Smart Block:
Web Attack Tracking Software

Team: sdmay21-17 | Paul Degnan | Megan Hill | Andrew Marek | Jamie Sampson | Emily Young
Client: Andrew Dakin (Cylosoft) | **Adviser:** Doug Jacobson

Introduction

Problem

Cylosoft hosts many customer websites. On a regular basis, the sites are probed by bots and hackers attempting to access user data.

Overview

SmartBlock is a .NET Core application written in C# that allows users to monitor blocked IPs and enforce various Microsoft Internet Information Service (IIS) security measures for multiple websites at once. It uses an Azure database to store IPs and implements a file watching system to track incoming log changes that are then parsed and analyzed.

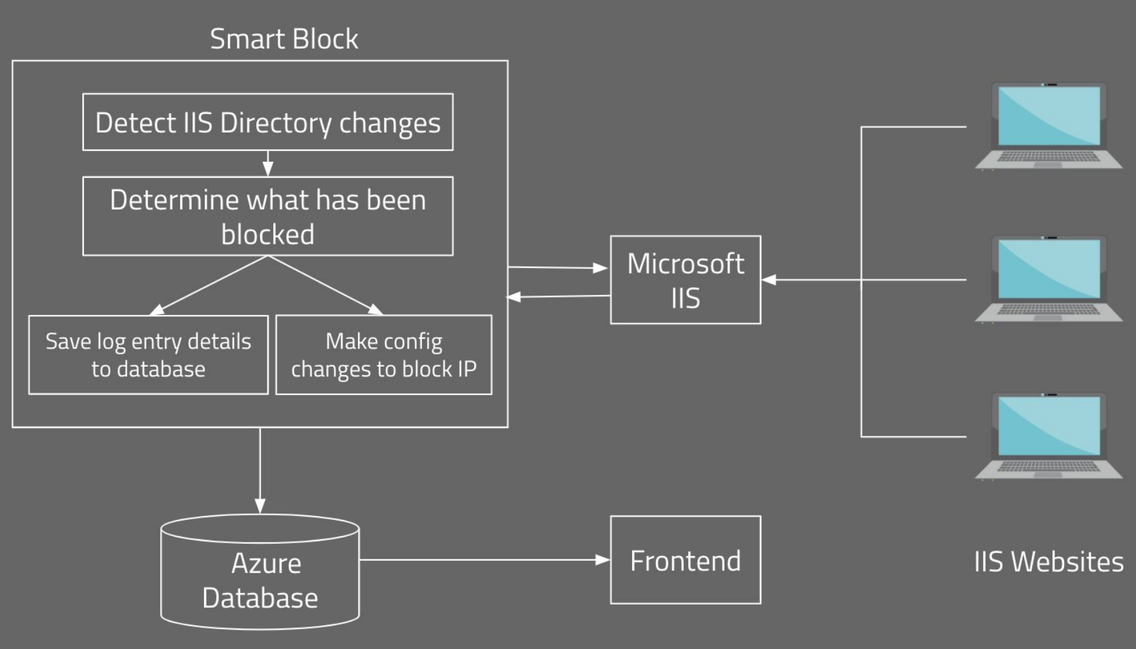

Figure 1: Concept Sketch

Design Requirements

Functional Requirements

- Record Blocked IPs in Azure Database
- Parse Microsoft IIS Log Files
- Process Multiple Sites on Single Server
- Block Malicious Actors with IIS Config Changes

Non-Functional Requirements

- Ease of Use
- Scalability Over Time

Engineering Constraints & Standards

- Run on Windows OS
- Use Client Provided Azure Database
- .NET Core App to Integrate with Existing Software
- Private Github Repository
- IETF Protocol Standards
- Code Reviews & User Documentation

Technical Details

- .NET Core Application (C#)
- Azure Database
- Microsoft Internet Information Services (IIS)
- NextJS
- IDEs: JetBrains Ride, DataGrip, & WebStorm
- NLog (Logging Tool)
- FileWatcherEx (Github Package)

Design Approach

IIS Config Changes

- JSON Website Specific IIS Settings
- Initializes IIS Configs Upon App Startup
- Connects with Multiple IIS Module APIs

