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:
Разина Анастасия Георгиевна,
группа ИУ8-62 (3 курс)

(подпись, дата)

Руководитель от предприятия:
ведущий разработчик, Борзых Сергей Сергеевич

(подпись, дата)

Руководитель от кафедры:
доцент кафедры ИУ8 Зайцева Анастасия Владленовна

(подпись, дата)

Оценка: хорошо

Москва, 2021

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 22 июля 2021 г. по 04 августа 2021 г.

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

За время прохождения практики студенту надлежит согласно программе практики:

- **Изучить** программу-вымогатель Ryuk и способы защиты от нее.

Студент:
Разина Анастасия Георгиевна,
группа ИУ8-62 (3 курс)

04.02.21
(подпись, дата)

Руководитель от предприятия: ведущий разработчик, Борзых Сергей Сергеевич

04.02.21
(подпись, дата)

Руководитель от кафедры: доцент кафедры ИУ8
Зайцева Анастасия Владленовна

(подпись, дата)

Оценка: хорошо

Является обязательным листом отчёта по практике. Лист 2
Документ не должен содержать информацию, отнесённую в установленном порядке к государственной тайне РФ.

Оглавление

Введение

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

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

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

Общие сведения о программе-вымогателе Ryuk.

Ryuk — программа-вымогатель, которая шифрует файлы и требует у жертвы выкуп в криптовалюте Bitcoin за предоставление ключей для дешифровки. Используется трой исключительно для целевых атак. Впервые этот вымогатель выявили в августе 2018 года.

Изначально предполагалось, что он имеет связь с северокорейской группировкой Lazarus, однако в последнее время Ryuk подозревали в том, что он был разработан двумя или более российскими преступными картелями. С помощью проведенного анализа первоначальных версий вредоносного ПО были выявлены сходства и общие фрагменты исходного кода с программой-вымогателем Hermes. Hermes — вымогатель массового распространения, который продается на подпольных форумах и используется несколькими группами хакеров. В отличие от многих других злонамеренных компьютерных хакеров, преступная группа Рюк в первую очередь стремится вымогать выкуп, чтобы раскрыть данные, которые ее вредоносное ПО сделало бесполезным с помощью шифрования. [3]

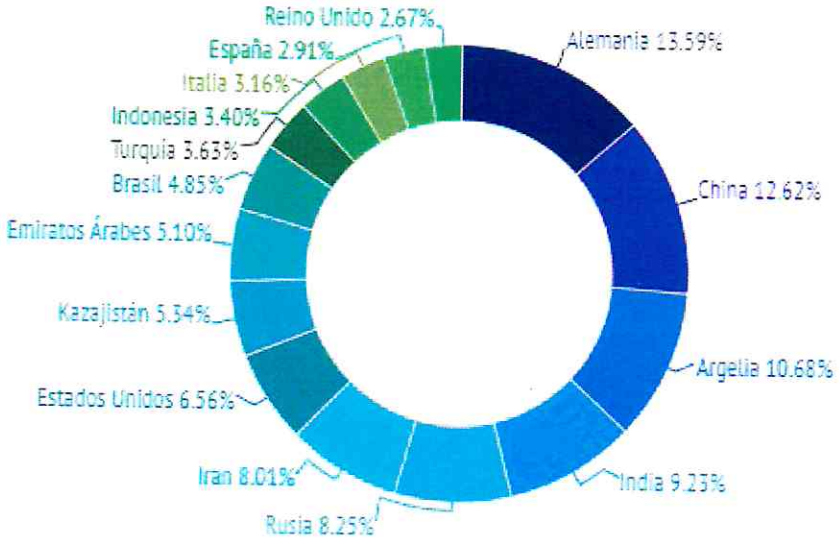


Рис.1. 16 стран, наиболее пострадавших от Ryuk

На какие сферы нацелен Ryuk.

Ryuk рекламировался как шифровальщик, который не будет работать на российских, украинских и белорусских системах. Такое поведение определяется функцией, обнаруженных в некоторых версиях Ryuk, где она проверяет язык системы, в которой запущен данный шифровальщик, и останавливает его работу в том случае, если у системы русский, украинский или белорусский язык. [3]

Ryuk нацелен на крупные организации, способные платить значительные суммы денег, чтобы восстановить доступ к своим ценным данным. В целом, по данным ФБР, за атаки вредоносного ПО Ryuk в 2018–2019 годах было выплачено более 61 миллиона долларов выкупа. В декабре 2018 года атака на Рюке затронула издание Los Angeles Times и газеты по всей стране с использованием программного обеспечения Tribune Publishing. После атаки Рюк был охарактеризован как «одна из самых опасных групп программ-вымогателей, которые действуют посредством фишинговых кампаний».

