



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)


ОТЧЁТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Тип практики: производственная

Название предприятия: АО «НПО «Эшелон»


Студент:

Яровиков Андрей Сергеевич,
группа ИУ8-62 (3 курс)

 18.07.21
(подпись, дата)

Руководитель от предприятия:

ведущий разработчик, Борzych Сергей Сергеевич

 18.07.21
(подпись, дата)

Руководитель от кафедры:

доцент кафедры ИУ8, Заичева Анастасия Владленовна

(подпись, дата)

Оценка:

Отлично





Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

Тип практики: производственная

Название предприятия: АО «НПО «Эшелон»

Сроки практики: с 05 июля 2021 г. по 18 июля 2021 г.


Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

За время прохождения практики студенту надлежит согласно программе практики:

- Изучить программу-вымогатель Netwalker и способы защиты от него.


Студент:

Яровиков Андрей Сергеевич,
группа ИУ8-62 (3 курс)

 18.07.21
(подпись, дата)

Руководитель от предприятия:

ведущий разработчик, Борзых Сергей Сергеевич

 18.07.21
(подпись, дата)

Руководитель от кафедры:

доцент кафедры ИУ8 Запцева Анастасия Владленовна

(подпись, дата)

Оценка: 



Является обязательным листом отчёта по практике. Лист 2

Документ не должен содержать информацию, отнесённую в установленном порядке к государственной тайне РФ.

Оглавление

Введение.....	4
Основная часть	5
1. Характеристика организации.....	5
2. Практическая часть	6
Заключение	15
Список использованных источников	16

Введение

Целью данной работы является комплексное изучение работы программы-вымогателя Netwalker:

- Что из себя представляет программа-вымогатель Netwalker;
- На кого и на что нацелена программа Netwalker;
- Как программа Netwalker проникает и шифрует данные;
- Как защитить данные от вредного воздействия программы Netwalker;

Основная часть

1. Характеристика организации

НПО Эшелон — один из лидеров российского рынка информационной безопасности. Команда объединяет профессионалов, имеющих различные звания и статусы, среди которых: кандидаты наук, CISSP, CISA, SBCI и сертифицированные специалисты Cisco, IBM, Microsoft и др. Компания «Эшелон» аккредитована в качестве испытательной лаборатории Минобороны России, ФСТЭК России, ФСБ России. ЗАО «НПО «Эшелон» является органом по сертификации ФСТЭК России, органом по аттестации ФСТЭК России и аттестационным центром Минобороны России[1].

АО «НПО «Эшелон» специализируется на комплексном обеспечении информационной безопасности[2].

Основными направлениями деятельности являются:

- проектирование, внедрение и сопровождение комплексных систем обеспечения информационной безопасности;
- сертификация программных и программно-аппаратных средств;
- аттестация объектов информатизации, в том числе защищенных помещений, автоматизированных рабочих мест, локальных вычислительных сетей;
- проведение анализа защищенности компьютерных систем;
- аудит информационной безопасности организаций;
- поставка оборудования и средств защиты информации;
- выстраивание процессов безопасной разработки;
- аудит информационной безопасности программного обеспечения, а также банковских приложений;

2. Практическая часть

На 1 этапе разберемся, что такое программа-вымогатель Netwalker.

Netwalker – это быстро набирающая масштабы программа-вымогатель, созданная в 2019 году группой киберпреступников, известной как Circus Spider.

На первый взгляд Netwalker действует, как и большинство других разновидностей программ-вымогателей: проникает в систему через фишинговые письма, извлекает и шифрует конфиденциальные данные, а затем удерживает их для получения выкупа. Но одновременно с этим Circus Spider публикует образец украденных данных в интернете, заявляя, что, если жертва не выполнит их требования вовремя, то в даркнет попадут и остальные данные (рис.1). Киберпреступники выкладывают конфиденциальные данные жертвы в даркнете в защищенной паролем папке и публикует пароль в интернете. К тому же программа-вымогатель Netwalker использует модель «вымогательство как услуга» (RaaS). Это означает, что помимо команды разработчиков (Circus Spider), вербуются помощники для содействия, что приводит к расширению масштабов Netwalker, что позволяет нацелиться на большее количество организаций и увеличить размеры получаемых выкупов.

