Список использованных источников

1. В России обсуждают потери ЕС от санкций. Европа лишилась миллиардов. Bbc.com. [Электронный ресурс]. URL: https://www.bbc.com/russian/news-50044439 (дата обращения: 11. 11. 2020.
2. Статья «Малый бизнес. Малое предпринимательство России» 2022 г. [Электронный ресурс] //https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9C%D0%B0%D0%BB%D1%8B%D0%B9_%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)
3. Бордуновский В. В., Сухаренко А. Н. Обеспечение экономической безопасности как стратегическая задача государства. 2017 г. // [Электронный ресурс] https://www.elibrary.ru/download/elibrary_32535094_29571816.pdf)
4. Развитие информационной экономики как системы, повышающей социализацию инвалидов. Шафранская Ч.Я., Абулханова Г.А. // «Преемственная система инклюзивного образования: взаимодействие специалистов разного профиля». Материалы VI Международной научно-практической конференции. Элиста. 2018. С. 422-425.
5. Социальное управление как инструмент сохранения человеческого капиталла в условиях пандемической реальности. Шафранская Ч.Я., Саяркина П.В. // «Тренды социально-экономического развития в условиях реального и виртуального мира». Материалы Национальной студенческой научно-практической конференции с международным участием. Редколлегия: К.Е. Бадмаева [и др.]. Элиста, 2021. С. 155-157.

УДК 681.3:553.98(574.4)

А.Д. Репова, С.С. Ораев,
Ч.Г. Гылычдурдыева, Д.М. Агаева
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ПРОФИЛАКТИКА КИБЕРАТАК

Аннотация. *В статье рассматриваются вопросы обеспечения кибербезопасности, проделан анализ основных причин и особенностей кибератак и кибервойн. Авторы дают описание особо важных для мониторинга ключей*

системного реестра. Также в работе представлено программное решение для профилактики и отражения некоторых угроз.

A.D. Repova, S.S. Orayev,
C.G. Gylychdurdyyeva, D.M.Agayeva
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

PREVENTION OF CYBER ATTACKS

Abstract. *The article deals with the issues of ensuring cybersecurity, an analysis of the main causes and features of cyber attacks and cyber wars is carried out. The authors give a description of the system registry keys that are especially important for monitoring. The paper also presents a software solution for the prevention and reflection of some threats.*

Защита информации всегда была приоритетной задачей для любой из областей человеческой деятельности. Особенно остро встал вопрос защиты информации в наше время – в период информатизации и компьютеризации. Появился новый вид угрозы информационной безопасности – кибератака, а также связанные с ней кибервойны. В киберпространстве могут развиваться все более опасные и сложные угрозы. Кибербезопасность имеет целью решение этих вопросов и обеспечение нормального функционирования киберпространства, защищая его от возникающих угроз эффективным образом, в том числе и от кибервойн [1].

Термин «кибервойны» прочно вошел в лексикон военных и специалистов по информационной безопасности, а также политиков, представителей экспертного сообщества. Средством боевого воздействия в кибервойнах является программный код, нарушающий работу, выводящий из строя, либо обеспечивающий перехват управления различного рода материальными объектами и сетями, оснащенными электронными системами управления.

Существует множество методов и технологий противодействия кибератакам, их сложность и эффективность зависят от профессионализма разработчиков, и конечно же от инвестиций. Не секрет, что самый эффективный способ борьбы с киберугрозами это профилактика и принятие мер на самих ранних стадиях начавшейся кибератаки.

В данной работе мы решились взяться за одну из самых больших проблем обеспечения кибербезопасности – это профилактика и своевременное обнаружение начавшейся и пока не разросшейся кибератаки. Для этого на языке программирования нами было разработано специальное программное обеспечение, которое способно

решить проблему своевременного обнаружения скрытой и потенциальной угрозы.

Основная цель данной работы заключается в том, чтобы показать что даже не владея особыми навыками программирования и опыта в сфере кибербезопасности, а применяя простую логику и доступные процедуры и программные коды, можно разработать свой собственный код по профилактике киберугрозы, не уступающий в отдельных частных случаях по эффективности признанным лидерам программной индустрии.

