HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Characterizing Adversaries through Adaptive Honeypots

Amplification and Direct Path Attacks

Adversaries today typically perform (distributed) denial of service (DoS) attacks by abusing third parties to hide their whereabouts. Attackers either locate a large number of servers that provide amplification (a small request results in a large response), or compromise a large number of devices that are abused to perform the attack.

Unique Characteristics

Even though attacks such as a DoS are simple, many adversaries have their unique "style" in performing it. This allows us to track the actors behind the attack, link individual attacks on victims to campaigns and see how attackers evolve over time.

By exposing abusable servers on the open Internet and responding to request, we can obtain a real-time view about DoS actors, the victims they currently target and the techniques they use to perform the attacks.

A Distributed Honeypot System

The Alvarium honeypot system is a distributed research framework for cybercrime research. Volunteers can operate a honeypot instance which invites connection attempts from adversaries, which are internally forwarded to our servers and evaluated in a safe environment. All honeypots are controlled through a central coordinator so that they can't actually participate in attacks but appear as legitimate victims to adversaries.

Characterizing Adversaries with Alvarium

In this project, we extend the honeypot framework by making the honeypot coordinator and backend adaptive, so that we can study how attackers discover, investigate and ultimately abuse services on the Internet. We will

- implement, deploy and expose amplifying services and vulnerable IoT images in various public clouds and ISP networks
- adapt the honeypot coordinator to craft customized responses to connection requests, so that we can track the full attacker lifecycle from service discovery to abuse and track collaboration between adversaries
- improve the system and make it accessible to the general public and researchers as a platform
- deploy a proof of concept honeynet with experiments to characterize the landscape of adversaries behind IoT botnets and DoS amplification campaigns