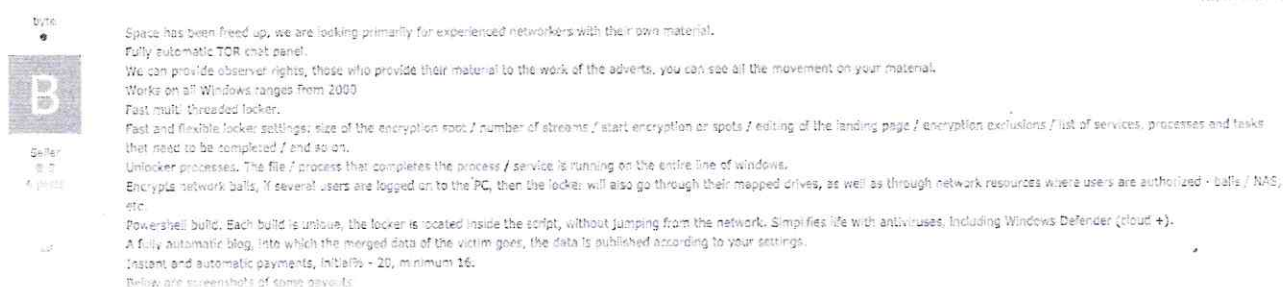


Рис.1. Угроза публикации конфиденциальных данных

На 2 этапе необходимо понять, на какие сферы нацелен Netwalker.

В первую очередь, целями Netwalker стали учреждения здравоохранения и образования. Программа-вымогатель похитила конфиденциальные данные одного из университетов, и, чтобы показать серьезность намерений, злоумышленники выложили образец украденных данных в открытый доступ.

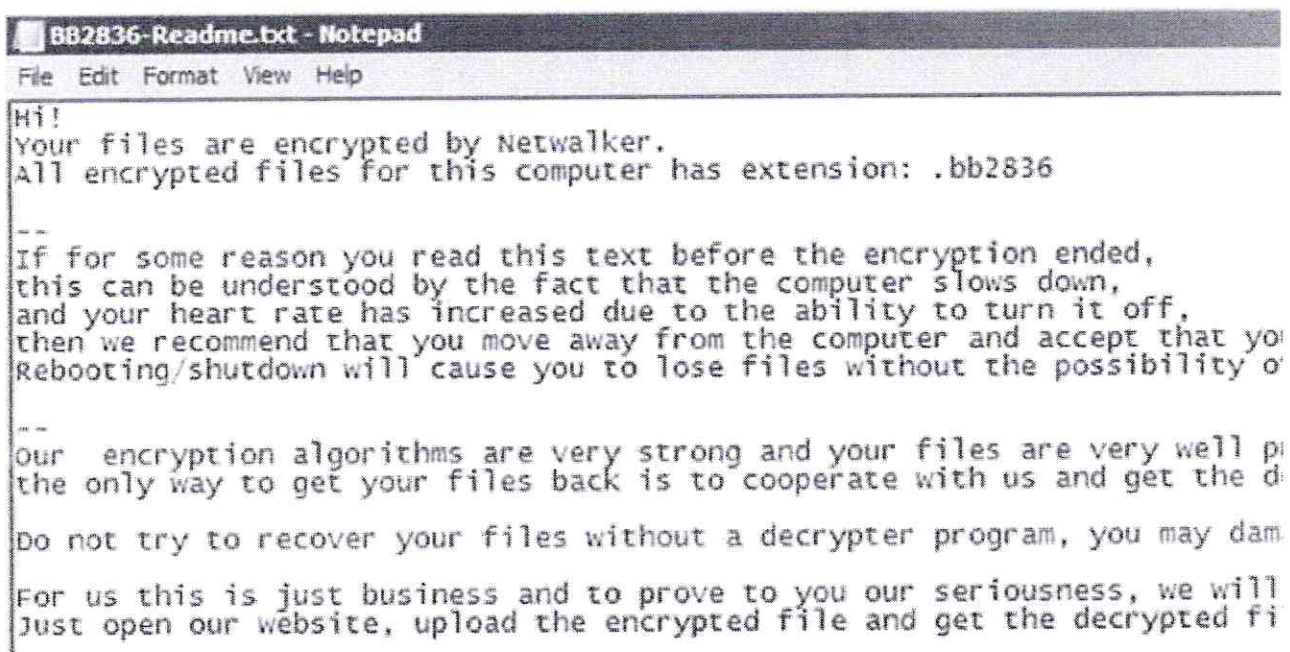
Эти данные включали студенческие приложения, содержащие такую

информацию, как номера социального страхования и другие конфиденциальные данные. Это нарушение привело к тому, что университет заплатил злоумышленникам выкуп в размере 1,14 миллиона долларов за расшифровку их данных.