Цель программы, главное и единственное окно которого представлено на рисунке (рис. 1) – проведение профилактических мер и проверка перед использованием комплекта неизвестных файлов или файлов, загруженных из Интернета на предмет наличия среди них потенциальных загрузчиков и тел вирусов. Наша программа выполнена в виде стандартного Windows приложения.

Тут следует объяснить два момента. Что такое потенциальный загрузчик и что такое тело вируса? На практике много объяснений и определений, но, по нашему мнению, давать их нужно отталкиваясь от каждого конкретного случая. Итак, потенциальный загрузчик – программа, внешне не имеющая признаков исполняющегося файла и загружаемая при запуске пользователем в оперативную память. Обычно имеет иконку какого-нибудь документа популярного редактора (например, MS Word), загружаясь «впрыскивает» вредоносный код в систему, заражая загружаемые файлы.

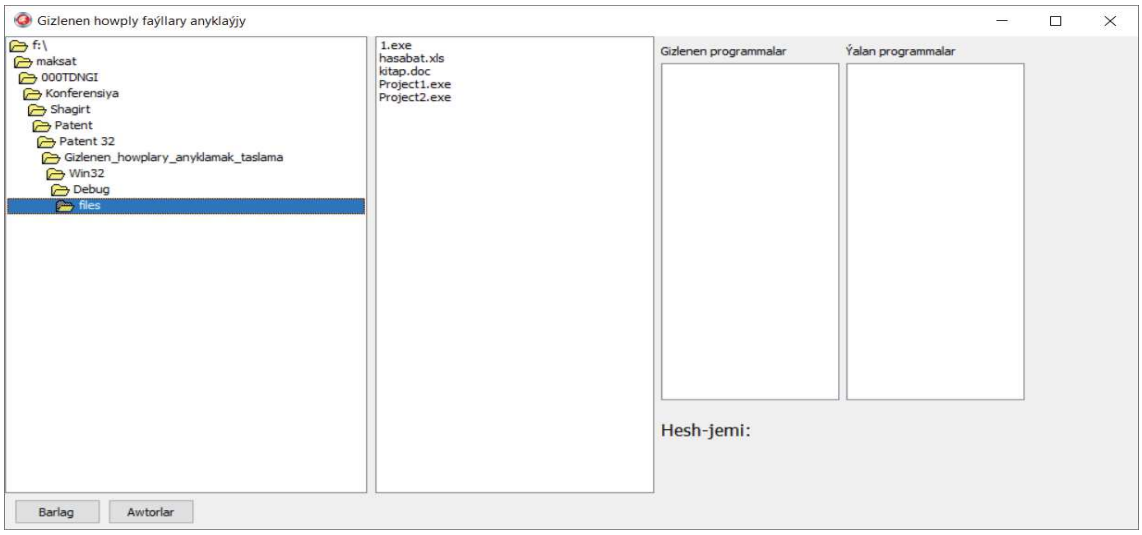

Рис. 1 - Внешний вид программы

Другой случай - тело вируса. Это неисполняемый файл, однако имеющий внешние признаки исполняемого файла (например расширение *.exe). При запуске пользователем или внешней

программой, сама не загрузится, однако внутри нее скомпилируется ее вредоносная часть кода. Таким образом оба вида вредоносных программ рассчитывают на неосторожность пользователя. Следует отметить, что в повседневной жизни, работая в Интернете, локальной сети или просто на локальном компьютере мы сталкиваемся с сотнями подобного рода файлов. Их количество настолько велико, что современные антивирусные сканеры и мониторы просто не успевают вовремя их выявлять. Однако определить такие файлы даже неопытному пользователю не составляет никакого труда.

