Функционал данного голосового ассистента реализован на мультипарадигменном языке программирования Python с использованием: библиотек по распознаванию речи SpeechRecognition и Vosk; библиотеки fuzzywuzzy для оценки совпадения голосовой команды со встроенной; библиотеки pyttsx3, позволяющей создавать речь на основе текста с использованием различных голосов; библиотеки opencv-python для машинного зрения; библиотек webbrowser и requests для работы с браузерами и осуществления поисковых запросов; библиотеки serial для работы с COM портами, а также с графическим интерфейсом.

В проекте использовался ноутбук вместе с голосовым ассистентом, программируемая платформа Arduino с прошивкой, предназначенной для управления подключённой аппаратурой: датчиками, реле, светодиодными лентами и моторами постоянного тока.

Литература

1. П. С. Скочко, В. Ф. Барабанов, Н. И. Гребенникова, С. Л. Кенин, Голосовой помощник для управления операционной системой / Вестник Воронежского государственного технического университета Т. 18. № 2. 2022.

2. Hinton, G., Deng, L., Yu, D., Dahl, G. E., Mohamed, A. R., Jaitly, N. et al. (2012). Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups / Signal Processing Magazine, IEEE, 29(6). Pp. 82–97.

А. Д. Иванов
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Васькевич**, ст. преподаватель

МЕТОДЫ СОКРЫТИЯ SYSMON В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

Sysmon – это системная служба Windows и драйвер, который продолжает работу в системе после перезагрузки для мониторинга и сбора данных о системной активности в журнале событий Windows. Он предоставляет подробную информацию о создании процессов, изменении времени создания файлов и сетевых подключениях. Проанализировав данные, можно выявить какие-либо подозрительные или вредоносные действия в системе или сети [1].

Sysmon важно скрывать в системе от злоумышленников или вредоносных программ, так как он никак не пытается скрыть себя в системе [1]. А злоумышленники или вредоносные программы смогут его обнаружить и деактивировать, чтобы у жертвы было меньше возможностей вовремя среагировать на заражение или атаку.

После установки Sysmon без дополнительных параметров в PowerShell можно увидеть то, что был установлен и запущен драйвер SysmonDrv, и установлена и запущена служба Sysmon (рисунок 1).

Рисунок 1 – Результат вывода консоли после установки Sysmon

Присутствие Sysmon в системе можно определить, введя команду PowerShell Get-Service, которая позволяет получить объекты, представляющие службы на компьютере. Также командной fltmc (если имеются права администратора) можно вывести список запущенных драйверов. Такие действия могут применить злоумышленники сразу после попадания в систему (рисунок 2).

Переименовав установочный файл Sysmon, можно избежать обнаружения по названию службы. Как вариант, замаскировать его, назвав каким-либо системным процессом (например, svchost.exe). Также, запустив установку Sysmon с флагом -d можно указать другое имя драйвера Sysmon (например, имя драйвера для принтеров). Для наглядности файл был назван “HiddenSysmon.exe”, а драйвер имеет имя “secret” После этого действия, по своему имени Sysmon невозможно найти, хотя он установлен в системе. Но «высота» осталась прежней (рисунок 3).

