R&D for the Gas Retailer

Labyrinth Deception Platform

INTRODUCTION

One of our clients is a large oil and gas company, which owns one of the largest networks of gas stations.

Gas retailers are aware of the risks tied to their business and so heavily invest in equipment that allow them to remotely monitor and manage gas levels to avoid industrial accidents. An explosion of any kind is considered dangerous. Physical damages can have an irreversible impact on a business's bottom line or the business itself, if an explosion is sufficiently large enough to deplete its assets.

SOLUTION

For this case was developed a way to simulate the existence of these devices to check whether threat actors will find them venues attractive enough to go after.

We created virtualized Guardian AST tank-monitoring systems, complete with function and input/output (I/O) controls and other features and functions of the gas stations, that make attackers believe they are real. We observed the attacks and monitored the attacker's actions, essentially gathering intelligence on the actors.

Essentially, a completely new Point type (network lure type) was written to serve as a functional honeypot that logs connections and compromise attack attempts. They emulated a gas station with several tanks for different types/brands of fuel. The following

indicators were taken into consideration: fuel name, temperature and humidity in each fuel tank, location, time stamp.

TESTS

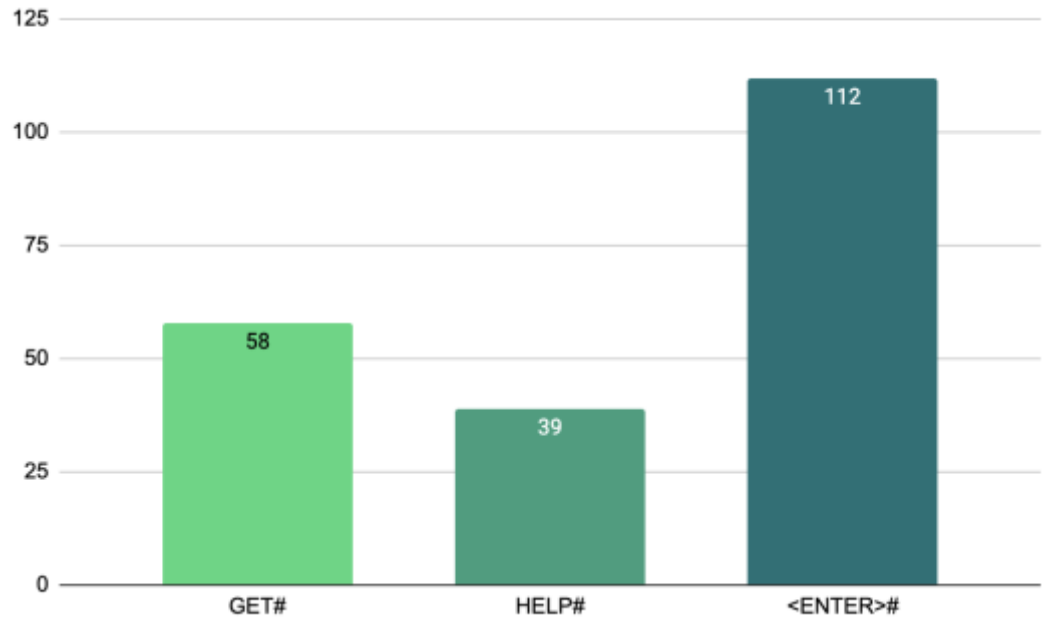
Before the presentation to the Client, we conducted a variety of tests.

Firstly, we tested this Point type functionality on a variety of scanners and tools to ensure that it can be discovered and interacted with, much like an actual device.

Secondly, our goal was to collect statistics of real-life attackers' interaction with our emulations. We started from installing 5 decoys in different locations and made them available via the Internet. After that, we "advertised" them on several information security forums in the Tor-network, providing the addresses of the decoys for real-life attackers. All decoys were not located in cloud environments.

RESEARCH RESULTS

In most cases, monitoring of our honeypots allows us to observe reconnaissance done on our system. Most of the connections observed can be categorized as done by automated scanners performing “GET” and “HELP” command requests as well as “#” carriage returns.



According to the gathered data, the most commonly used command is I20100 , which lists basic gas-station information. Existing Nmap scripts pull out this information from out honeypots (Points), as well as Shodan.

Around 3% of all attackers tried not only to obtain information about the simulated infrastructure, but also sought opportunities through available services and commands to change the settings or disrupt the normal functioning of the simulated systems.

Even an attempted DoS attack was detected after unsuccessful attempts to disrupt the functioning of the system in other ways.

IMPLEMENTATION

Due to the very narrow specialization of these decoys and rather high technical requirements for them, it was decided not to include this point type in the Labyrinth system at the moment. These developments will be further improved.