МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**Исследование утилит** «**AutoRuns» и «Process Explorer»**

отчёт по лабораторной работе №4

по курсу «Системы обнаружения вторжений»

Выполнили: студенты гр. 230781 \_\_\_\_\_\_\_\_\_ Глейм С.М.

(подпись)

\_\_\_\_\_\_\_\_\_ Ивлев А.Р.

(подпись)

Проверил: асс. каф. ИБ \_\_\_\_\_\_\_\_\_ Чаговец С.Н.

(подпись)

Тула, 2022 г.

**Цель работы**

Изучение разделов конфигурации ОС семейства MS Windows, влияющих на автоматическую загрузку приложений при запуске ОС. Изучение и исследование утилиты **AutoRuns**. (пакет MS Sysinternals Suite). Изучение и исследование утилиты **Process Explorer**. (пакет MS Sysinternals Suite).

**Задание на работу**

1. Исследовать эффективность контроля автозагрузки запускающихся при старте операционной системы сервисов, приложений и других компонентов.
2. Проверить возможность быстрого нахождения и отключения (если необходимо и удаления) любого компонента из автозагрузки.
3. Какие возможны последствия в случае ошибочного отключения (удаления) системного компонента?
4. Проверить возможность формирования утилитой запроса на получения информации об интересующем приложении или сервисе.
5. Сохранить результаты сканирования и отправить по указанному преподавателем адресу электронной почты или выложить на указанный ftp-сервер;
6. Обнаружить и отключить с помощью программного обеспечения Autoruns потенциально опасные приложения, требующие дальнейшего анализа;
7. В каких участках современных ОС на базе MS Windows NT+ чаще всего регистрируются на автозапуск вредоносные приложения и почему?
8. Сравнить текущее состояние автозапуска ОС с предыдущим полученным, до выявления опасных приложений, оценить эффективность сравнения и поиска отличий средствами ПО Autoruns;
9. Какими средствами и утилитами ОС Windows можно частично заменить функционал ПО Autoruns?
10. Запустить диспетчер задач и программу Process Explorer. Сравнить их функционал;
11. По каким признакам можно определить вредоносное приложение с помощью программы Process Explorer?

**Ход работы**

После скачивания программы Autoruns был выполнен контроль приложений, запускающихся при старте системы. Программа показывает все пользовательские и системные компоненты, находящиеся в автозагрузке.

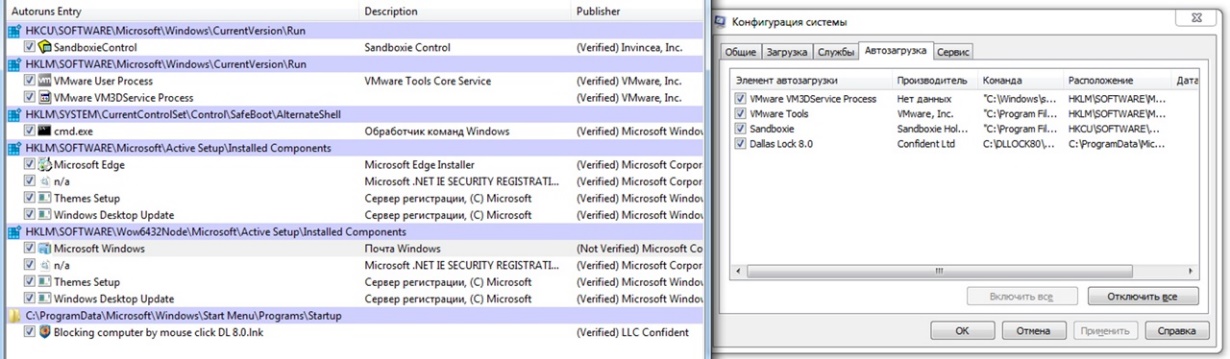


Рисунок 1 - Контроль автозагрузки в Autoruns и конфигурации системы

Были успешно проверены быстрый поиск и возможность отключения компонентов.