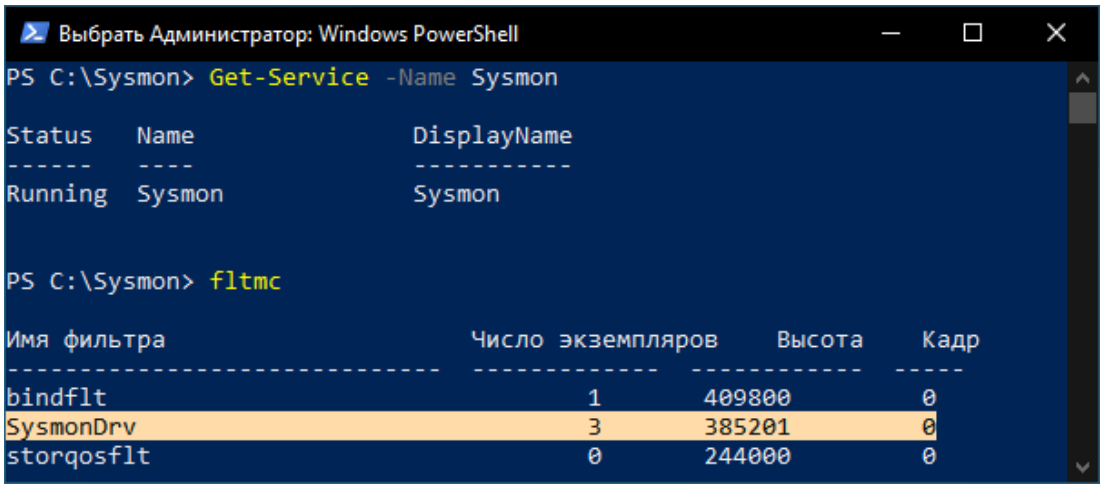

Рисунок 2 – Результат работы команд

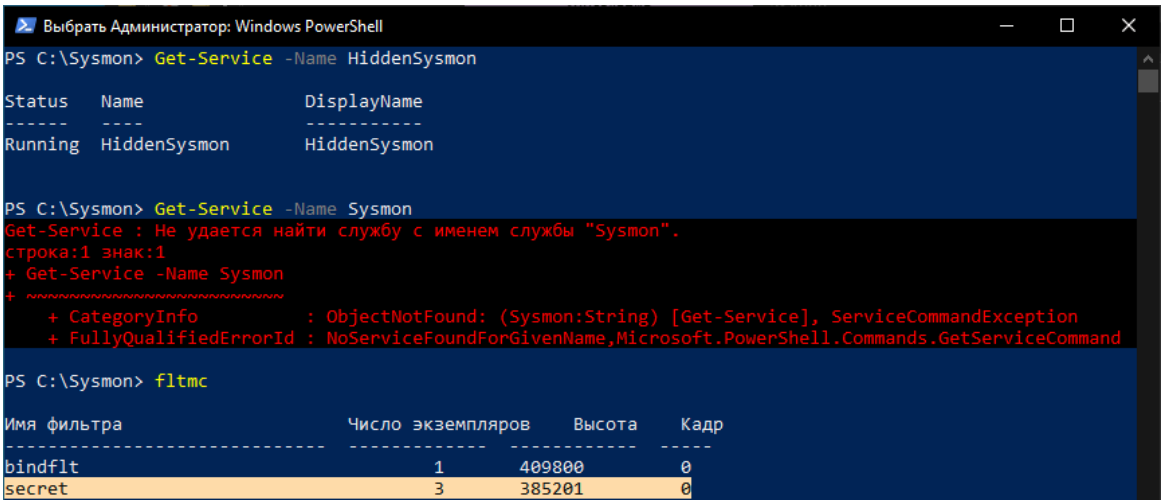

Рисунок 3 – Попытка найти Sysmon после изменения имен службы и драйвера

Однако, открыв «Службы» можно определить наличие Sysmon в системе по описанию его службы. Имя службы тоже можно легко изменить. Нужно открыть редактор реестра и пройти по пути HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services. В данной вкладке необходимо найти имя нашей службы, щелкнуть по ней и изменить значение у параметра Description (рисунок 4). После данной операции, в программе «Службы» можно обнаружить измененное описание.

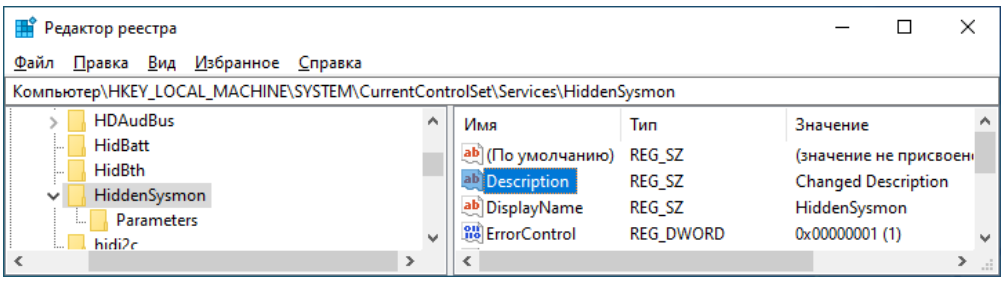

Рисунок 4 – Измененное описание в редакторе реестра

Еще одно действие – изменить параметр «высота» у драйвера. Однако нужно быть предельно осторожным, т. к. при наличии двух драйверов с одинаковой высотой, есть высокий риск «сломать» систему. Оставаясь в редакторе реестра, найти необходимый драйвер (“secret”) щелкнуть по нему и по пути имя_драйвера\Instances\Sysmon Instance изменить строковый параметр “Altitude” на нужное значение. Это же значение отвечает за порядок загрузки драйвера [2]. После можно убедиться в том, что «высота» изменилась (рисунок 5).

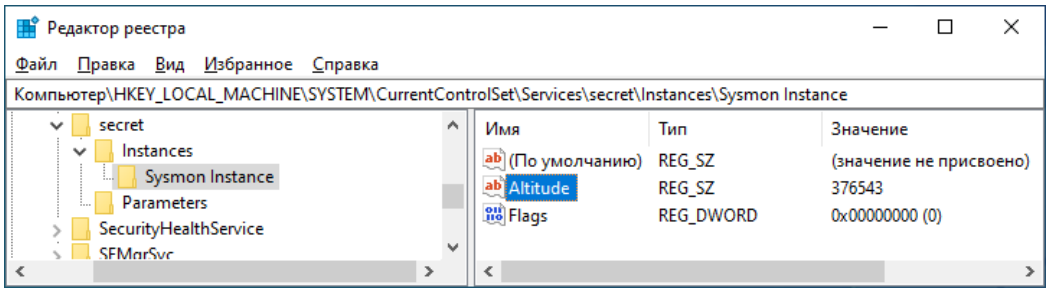

Рисунок 5 – Изменение «высоты» драйвера

Литература

1. Sysmon Sysinternals. | Microsoft learn [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/en-us/sysinternals/downloads/ sysmon. Дата доступа: 21.03.2024.

2. Load order groups and altitudes for minifilter drivers | Microsoft learn [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/load-order-groups-and-altitudes-for-minifilter-drivers. Дата доступа: 21.03.2024.

Е. В. Иванцова, Д. С. Сыч
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **А. В. Воруев**, канд. техн. наук, доцент

ДЕТЕКТОР ГРАНИЦ ЛАПЛАСА: ОПИСАНИЕ АЛГОРИТМА И ЕГО ПРИМЕНЕНИЕ В ОБРАБОТКЕ ИЗОБРАЖЕНИЙ

Детектор Лапласа – это математический оператор, используемый для выявления границ объектов на изображениях. Разработанный английским физиком и математиком Пьером-Симоном Лапласом в начале XIX века.

Принцип работы детектора Лапласа заключается в вычислении второй производной яркости пикселей изображения. Этот процесс позволяет определить резкие изменения яркости, что делает возможным выделение краев и контуров объектов, а также текстур и других свойств изображений. Обычно применяется в сочетании с гауссовым размытием для сглаживания изображения и подавления шумов.