Также злоумышленники, стоящие за Netwalker, предприняли серьезную попытку извлечь выгоду из хаоса эпидемии коронавируса. Они рассылали фишинговые электронные письма на тему пандемии, выбрав целью медицинские учреждения, которые уже перегружены пострадавшими от пандемии (рис.2). Сайт одной из первых жертв был заблокирован программой-вымогателем как раз в тот момент, когда люди начали обращаться к ним за советом во время пандемии. Эта атака вынудила жертву запустить второй сайт и направить пользователей на новый, вызвав беспокойство и замешательство у всех участников.

Помимо сфер здравоохранения и образования, Netwalker атакует организации в других отраслях, в том числе[3]:

- производство;
- управление бизнесом;
- управление потребительским опытом и качеством обслуживания;
- электромобили и решения для накопления электричества;
- образование;



```
BB2836-Readme.txt - Notepad
File Edit Format View Help

Hi!
Your files are encrypted by Netwalker.
All encrypted files for this computer has extension: .bb2836

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you
Rebooting/shutdown will cause you to lose files without the possibility of

--
our encryption algorithms are very strong and your files are very well pr
the only way to get your files back is to cooperate with us and get the d
Do not try to recover your files without a decrypter program, you may dam
For us this is just business and to prove to you our seriousness, we will
Just open our website, upload the encrypted file and get the decrypted fi
```

Рис.2. Атака на калифорнийский медицинский центр UCSF

На 3 этапе разберемся, как работает программа-вымогатель Netwalker.

Первый шаг заключается в проникновении вредоносной программы в систему. Netwalker в значительной степени полагается на фишинг и адресный фишинг. Если сравнивать с другими программами-вымогателями, рассылки фишинговых писем у Netwalker происходят гораздо чаще. Эти письма выглядят вполне безобидно, что легко вводит в заблуждение жертв. Обычно Netwalker прикрепляет сценарий VBS с названием *CORONAVIRUS_COVID-19.vbs*, который запускает программу-вымогатель, если получатель откроет вложенный текстовый документ с вредоносным сценарием (рис3).


```
44944, 44100, 44944, 44944, 42025, 44944, 44944, 42436, 44100, 42849, 44944, 44944, 42025, 42025,
43264, 44521, 42849, 44521, 43681, 42436, 44944, 44944, 43681, 43264, 44521, 44944, 44100, 43264,
42025, 42436, 42025, 42436, 42436, 42849, 43264, 42849, 43264, 43681, 43681, 44100, 44944, 42436,
44944, 42025, 44944, 41616, 41616, 41616, 41616, 44944, 44100, 43681, 44944, 42025, 44100, 42436,