File Watcher

- Monitors Root Directory for All IIS Website Logs on a System
- Watches for Changes in Site Log Directories
- Upon Change in Log File or an Added Log File, Notify SmartBlock
- Only Reports Newly Added Entries to Files

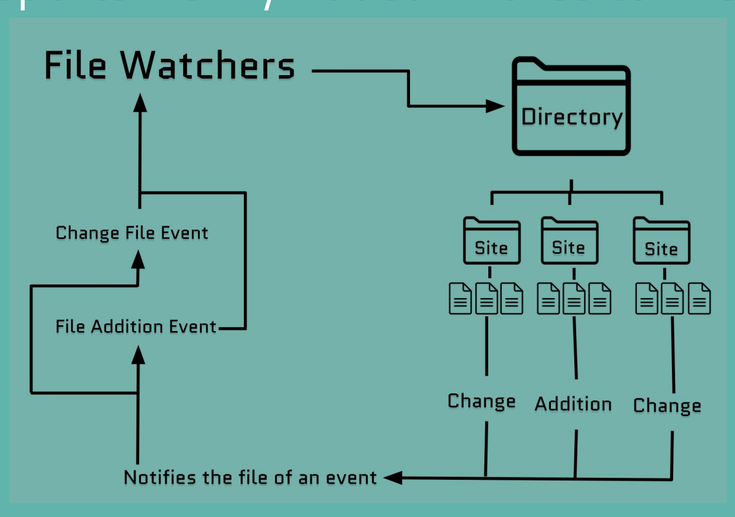

Figure 2: File Watcher Flow Diagram

Log Parser

- Receive Notification of Changes from File Watcher
- Read Log File Headers
- Parses through Logs in Log File Looking for:
  - cs-substaus: IIS blocked if 501, or 502
  - cs-uri-stem: client's URL
  - CF-Connecting-IP: IP address
- Upon Finding IIS Blocked IP, Insert into Database

Azure Database

- Connects to client-specific Azure Database
- Requires Public IP from Connecting System for Authorization
- Tools: MSSQL and DataGrip
- Methods: Read (Select], Delete, Add
- Initialize Once So Not Passing Around Object

NextJS Website

- Render Blocked Log Data from Database
- Graph of Number of IPs Blocked per Day
- Line Color Coding for csHosts Over Time
- Filter by Headers (Data/Time, csHost, etc.)
- Remove Headers to Isolate Data

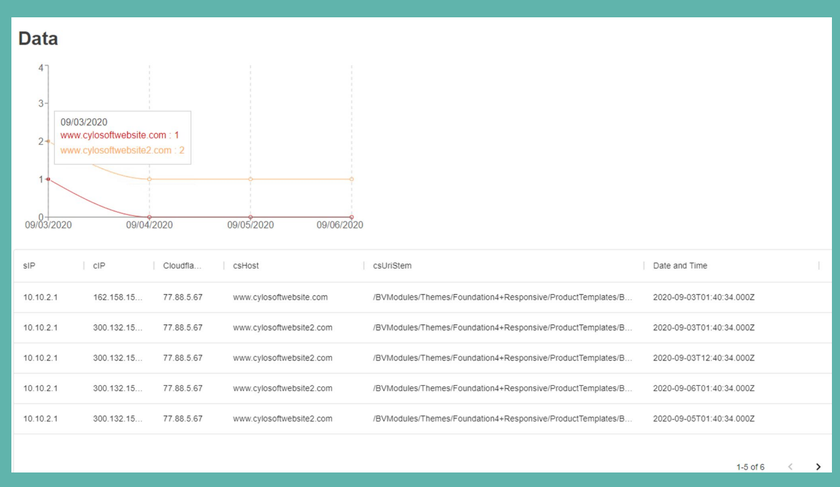

Figure 3: Sample Website Data Rendering

Testing

- Remote Desktop (Windows OS)
  - Microsoft IIS
  - Connects to Azure Database
- Unit Testing Log Parser (MSTest)
- Manual UI Website Testing
- Checking Enforcement of IIS Settings
- Connection to Client's Real IIS Websites

Intended Users/Uses

Users

- Our Client Cylosoft
- Future Open-source Repo

Uses

- Monitor Blocked IPs
- Enforce IIS Security Measures
- Prevent Malicious Attacks

cylosoft