В период с 2019 по 2020 год больницы США в Калифорнии, Нью-Йорке и Орегоне, а также в Великобритании и Германии были затронуты вредоносным ПО Ryuk, что привело к затруднениям с доступом к записям пациентов и даже ухудшению оказания неотложной помощи. Врачи в пострадавших больницах писали инструкции на бумаге вместо того, чтобы пользоваться своими вышедшими из строя компьютерами. В США 29 октября 2020 года три федеральных правительственных агентства, ФБР, CISA и Министерство здравоохранения и социальных служб выпустили совместное заявление, в котором предупреждали, что больницам следует ожидать увеличения и неминуемая «волна кибератак с использованием программ-вымогателей, которые могут поставить под угрозу лечение пациентов и раскрыть личную информацию», вероятно, из-за атак Ryuk. В конце 2020 года более десятка американских больниц подверглись атакам Рюка, в результате чего был закрыт

доступ к записям пациентов и даже прекращено лечение больных раком химиотерапией.

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

- производство;
- образование;
- правительственные учреждения;
- управление бизнесом.

Пример записки, оставленной вымогателями:

"Все файлы на каждом хосте в сети зашифрованы с помощью надежного алгоритма.
Резервные копии были либо зашифрованы, либо удалены, либо диски резервных копий были отформатированы.
Теневые копии также удаляются, поэтому F8 или любые другие методы могут повредить зашифрованные данные, но не восстановить.
У нас есть эксклюзивное программное обеспечение для дешифрования, подходящее для вашей ситуации.
Общедоступного программного обеспечения для дешифрования нет.
НЕ СБРОСИВАЙТЕ И НЕ ВЫКЛЮЧАЙТЕ - файлы могут быть повреждены.
НЕ ПЕРЕИМЕНОВАТЬ И НЕ ПЕРЕМЕЩАТЬ зашифрованные файлы и файлы readme.
НЕ УДАЛЯЙТЕ файлы readme.
Это может привести к невозможности восстановления определенных файлов.
Чтобы получить информацию (расшифровать файлы), свяжитесь с нами по адресу
MelisaPeterman@protonmail.com или же MelisaPeterman@tutanota.com
Кошелек BTC: 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
Рюк
Никакая система не является безопасной »

В более новых версиях Ryuk отображается записка с требованием выкупа, содержащая только адреса электронной почты, но не адреса кошелька BTC. [4]

Принцип работы программы-вымогателя Ryuk.

Характеристики: Начинается работа с загрузчика, чья задача заключается в том, чтобы идентифицировать систему, в которой он находится, чтобы можно было запустить «правильную» версию шифровальщика Ryuk. Хэш загрузчика следующий: MD5 A73130B0E379A989CBA3D695A157A495 SHA256 EF231EE1A2481B7E627921468E79BB4369CCFAEB19A575748DD2B664ABC469 [3]

Одна из особенностей этого загрузчика заключается в том, что он не содержит никаких мета-данных, т.е. создатели этой вредоносной программы не включили в него никаких сведений. Иногда они включают ошибочные данные для того, чтобы заставить пользователя думать, что он запускает легитимное приложение. Однако, в том случае, если заражение не предполагает взаимодействие с пользователем (как в случае с этим шифровальщиком), то злоумышленники не считают необходимым использовать мета-данные (рис 3).

Рис.3. Мета-данные образца

Загрузчик: Образец, который загружает и запускает Ryuk, попал в систему через удаленное соединение, а параметры доступа были получены благодаря предварительной RDP-атаке. Когда загрузчик выполняется, он записывает файл ReadMe в папку %temp%, что типично для Ryuk. Данный файл — это требование о выкупе, содержащее адрес электронной почты в домене protonmail, который довольно часто встречается в этом семействе вредоносных программ. Во время выполнения загрузчика можно увидеть, что он запускает несколько исполняемых файлов со случайными названиями. Они хранятся в скрытой папке PUBLIC, но если в операционной системе не активна опция «Показывать скрытые файлы и

папки», то они так и останутся скрытыми. Более того, эти файлы 64-разрядные в отличие от родительского файла, который 32-разрядный.

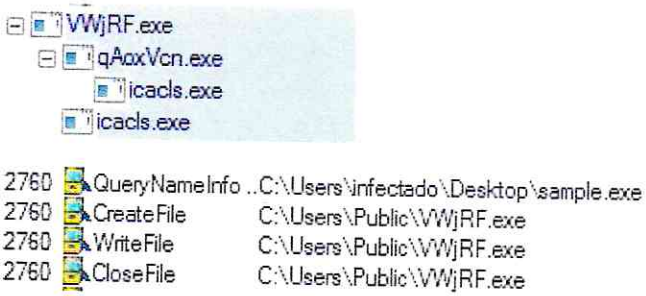


Рис.4. Исполняемые файлы, запускаемые образцом

Ryuk запускает icacls.exe, который будет использоваться для изменения всех списков контроля доступа ACL (Access control list), таким образом гарантируя доступ и изменение флагов. Он получает полный доступ под всеми пользователями ко всем файлам на устройстве (/T) независимо от ошибок (/C) и без показа каких-либо сообщений (/Q). Важно учитывать, что Ryuk проверяет, какая запущена версия Windows. Для этого он выполняет проверку версии с помощью GetVersionExW, в котором он проверяет значение флага lpVersionInformation, показывающего, является ли текущая версия Windows более поздней, чем Windows XP. [3]

```
mov     edi, [ebp+var_40]
mov     ecx, 13h
mov     esi, offset aDocumentsAndSe ; "C:\Documents and Settings\Default User"...
rep movsd
jmp     short loc_401572
```

```
mov     edi, [ebp+var_20]
mov     ecx, 7
mov     esi, offset aUsersPublic ; "C:\Users\Public\"...
rep movsd
movsw
```

Рис.5. Проверка операционной системы

В зависимости от того, работает ли более поздняя версия нежели Windows XP, загрузчик будет записывать в папку локального пользователя.