42025, 41616, 42849, 42849, 42849, 44944, 42849, 44100, 43264, 42849, 44944, 42436, 41616, 41616,
43681, 44100, 44521, 42436, 42436, 44100, 43264, 42849, 44521, 44521, 43681, 44100, 44521, 42025,
42849, 44100, 42849, 44521, 43681, 44944, 44944, 41616, 44100, 41616, 44100, 42849, 43264, 43264,
43264, 42849, 41616, 42436, 42436, 43681, 42436, 44521, 41616, 42849, 44944, 42025, 42849, 43264,
44100, 41616, 44944, 44944, 42436, 44100, 41616, 42849, 44944, 42436, 42849, 42025, 44100, 44521,
43681, 43681, 44944, 42436, 44944, 43681, 44100, 42849, 42436, 44100, 41616, 43681, 42436, 41616,
43264, 43681, 42025, 43264, 42436, 42849, 44944, 42025, 42025, 42436, 42025, 41616, 44521,
44521, 44521, 43681, 44944, 44100, 43264, 43681, 44944, 43681, 44100, 42025, 43681,
44944, 42849, 44521, 43681, 43681, 44521, 44944, 41616, 44944, 42849, 42849, 44521, 42436, 42849,
43681, 43264, 43681, 41616, 42025, 44521, 43264, 43681, 42436, 43264, 43681, 44521, 42436, 42025,
44100, 42849, 42849, 43681, 43681, 44100, 44944, 41616, 43264, 44944, 44521, 43681, 44521,
44521, 44100, 44100, 42849, 43681, 44521, 43264, 43681, 43264, 41616, 44521, 44944, 44944, 44944,
42436, 44521, 41616, 42849, 42849, 42849, 43681, 42025, 41616, 42436, 43264, 42025, 42849, 42436,
41616, 41616, 41616, 42849, 42436, 42849, 44944, 43264, 44521, 44944, 43264, 42849, 44521, 43264,
44944, 42849, 42849, 43681, 43681, 42025, 41616, 42849, 41616, 41616, 42025, 44100, 44944, 44521,
43681, 44944, 43681, 44521, 43264, 42025, 44944, 43264, 44944, 44944, 42436, 44521, 44100, 42025,
42436, 44521, 42436, 41616, 44944, 42436, 41616, 44521, 42436, 43681, 42025, 41616, 44100, 43264,
44100, 43264, 41616, 44521, 42436, 42436, 43264, 44521, 44944, 44100, 42025, 41616, 44521, 44944,
44521, 42849, 44521, 44944, 43681, 43681, 44100, 44100, 42025, 42849, 42025, 42436, 43681,
43264, 42436, 44944, 44521, 44521, 41616, 42025, 42025, 43681, 41616, 42025, 42849, 44944, 44521,
43264, 43681, 44944, 43681, 44944, 43264, 44100, 43681, 42849, 43264, 42436, 42025, 44944, 44100,
41616, 44521, 42025, 41616, 41616, 41616, 44944, 42436, 44521, 44100, 41616, 42436, 43264, 42025,
42025, 44100, 44044, 42025, 43681, 44100) : for nqhICuKfVmaJBtUKVvHLjwNRPgMyriPbIQgnzQg = Ibound(
UHSCKpiIgyaYOXAgGwNbKK) to ubound(YechKJPerXvgZDJbI) : noXghCyOTjVIDXiOCTQYgyNMmbH = sqr(
UHSCKpiIgyaYOXAgGwNbKK(nqhICuKfVmaJBtUKVvHLjwNRPgMyriPbIQgnzQg)) : ikWqcctDAwibpoPQNwYay = sqr(
YechKJPerXvgZDJbI(nqhICuKfVmaJBtUKVvHLjwNRPgMyriPbIQgnzQg)) : execute(
"nnWNUPyWYacQFPZdjUGTLkvGZYqouHxb = nnWNUPyWYacQFPZdjUGTLkvGZYqouHxb &
chr(noXghCyOTjVIDXiOCTQYgyNMmbH - ikWqcctDAwibpoPQNwYay)") : next : execute(
nnWNUPyWYacQFPZdjUGTLkvGZYqouHxb)
```

