CASE STUDY

ПОЛІГРАФКОМБІНАТ
УКРАЇНА

Summary

State Enterprise "Polygraph Combine "Ukraina" for securities' production" many years maintains its leading position for the production of identification documents, securities forms, secure printing products, etc.

Passport of Ukraine "to travel abroad" is rated 27th among 130 countries and entitling entry without a visa up to 89 countries; with a visa when crossing the border – up to 41 countries.

Client's Infrastructure include:

- Up to 1000 LAN hosts;
- Up to 3 web services in DMZ;
- Up to 9 non-web services in DMZ on different servers;

Challenge

With the transition of the Company's employees to remote work due to quarantine, obtaining the maximum visibility of events inside the perimeter and detection of anomalous actions of employees connected via VPN were crucial tasks for IT team.

It was also essential to collect more data about the DMZ segment and the hosts interacting with it.

Special efforts had to be contributed to securing access to the Askod system within the network.

Realization

One Labyrinth Admin VM and several Labyrinth Worker VMs were deployed on the VmWare vSphere hypervisor in the server LAN and DMZ (only Worker VMs) segments.

Five Honeynets were composed:

- For Points in the DMZ (25 IPs);
- For Points in IT test-segment (45 IPs);
- For Points in physical security devices segment (30 IPs);
- For Points in the company-management segment (120 IPs);
- For Points in production segment (64 IPs);

UniversalWebPoint was used in most cases within all segments. In the segment of the Company's management, AskodPointType was additionally used.

Seeder agents have been extended to:

- Real servers running production web services;
- All test servers;
- On laptops and workstations of the company management segment;
- Home laptops, that were used for VPN-connection Solution.

Solution

Deployment of the Labyrinth system and coverage of the Client's infrastructure was provided in a few directions:

- Several UniversalWebPoint imitating real services from this segment were located in the DMZ, and several Points were deployed with imitation of remote-control services: ssh, rdp, rest-api.
- Within the company-management-segment both specialized Point types (Ascod, 1C) and workstation simulations were used: RDP, wmi, ssh, netbios & etc.
- The IT-segment was flooded with a wide variety of IT decoys for providing attackers the maximum number of different vectors of further "attacks".
- The LAN was filled with Points' imitating various file storages: ftp, sftp, samba, nfs, webdav. Simulations of various databases were also created.
- Multiple Breadcrumbs were distributed on all critical hosts to distract the attacker to simulated services / hosts.

Results

Before Labyrinth's deployment within the perimeter of the Client's network, no tool to increase the visibility of user actions and network software was used.

After the system was deployed, it was possible to detect anomalous software behavior in the DMZ segment, which was the result of an incorrect configuration.

Cases of unauthorized use of LAN resources by users who connected to the network via VPN due to quarantine were identified and studied.

On one of the workstations, suspicious scripts that scanned the network and carried out bruteforce attacks on the ssh and rdp services were identified.

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.