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 use the existing honeypot framework to collect data about real attacks and derive information about the techniques used by the attackers. Tasks

- Deploy honeypot infrastructure with vulnerable software and hardware images on the public Internet and in company environments
- Automatically characterize exploits and fingerprint based on connection and interaction behavior
- Perform access pattern mining to optimize honeypot resource utilization on interesting activities
- instrument software in high-engagement honeypots to obtain deeper insights into adversarial behavior and machine-collectable indicators of compromise (IoC)