Course Overview and Agenda

Bot Manager: Foundations

Version 1.0

Course Overview

This course will cover the current threat landscape, attacker motivations, and technical mitigation strategies for automated non-human attacks. These range from a single host running command line scripts to distributed botnets actively trying to appear as legitimate clients.

Attack types covered will range from basic page/price scraping to more advanced credential stuffing attacks. Highlighted will be some of the newer advanced actions within Bot Manager, which obfuscate the response to the attacker that they are being mitigated.

Objectives

After completing this course, participants will be able to do the following:

- Provide an overview of the Akamai Cloud Security Solutions portfolio
- Identify the top bot use cases Akamai customers encounter
- Describe in technical detail each Bot Manager detection category
- Describe and configure Bot Manager detection categories appropriate for each use case using Luna
- Describe and Configure Bot Manager actions appropriate for each use case using Luna
- Describe in detail how Bot Manager 2.0 Premier and Bot Manager Standard products can mitigate bot attacks
- Using Luna Control Center, Prepare and deploy a Bot Manager configuration to mitigate bot attacks

Prerequisites

To maximize your time in the class and ensure you get the most out of the two-day training, Akamai University recommends that you will have completed the following prerequisites:

- You have at least one Akamai Security Product on contract
- You have an account set up in the Luna Control Center (control.akamai.com)
- You have deployed an Akamai Configuration to staging or production

Agenda

The Akamai University Bot Manager: Foundations advanced course curriculum consists of 9 modules and two labs over a duration of two days. The agenda for this training is listed below.

DAY 1

Duration	Module Name & Description
60	**MODULE 1: INTRODUCTION** *This module is an introduction to Akamai's Cloud Security Solutions portfolio, and a reference architecture for Bot Manager discussion.*

60	**MODULE 2: THREAT LANDSCAPE**
	This module is a discussion on the bot problem and the various pain points that they cause (scraping, travel room lockout, account checking, origin load, customer satisfaction impact, advertising revenue loss)
	- *Problem Statement*
	- *Why is defense so hard?*
	- *The top five problematic (non-DDoS) bot use cases*
	  - *Akamai customers encounter*
	  Credential Abuse (transactional)
	  3rd Party Account Aggregators (transactional)
	  Automated Inventory Purchasing (transactional)
	  Targeted Web Content Scraping (price, inventory level)
	  Broad Web Site Scraping

45	**MODULE 3: CUSTOMER REFERENCE ARCHITECTURE** *This module is a technical review of Akamai's Security Cloud Security Solutions portfolio and discusses how the products work together in defense of customer web sites for bot mitigation.*
60	**MODULE 4: ANATOMY OF A BOTNET** This module is a presentation on how attackers would set up both a simple single host bot as well as a complex Command & Control botnet. The various types of methods of creating a botnet are discussed, including Curl, Python, Java, Selenium, headless Chrome, PhantomJS, and other frameworks.
60	**MODULE 5: BOT MANAGER DEEP DIVE** This module is a deep dive into Akamai's Bot Manager Premier and Standard products, analyzing the reporting, detection, and mitigation options available.
45	**DEMO/LAB: BOTNETS IN ACTION** *This module features an instructor-led demo and student lab where the instructor will launch two botnets against student' hosts. Students will use Luna Control Center to detect and analyze the botnets in use.*

DAY 2

Duration	Module Name & Description
30	**DAY 1 REVIEW** *This module will review the Day 1 activities, specifically the threat landscape, the techniques used to build and execute bots, the common bot detection tools, techniques and strategies.*
60	**MODULE 6: REPORTING** *This module introduces detection use cases in the Bot Manager product, introduces Bot Analysis View, and reviews various reports used to detect Bots.*
60	**MODULE 7: BOT MITIGATION** *This module will identify mitigation strategies available in Bot Manager and review appropriate mitigation strategies based on the type of botnet detected.*
120	**MODULE 8: BOT MANAGER PREMIER** *This module will allow students to assess appropriate detection and mitigation strategies using the botnets from Day 1 using Luna Control Center.*
75	**BOT MANAGER PREMIER CAPSTONE LAB** *This hands-on instructor-led lab will serve as a capstone assignment in which students will detect and mitigate botnets from Day 1 using Luna Control Center. Students will create an appropriate mitigation for a botnet, deploy it, and evaluate the effectiveness of the mitigation strategy chosen.*
60	**Survey, Quiz & Certification**