Рис.3. Сценарий VBS для запуска Netwalker

Если такой сценарий открывается и запускается в системе, это означает что Netwalker начал проникать в сеть системы и с этого момента начинается отсчет времени до шифрования файлов в этой системе.

На **втором шаге** программа-вымогатель, попав в систему, превращается в не вызывающий подозрений процесс, обычно в виде исполняемого файла Microsoft (рис.4). Это достигается за счет удаления кода из исполняемого файла и внедрения в него собственного вредоносного кода. Благодаря такому методу Netwalker получает возможность находиться в сети достаточно долго для извлечения и шифрования данных, удаления резервных копий и создания лазеек на случай, если кто-либо заметит, что что-то не так (рис.5).

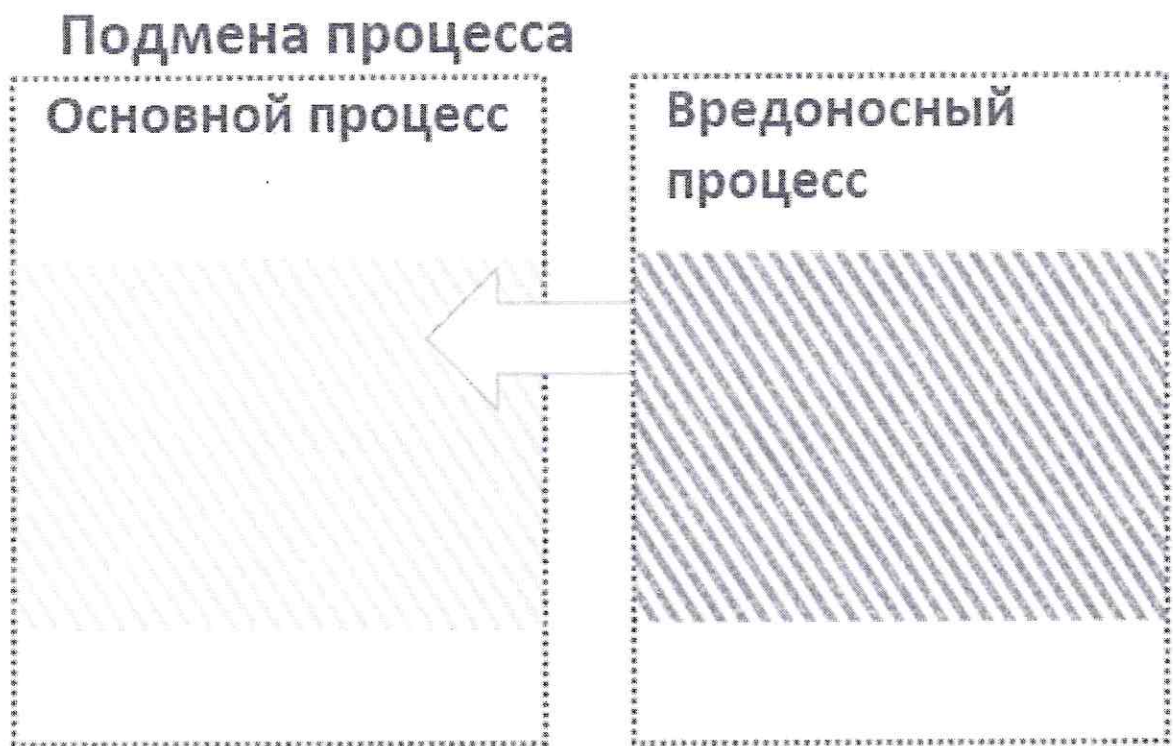


Рис.4. Процесс удаления кода из исполняемого файла и внедрения в него собственного вредоносного кода

