LABYRINTH

CASE STUDY

Summary

The state agency Ukravtodor was established as a state corporation in 1990, replacing the Ministry of Roadways of Soviet Ukraine as the state governing body of automobile roads in modern Ukraine. It is supplemented by a project institute Ukrhiprodor which designs objects of road management.

Ukravtodor is supervised by the Ministry of Infrastructure of Ukraine. On February 28, 2002, by Presidential order, the state-owned open stock company “Avtomobilni dorohy Ukrainy” (ADU) was created.

The company was directly involved in road construction and maintenance. In 2016 ADU was merged into Ukravtodor, with the latter now owning 100% of its shares.

Client’s Infrastructure:

- Up to 750 LAN hosts
- Up to 100 VLANs

Challenge

The Client's infrastructure mainly consists of servers and various network equipment. The percentage of workstations is insignificant. The main feature is that critical assemblies are dispersed geographically.

The main task of Deception-system implementation was to increase the visibility of attackers' actions about all kinds of Web applications/services, many of which are in the infrastructure.

NTA solutions could have been more rational in such network architecture. Web-UI's volume was huge: on network equipment and specialized software explicitly created for this company.

Realization

Labyrinth Admin VM and 4 Worker VMs

were deployed on the VMware vSphere hypervisor in the management LAN segment.

Using the orchestration system used in the Company, Seeder Agents were distributed to most of the servers.

The total number of file baits is over 4500. More than 55 Honeynets were created to host Points network baits responsible for specific VLANs.

In each of the VLANs, approximately 15% of the address space has been allocated for network baits (Points).

Solution

1. Initially, the most critical of the services with WebUI/REST APIs and the most attractive targets for a potential attacker were identified.

2. The next step was to create multiple decoy Web services that were dynamic emulations of existing Web interfaces on the Company's network. These emulations contained many types of Web vulnerabilities providing the attacker with more options for attack development while increasing the chances of detecting network penetration and collecting data about the attackers' methods/tools.

3. Seeder agents were run on all file servers, through which the Labyrinth Deception Platform system spread file baits to real hosts pointing to functioning network baits (Points).

4. Special attention was paid to the propagation of different network decoys in the DMZ segment. Network decoys in this part of the network are most often regenerated so the environment does not look static. Regeneration takes up to three minutes.

Results

Implementing the system significantly increased the level of detection of intranet events, which was confirmed by penetration testing conducted after the system's deployment.

The system showed high effectiveness in the pentest, taking a lot of time away from the attackers and distracting them with multiple Web-baits scattered throughout the Client's subnets.

A side effect of using the system was the detections associated with shadow IT assets in the form of forgotten security scanners and asset-management software.

Network decoys in the DMZ segment allowed the collection of information that improved external perimeter infrastructure protection settings.

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.