CASE STUDY

Summary

One of the largest pharmaceutical companies in Ukraine, operating on the market for over a decade.

As an industry leader, the Client proposes a product portfolio that includes generic and original drugs in 11 of 14 pharmacotherapeutic groups.

Client's infrastructure:

- Up to 900 LAN hosts;
- Up to 80 VLANs;

Challenge

Every day employees of the company process many e-mail messages.

The anti-spam system processes incoming messages, but it can only function as a signature analysis of the content of the message.

It was necessary to add another layer of security that would be responsible for detecting successful phishing attacks and would not rely on signatures.

Realization

Labyrinth Admin VM and several Worker VMs were deployed on the VmWare vSphere hypervisor in the server LAN segment.

Seeder agents were distributed using the orchestration system used by the Company.

More than 15 Honeynets have been created to host the Points network honeypots, which are responsible for specific VLANs.

In each VLAN, 20% of the address space was allocated for network honeypots (Points).

Solution

Labyrinth's experts allocated Seeder Agents to all employee workstations of the Client's network.

With the help of it the Labyrinth Deception Platform system distributes file honeypots to actual hosts that point to functioning network honeypots (Points).

At least 20 file-breadcrumbs (file decoys) were generated for each workstation, each indicating one or more Points.

We maximized network decoys' usage for the network segments containing critical IT assets. These were imitations of DBMS and Web applications.

The Labyrinth system automatically verifies and maintains the relevance of file honeypots so that they fully consider changes when network honeypots change.

Additionally, we integrated the system with SIEM to enrich the context of detected events and two-way information exchange.

Results

After the system's deployment on the Client's network, several cases when the attacking party bypassed the mail message signature analysis system and gained access to workstations were detected.

In the second stage of the attack, we gathered essential information on the workstation, which would help to gain a foothold and develop the attack deep into the network.

Intruders were revealed using information from file honeypots found on the hosts, which pointed to imitation databases.

In addition to detecting the fact of penetration, the Labyrinth system won more time for the SOC to react and decide on further incident response.

Despite this advanced breach detection, the complexity of the attack and the subsequent data compromise highlighted the need for an integrated, multi-layered security approach.

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.

Follow us on:

Labyrinth Development

Labyrinth Deception Platform