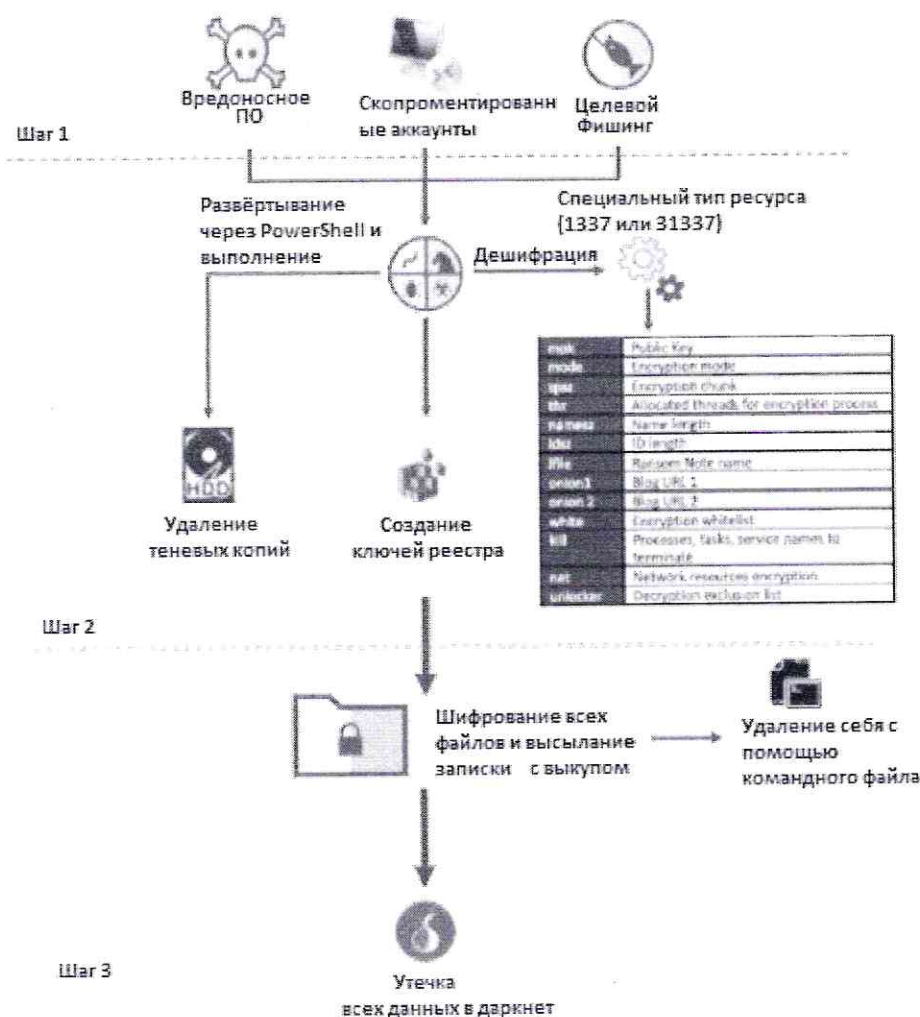


Рис.5. Схема конкретного пути атаки Netwalker

Для извлечения и шифрации данных в Netwalker задействован специальный тип ресурса (1337 или 31337), содержащий всю его конфигурацию[4]. Этот файл извлекается в память и дешифруется с жестко закодированным ключом в ресурсе (рис.6). Сам по себе Netwalker представляет собой двоичный 32-битный файл, который можно найти как EXE-файл (рис.7).

