****

**Architecture + Design Overview**

**for**

**SEng Malware (SEM)**

**Version 0.3**

**Prepared by:**

1. John Dornheim
2. Chris Durand
3. John Schlatter
4. Shelby Mitchell
5. Alex Lopez
6. Jon Harrity

**CSC 190 Term Project**

**Advisor:** Dr. Scott Jeffreys

Spring 2019

*Made with love in Axinn 806*

**Table of Contents**

1. Overview
   1. Purpose
   2. Roles and Responsibilities
2. User Interface
   1. Deep/Shallow Scan Page
   2. Settings Page
   3. Log Page
3. System Architecture
   1. Box and Line Diagram
   2. Layered Architecture Pattern
   3. Adapter Design Pattern
4. Current Revision Log of SEng Malware
5. **Overview**

1.1 Purpose

The purpose of this document is to provide an in depth description of SEng Malware, which is a malware scanner for Windows 10. SEng Malware was created for clients who might not be the most tech-inclined, but would like to keep their desktop safe from malicious files. This Architecture and Design overview will review the components of SEng Malware, its prototypes for the user interface, its design considerations, and its current revision log. This living document will continue to be updated until this project is completed.

1.2 Roles and Responsibilities

The following is a list of all SEng Malware team members and their roles within this project:

Shelby Mitchell — Project Manager, Scheduler, UI builder

Jon Harrity — Head of Configuration Management, UI builder

Alex Lopez — Head creator of the GUI

John Dornheim — Head of ClamAV functionality

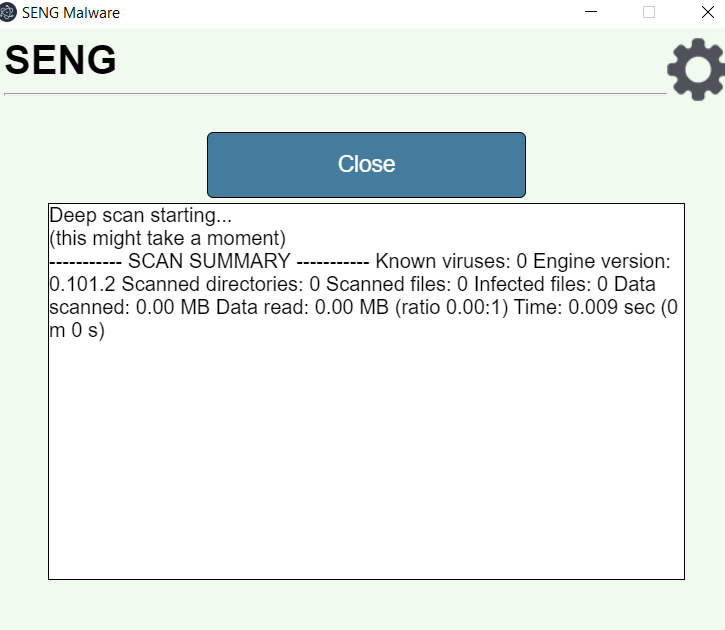
Chris Durand — ClamAV functionality, UI builder

John Schlatter — UI builder, software tester

1. **User Interface**

A screenshot of a cell phone

Description automatically generated 2.1 Deep/Shallow Scan Page



Page Functions

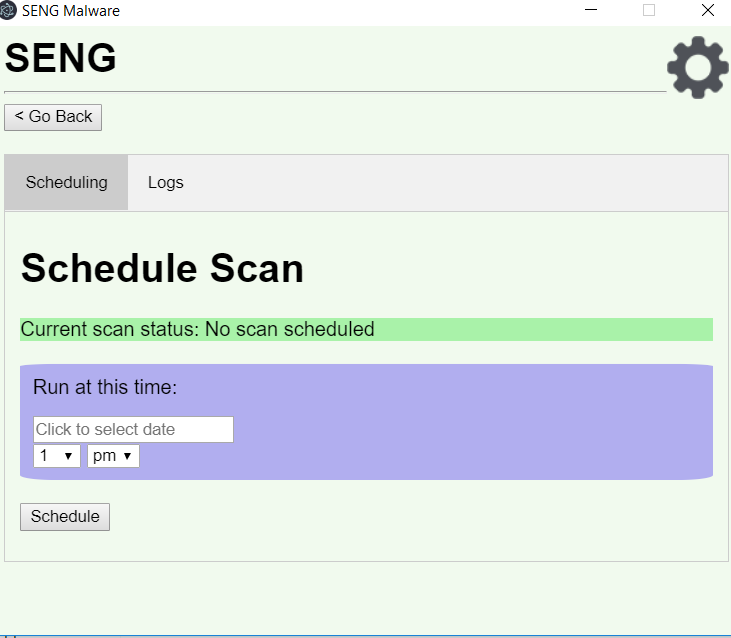
1. Page will include a gear icon at the top right to access the Settings page

Deep Scan Functions

1. The Deep Scan will scan the C: directory of the current device
2. Text box will display what is currently being scanned. Files that are not malicious will be labeled “OK” while malware will be labeled “Found”
3. Empty files will also be tagged
4. Log will be generated from the results

