В то же время необходима гармонизация существующих нормативно-правовых актов для более эффективного и ускоренного инновационного развития Республики Беларусь.

Список использованных источников

1. Национальная стратегия устойчивого развития Республики Беларусь до 2035 года. https://economy.gov.by/uploads/files/ObsugdaemNPA/NSUR-2035-1.pdf - Дата доступа: 03.02.2025
2. Указ Президента Республики Беларусь от 3 января 2007 г. № 1 «Об утверждении Положения о порядке создания субъектов инновационной инфраструктуры»
3. Закон Республики Беларусь от 10 июля 2012 г. № 425-З «О государственной инновационной политике и инновационной деятельности в Республике Беларусь»
4. Постановление Совета Министров Республики Беларусь от 10 апреля 2007 г. № 459 «О мерах по реализации Указа Президента Республики Беларусь от 3 января 2007 г. № 1»
5. УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ№ 123 от 9 марта 2009 г. «О некоторых мерах по стимулированию инновационной деятельности в Республике Беларусь»
6. УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ОТ 7 августа 2012 г. № 357 «О порядке формирования и использования средств инновационных фондов»
7. УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ОТ 27 мая 2019 г. № 197 «О научной, научно-технической и инновационной деятельности»
8. УКАЗ ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ОТ 7 сентября 2009 г. № 441 «О дополнительных мерах по стимулированию научной, научно-технической деятельности»

УДК 681.3:553.98(574.4)

Г.К. Аррыкова, А.Р. Аннаева, С.О. Гелдиев, О.Д. Ныязгылыджева
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ПРОТИВОДЕЙСТВИЕ ВИРУСНОМУ ПРОГРАММНОМУ КОМПЛЕКСУ SYSTEM

Аннотация. *В статье исследуется работа вредоносного комплекса System и представлено программное решение для его полного удаления. Описаны механизмы маскировки вируса, принципы его обнаружения и этапы ликвидации через WinAPI и ShellAPI. Разработанная программа эффективно устраняет скрытые системные угрозы.*

G.K. Arrykowa, A.R. Annayeva, S.O. Geldiyev, O.D. Nyyazgylyjeva
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

COUNTERACTING THE SYSTEM MALICIOUS SOFTWARE COMPLEX

Abstract. *The article studies the behavior of the System malicious software complex and presents a program designed for its complete removal. It details the malware's masking mechanisms and step-by-step elimination using WinAPI and ShellAPI. The solution effectively removes hidden system threats.*

В данной работе была поставлена задача изучить работу вредоносного вирусного комплекса “System”, выполняющего шпионские функции b разработать мероприятия по его полному удаление из операционной системы.

В результате работы было создано программное обеспечение, которое с помощью функций ShellAPI и WinAPI точно определяет системный вредоносный вирус и полностью удаляет его из операционной системы [1].

Для начала была изучена природа данного вирусного программного обеспечения, его функционал и цели.

Загрузчик вируса генерирует файл autorun.inf и папку SYSTEM на всех локальных дисках компьютера, а также на подключенных носителях информации.

Основную работу вирусной системы выполняет explorer.exe. Рассмотрим подробнее этот вирусный файл.

Этот вредоносный файл маскируется под другой необходимый системный процесс, работая незаметно. Определить его активность по внешним признакам сложно, так как его разрушающие действия трудно выявить. Однако, разобравшись в его механизме, можно обнаружить и удалить этот вирус.

Файл explorer.exe имеет скрытые, системные и только для чтения атрибуты, что позволяет ему скрываться от пользователя, затруднять его удаление и защищаться от антивирусных программ.

Этот файл остается неактивным, пока пользователь сам его не запустит. При нажатии на него двойным щелчком мыши операционная

система Windows начинает перезагрузку проводника, для запуска других компонентов вредоносного комплекса.

Процесс загрузки Windows становится немного медленнее, и после завершения загрузки автоматически открывается окно "Мои документы". При проверке локальных дисков визуально никаких изменений не наблюдается [2].

При просмотре диспетчера задач (Ctrl+Alt+Del) и переходе во вкладку "Сведения", можно обнаружить два процесса с именем explorer.exe. Один из них — системный, а второй — ложный, вредоносный. Его необходимо немедленно завершить.

Но на этом процесс удаления не заканчивается. Нужно также удалить файл explorer.exe из папки D:\Windows\System32. Хотя он уже не представляет угрозы, наличие записи о нем в системе может привести к нежелательным последствиям.

Далее следует очистить autorun.inf и папку SYSTEM из корневых каталогов всех локальных дисков и подключенных носителей.

После выполнения этих действий вредоносная системная вирусная программа будет полностью удалена.

Для программирования процесса удаления необходимо определить его этапы [3]. Которые включают себя выполнение следующих задач:

- сначала определяется путь к файлу Explorer.exe, загружаемому из папки Windows\System32 на системном диске Windows;
- затем с помощью функции KillTask завершаются процессы с именем explorer.exe, работающие в оперативной памяти и поддерживающие вирусный комплекс;
- с помощью функции DeleteFiles удаляются файлы autorun.inf, находящиеся в корневых каталогах подключенных флеш-накопителей и локальных дисков, а специальные функции ShellAPI уничтожают вредоносные папки с названием SYSTEM.

Программа разработана в виде стандартного приложения Windows. Внешний вид программы представлен на следующем изображении (рис. 1).

Рис. 1- Дружественный интерфейс разработанной программы

При нажатии кнопки GÖZLEMEK (Проверить), если вирус обнаружен, на экране появится сообщение System. В этом случае необходимо нажать кнопку Ýok etmek (Удалить). Если же появится сообщение Wirus tapylmady (Вирус не найден), никаких действий предпринимать не нужно.

Если вирусное программное обеспечение обнаружено, то после нажатия кнопки Ýok etmek (Удалить) начнётся процесс проверки, и на экране будут отображаться названия проверяемых файлов. Если среди них будет обнаружен вирус, рабочий стол обновится (так как процесс Explorer.exe будет перезапущен).

Программа может использоваться во всех учреждениях и предприятиях для обнаружения и полного удаления скрытой шпионской вирусной системы, работающей в Windows в виде системных процессов.

Список использованных источников

1. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил.

2. "Possible Minds: Twenty-Five Ways of Looking at AI" by John Brockman (Editor) (2019).

3. M.Çuriýew, R.Mahmudow, J.Geldiýew. Kiberhowpsuzlyk. Ýokary okuw mekdepleri üçin okuw gollanmasy. A.: “Ylym”, 2023ý. – 340 s.