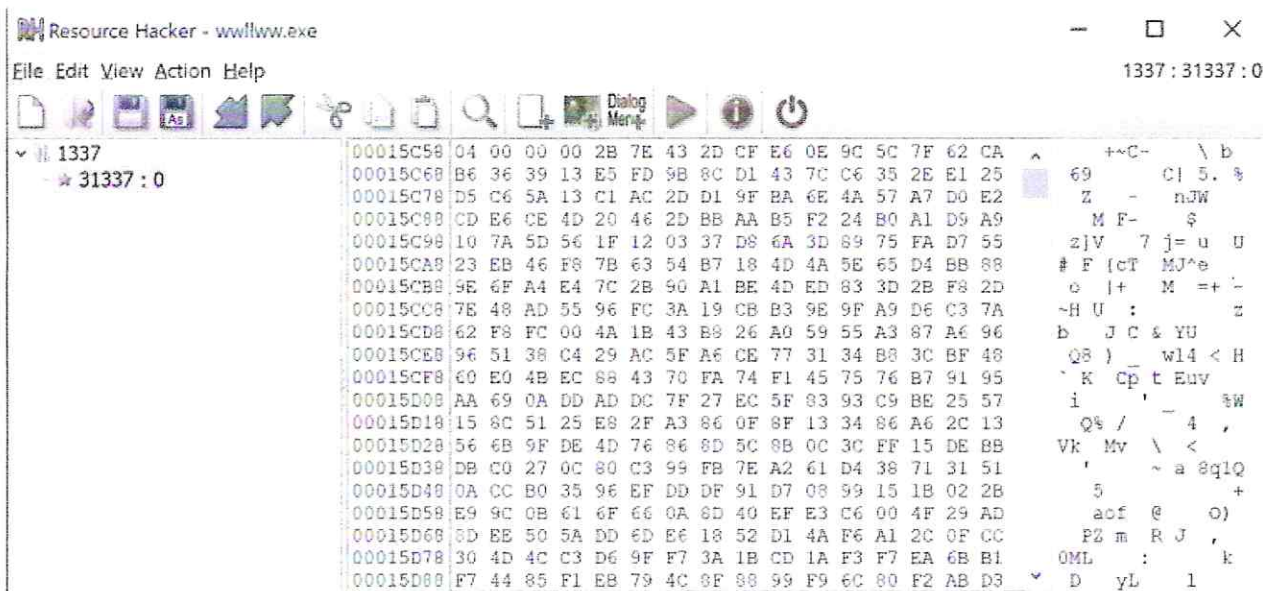


Рис.6. Файл конфигурации программы-вымогателя Netwalker

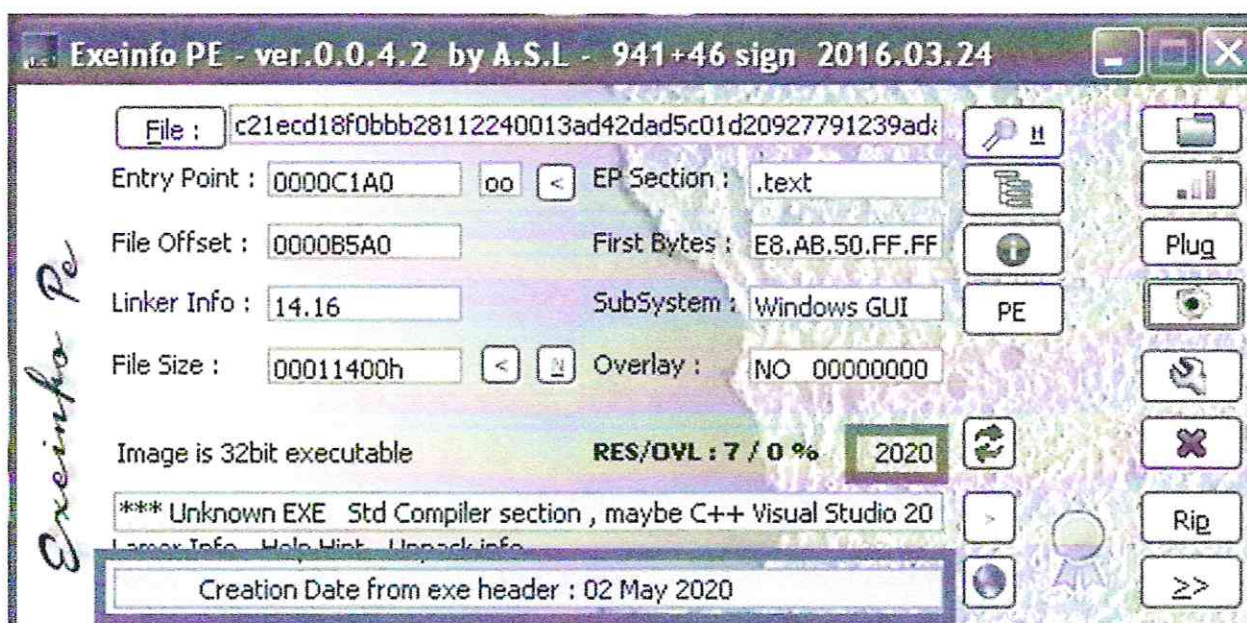


Рис.7. 32-битный EXE-файл Netwalker

На **третьем шаге** после шифрования данных, жертва обнаружит, что данные украдены, и найдет записку с требованием выкупа (рис.8). Записка с требованием выкупа Netwalker относительно стандартна: в ней объясняется произошедшее и что пользователь должен делать, если хочет вернуть свои данные в целости и сохранности. Затем киберпреступники потребуют определенную сумму денег для оплаты в биткоинах, используя браузер TOR.

