CASE STUDY

Summary

The client is a leading freight audit and logistics visibility provider, which provides informational services as a B2B intermediary for building supply chains. Data protection is a crucial issue for this type of business.

Client's Infrastructure consists of:

- Up to 500 LAN hosts.
- 6 main web services in DMZ on different servers.

Challenge

In a short span of time (few weeks), several Client's competitors were hacked at once that resulted in all their users' data exfiltration and settling it for sale by hackers or resellers.

The Client's request was to increase company's infrastructure visibility immediately in terms of information security, as well as enchase the chances of detection of a potentially occurred attack and invasion beyond the perimeter.

Realization

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

Three Honeynets were composed for Points:

- in the DMZ segment (12 IPs);
- in dev/test segment (30 IPs);
- in the dir-hosts segment (58 IPs).

For Honeynet Points in the DMZ, UniversalWebPoint was used, while for the other two segments, all available Point types were selected.

Seeder agents have been extended to:

- Real servers running production web services;
- All dev/test servers;
- On laptops and workstations of the dir-hosts segment.

Solution

Deployment of the Labyrinth system and coverage of the Client's infrastructure was provided in two directions. The first one - deployment of several UniversalWebPoint's in the DMZ next to real production servers and opening access to them from the Internet.

This vector is aimed at collecting data about the attacker and determining the most demanded resource or dataset, detection the most essential data for the attacker from a scope of Client's production services.

.

The second one was integration of a set of Points into segments: dev/test-servers and into VLANs used for computers of the Company's management and accounting.

This integration was aimed at detecting an attacker who has already penetrated the LAN via remote access channels, corporate VPN, while most of the employees work remotely in quarantine.

For all web services, services based on UniversalWebPoint were created, with slight visual differences from the original and emulated vulnerabilities (DirTraversal, LFI, RCE). We generated subdomains, which might be accessed via the Internet. In the other two Honeynets, groups of different types of points were generated.
The entire system deployment took less than two hours.

Results

The evaluation team identified that the attackers' efforts were aimed on unfinished transactions database (unfinished trades), while the Client's previous assumption was that the main goal would be a database of companies using their services.

Based on the received information, an immediate additional review of the code was made in terms of all points of receipt of data from the user by a web application related specifically to unfinished transactions.

Under the second vector, we discovered that LAN scans are taking place from the home workstation of one of the client's software developers connected via VPN in non-business time and the examination (recon) of the hosts located in the dev/test segment is performed. Also, brute-force attacks and attempts to use exploits on network services with the further execution of privilege-escalation were indicated. The employee's workstation was isolated and submitted for forensic analysis.

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.