Shallow Scan Functions

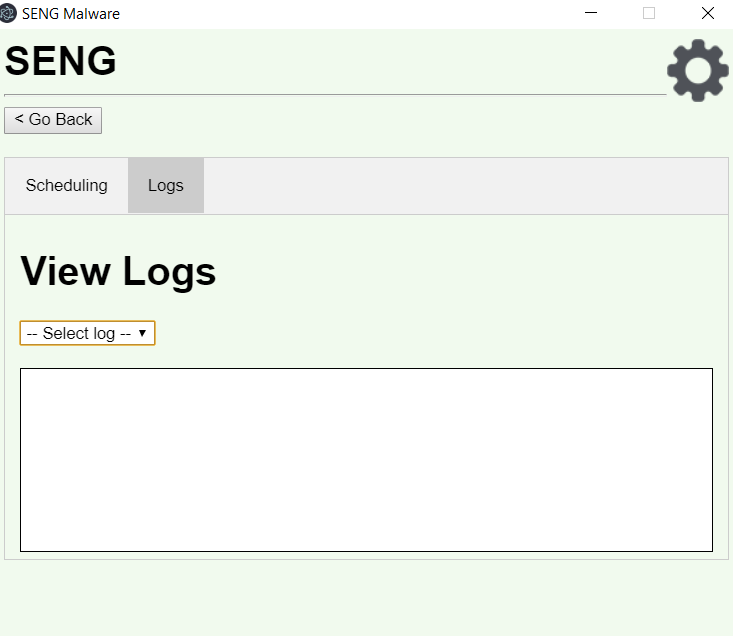
1. Shallow Scan button will initialize the shallow scan
2. The shallow scan will scan the Windows Temp folder
3. Text box will display what is currently being scanned. Files that are not malicious will be labeled “OK”, malware found will be labeled “Found”, and empty files will be labeled “Empty File Found”

2.2 Scheduling Page

Scan Schedule Function

1. User will be able to schedule a scan for a future date
2. Simple Month/Day/Year/Time input with a schedule button

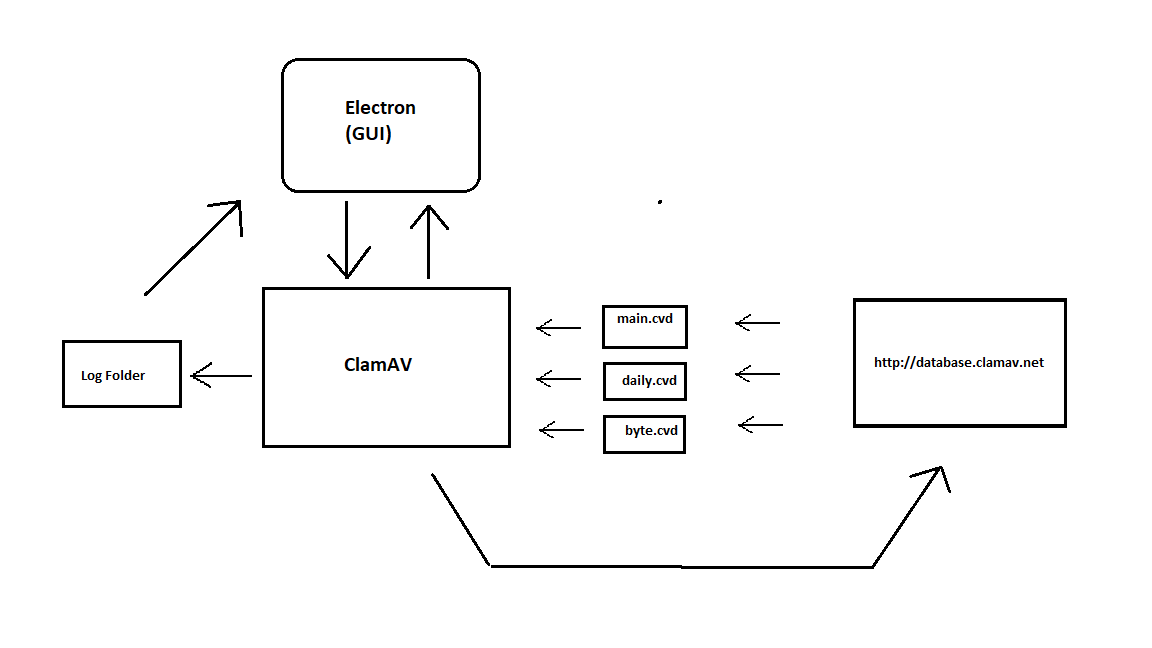
2.3 Log Page



Log Page Functions

1. Displays a list of previous virus scans
   1. Drop down menu of log files included for user to specify which log they would like to view.
   2. Clicking on a log will open the entire log of the scan in the text box. This will include the files scanned, number of files scanned, number of viruses checked for, number of infected files, and number of quarantined files.

**3. System Architecture**

3.1 Box and Line Diagram

3.1.1 Descriptions

ClamAV - anti-virus engine

Electron - GUI. Utilizes node.js

Log Folder - contains the virus logs generated by the ClamAV engine

Main.cvd - main virus database

Daily.cvd - daily virus database

Byte.cvd - byte virus database

<http://database.clamav.net> - ClamAV virus database server

The box and line diagram describes the flow of information between components. This is in reference to how individual components talk to each other, as well as interactions with the database files and the internet.

3.2 Layered Architectural Pattern 