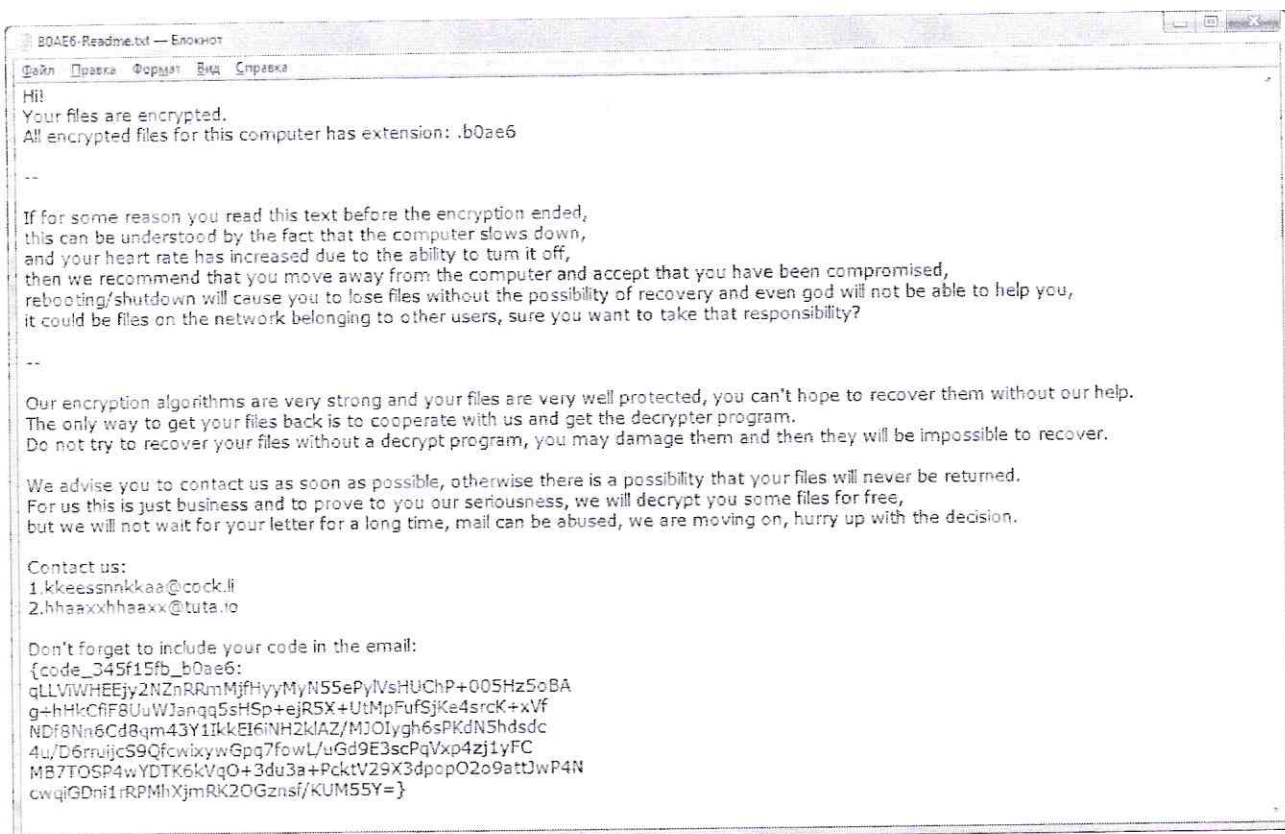


Рис.8. Записка с требованием выполнения условий киберпреступников

Как только жертва удовлетворяет выдвинутые требования, она получает доступ к своему индивидуальному инструменту дешифрования и может безопасно расшифровать свои данные.

Если жертва не выполнит требования вовремя, злоумышленники увеличат размер выкупа или опубликуют в даркнете все украденные данные либо их часть.

На 4 этапе разберемся, как противодействовать программе-вымогателю Netwalker.

Для того чтобы защитить систему и данные от Netwalker необходимо прежде всего[5]:

- Никогда не переходить по небезопасным ссылкам — избегать перехода по ссылкам в спам-сообщениях или на неизвестных веб-сайтах. При переходе по вредоносным ссылкам может начаться

автоматическая загрузка, что может привести к заражению системы и потере данных;

- Никогда не открывать подозрительные вложения в сообщениях электронной почты – убедиться в доверенности сообщения электронной почты следует обратить внимание на адрес отправителя;
- Установить и регулярно обновлять антивирусное ПО – чтобы своевременно проверить и ликвидировать небезопасную программу;
- Регулярно обновлять компьютеры, устройства и приложения – Netwalker, как и другие программы-вымогатели, использует уязвимости в системах и инфраструктуре, чтобы взять под контроль компьютеры пользователей и целые сети;

Также следует:

- Выполнять резервное копирование важных данных на локальные хранилища данных;
- Убедиться, что копии критически важных данных хранятся в облаке, на внешнем жестком диске или устройстве хранения;
- Защитить резервные копии и убедиться, что данные невозможно изменить или удалить из системы, в которой они хранятся;

Заключение

В результате выполнения практики были реализованы поставленные цели и задачи:

- Было изучено, чем является программа-вымогатель Netwalker;
- Было выяснено на кого и на что нацелена программа-вымогатель Netwalker;
- Была освоена работа программы-вымогателя Netwalker. Из-за чего происходит заражение системы и с помощью чего шифруются данные;
- Было выяснено, какие меры следует предпринять, чтобы защитить систему и данные;

Список использованных источников

- 1) Характеристика АО «НПО «Эшелон». – Режим доступа:
<https://ru.bmstu.wiki/%D0%9D%D0%9F%D0%9E%D0%AD%D1%88%D0%B5%D0%BB%D0%BE%D0%BD> (дата обращения: 14.07.2021)
- 2) Основные направления деятельности АО «НПО «Эшелон». – Режим доступа: <https://npo-echelon.ru/about> (дата обращения: 14.07.2021)
- 3) Руководство по программе-вымогателю Netwalker. – Режим доступа:
<https://www.varonis.com/blog/netwalker-ransomware> (дата обращения: 14.07.2021)
- 4) Руководство по программе-вымогателю Netwalker. – Режим доступа:
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side> (дата обращения: 14.07.2021)
- 5) Руководство по противодействию программе-вымогателю Netwalker. – Режим доступа: <https://www.ncsc.org/trends/monthly-trends-articles/2020/netwalker-ransomware> (дата обращения: 14.07.2021)