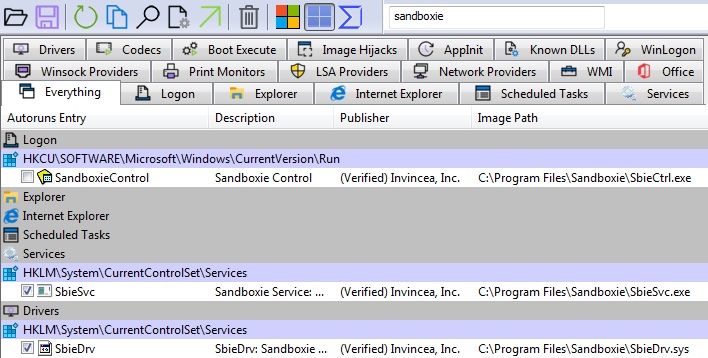


Рисунок 2 - Быстрый поиск и отключение компонента

В случае отключения системного компонента из автозагрузки возможны ошибки при работе системы. Последствия могут не проявляться, если служба активно не используется. Также возможно возникновение критических сбоев при запуске системы без некоторых служб. Пример критической ошибки при отключении системных служб представлен ниже на картинке.

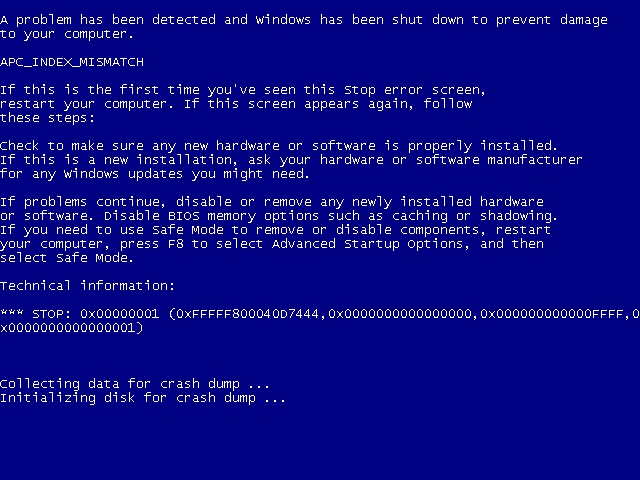


Рисунок 3 - Критическая ошибка при запуске системы

Также был выявлен и исключен из автозагрузки опасный компонент (выявлен на Virus Total).



Рисунок 4 - Опасный компонент

Чаще всего вредоносные компоненты располагаются в следующих разделах:

* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run – раздел реестра, из которого программы выполнятся при старте системы.
* %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup (Автозагрузка) – директория, из которой программы выполнятся при старте системы.
* Назначенные задания (Планировщик задач) – служба, через которую выполняется автозагрузка программ.

Эти разделы являются самыми распространенными для выполнения автозагрузок.

Затем было сохранено состояние автозагрузки в отдельный файл и добавлено приложение на автозапуск. После запущено сравнение, в результате которого был выявлен только что добавленный компонент. Результат сравнения представлен на рисунке ниже.

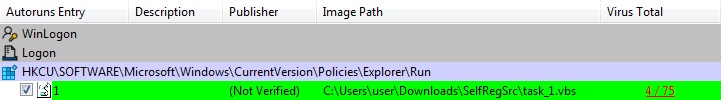


Рисунок 5 - Сравнение состояния автозагрузки

Программу Autoruns могут частично заменить Диспетчер задач на последних версиях OC Windows или настройка конфигурации системы в Windows 7 и более ранних системах. Также можно использовать редактор реестра, чтобы вручную редактировать раздел реестра, отвечающий за автозагрузку программ.

Программа Process Explorer имеет полный функционал Диспетчера задач, а также следующий ряд преимуществ:

* Проверка через Virus Total запущенных процессов
* Поиск процесса по названию
* Информация о PID номере процесса
* Просмотр dll и handle процессов
* Приостановка и перезапуск процессов
* Быстрый поиск информации о процессе в Интернете

Вредоносное приложение можно определить в Process Explorer по следующим признакам:

* Высока загрузка сети, диска, процессора или видеокарты
* Отсутствие описания процесса и разработчика ПО
* Непройденная проверка на Virus Total
* Загрузка подозрительных dll файлов

**Вывод**

Были изучены разделов конфигурации ОС семейства MS Windows, влияющих на автоматическую загрузку приложений при запуске ОС. Были исследованы утилиты **AutoRuns и Process Explorer**.

AutoRuns – бесплатная утилита для операционных систем Microsoft Windows, разработанная Sysinternals. Утилита способна управлять автозагрузкой программ, сервисов, модулей, драйверов и других компонентов системы. Autoruns отображает абсолютно всё, что будет запущено на компьютере при старте операционной системы, регистрации пользователя и других событиях.

Process Explorer — приложение для мониторинга процессов в системе. Используя эту программу, можно не только отследить какой-либо процесс, но и уточнить такие данные, как используемые этим процессом файлы и папки.