the task for the IS department to reduce the risks of potential intrusions and unauthorized access to the LAN and improve the ability to detect attacks within the network, as the perimeter was already built using Cisco and CloudFlare products.

Realization

An AdminVM and two WorkerVMs were deployed, as presenting all VLANs in one TRUNK was impossible. At the same time, the WorkerVMs were distributed across different hypervisor clusters. One WorkerVM served network segments with workstations; the other was deployed on server subnets.

Seeder agents were distributed to 25% of all workstations and all available Windows servers. This made it possible to create about 10,000 file decoys that dynamically change when changes are made to network decoys.

Solution

First of all, a large number of network decoys were created that:

- imitated Windows hosts;
- simulated user behavior: web surfing, accessing SMB shares, DNS queries, etc.

Such actions allowed us to create an environment where Labyrinth could detect attempted MiTM attacks and provide many false targets for the attacker that looked entirely organic among real systems in the Client's network.

In the server segment, decoys imitating VMware ESXi and Ascod were deployed. In addition to them, we created imitations of all Web services using UniversalWebPoint decoys (including the WebUI of all Cisco equipment).

Results

The system deployment allowed us to improve the detection of attempted MiTM attacks and use the data obtained from the traffic to conduct further Lateral Movement. At the same time, it was much easier than using a SIEM with many correlation rules for similar tasks.

After deploying Web decoys that emulated all existing Web services on the network, the attacker's task of moving around the infrastructure unnoticed became unsolvable.

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.