Например, откроем через стандартную программу «Блокнот» (Notepad) машинозапись кода любой из программы (рис. 2). Как видно из рисунка – первые два байта машинного кода нашей программы составляет слово или запись MZ. Это и есть цифровая подпись исполняемого файла или PE файла (Portable Executeble). Таким образом наша идея и алгоритм программы достаточно прост – мы проверяем расширение файла на предмет его соответствия исполняемому файлу или программе, далее считываем первые два байта машинного кода нашего файла и проверяем их на предмет соответствия цифровой подписи MZ. Если файл не имеет внешних признаков программы, однако первые байты его кода равны MZ, значит он потенциальный загрузчик, и наоборот если файл имеет внешние признаки программы, однако у него нет цифровой подписи MZ, значит он ложная программа или тело вируса.

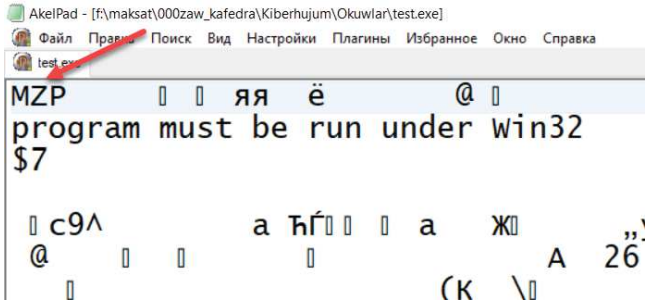

Рис. 2 - Цифровая подпись программы (MZ)

Конечно, данная процедура имеет свои недостатки, выраженные в том, что при большом количестве данного рода фалов, пользователь просто может не успеть их всех проверить. Вот для этого то и была разработана наша программа.

Программа последовательно открывает каждый файл размещенный в указанной папке, считывает с помощью WinAPI функций цифровую подпись файлов [3], и если файл имеет цифровую подпись исполняющего файла, а его расширение другое, то программа размещает его в списке скрытых программ (потенциальных троянов и

загрузчиков вирусов), и наоборот, если файл не являясь исполняемым, имеет расширение исполняемого файла, то программа размещает его в списке ложных программ (потенциальных тел вируса). Ниже на рисунке (рис.3) показан результат одной из проверки, в которой было определено две скрытых программ и одна ложная программа.

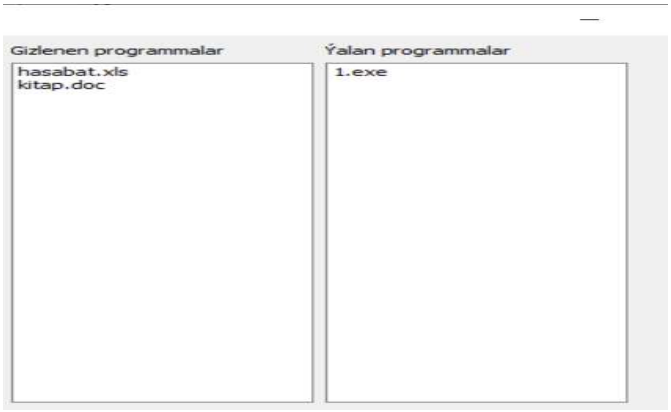

Рис. 3

Программа способна за 5-10 секунд «прочитать» папку содержащую около 100 файлов. Помимо этого программа способна определить Хэш-сумму указанного файла с помощью алгоритма MD5 [4].

Область применения программы - любое предприятие-организация в независимости от ведомственной принадлежности и форм собственности. Программа может быть использована как средство выявления первой стадии кибератаки – шпионажа, а также как средство соблюдения правил по кибербезопасности.

Данная программа очень хорошо себя зарекомендовала, позволив автоматизировать процесс домашнего «аудита» пользовательских папок и файлов, в соответствующем порядке на нее был получен патент (№ 206).

Список использованных источников

1. Сикорски М., Хониг Э. Вскрытие покажет! Практический анализ вредоносного ПО. — СПб.: Питер, 2018. — 768 с.: ил. — (Серия «Для профессионалов»).
2. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. – М.: ДМК Пресс, 2019. – 452 с.: ил.
3. M. Çuriýew. Maglumatlaryň gory we banklary. Ýokary okuw mekdepleri üçin okuw kitaby.- A.: „Ylym“ neşirýaty, 2015.
4. А.Я. Архангельский. Программирование в Delphi. М., Издательство БИНОМ, 2008.