Записываемый файл — это Ryuk запуская его, передается собственный адрес в качестве параметра. Первое, что делает Ryuk, — это получение входных параметров. В рассмотренном примере существуют два входных параметра (сам исполняемый файл и адрес дроппера), которые используются для удаления собственных следов.

Присутствие: Для скрытного создания и запуска исполняемых файлов наиболее распространенной практикой является изменение ключа

реестра CurrentVersion\Run. В данном случае для этой цели первый запускаемый файл VWjRF.exe (название файла генерируется случайным образом) запускает cmd.exe.

Рис.6. Выполнение файла VWjRF.exe

Затем вводится команда RUN с именем "svchos". Таким образом, если в любое время проверить ключи реестра, достаточно легко не заметить это изменение, учитывая схожесть этого названия с svchost. Благодаря этому ключу Ryuk обеспечивает свое присутствие в системе. Если система до сих пор не была заражена, то при ее перезагрузке, исполняемый файл повторит попытку снова, он останавливает две службы: "audioendpointbuilder", которая, как следует из ее названия, соответствует системному аудио, и samss, которая является службой управления учетными записями. Остановка этих двух служб является характеристикой Ryuk. Если система связана с SIEM-системой, то шифровальщик пытается остановить отправку в SIEM каких-либо предупреждений. Таким образом, он защищает свои следующие шаги, поскольку некоторые SAM-службы не смогут правильно начать свою работу после выполнения Ryuk.

Ryuk начинается с горизонтального перемещения внутри сети или он запускается другой вредоносной программой, такой как Emotet или Trickbot, которые в случае эскалации привилегий передают эти повышенные права шифровальщику. [3]

Внедрение: Основной целью процесса внедрения, как и эскалации, является получение доступа к теневым копиям. Для этого ему нужно работать с потоком с правами выше, чем у локального пользователя. Как только он получит такие более высокие права, он удалит копии и внесет изменения в другие

процессы для того, чтобы сделать невозможным возврат к более ранней точке восстановления в операционной системе. Для выполнения внедрения он использует CreateToolHelp32Snapshot, поэтому он делает снимок запущенных в данный момент процессов и пытается получить доступ к этим процессам с помощью OpenProcess. Как только он получает доступ к процессу, он также открывает токен с его информацией для получения параметров процесса. После их получения он проходит по списку, пытаясь один за другим открыть процессы с помощью OpenProcess до тех пор, пока у него не получится это сделать. Он также проверяет, что процесс, в который он будет внедряться, не является csrss.exe, explorer.exe, lsaas.exe или что он имеет набор прав NT authority.

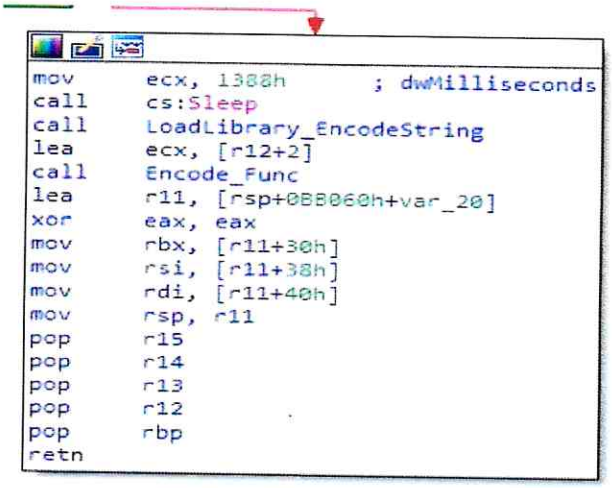
```
test    eax, eax
jz      short loc_140005AE5
mov     rdx, rsi        ; Str2
lea     rcx, Str1       ; Str1
call    wcscmp
test    eax, eax
jz      short loc_140005AE5
cmp     [rbx+4], r15d
jnz     short loc_140005AE5
lea     rdx, aCsrssExe  ; "csrss.exe"
mov     rcx, rsi        ; Str1
call    wcscmp
test    eax, eax
jz      short loc_140005AE5
lea     rdx, aExplorerExe ; "explorer.exe"
mov     rcx, rsi        ; Str1
call    wcscmp
test    eax, eax
jz      short loc_140005AE5
lea     rdx, aLsaasExe  ; "lsaas.exe"
mov     rcx, rsi        ; Str1
call    wcscmp
```

Рис. 7. Исключенные процессы

После того как он сделал снимок процессов, открыл процессы и проверил, что ни один из них не является исключенным, он готов записывать в память процессы, которые будут внедрены. Для этого он сперва резервирует область в памяти (VirtualAllocEx), записывает в нее (WriteProcessmemory) и создает поток (CreateRemoteThread). Для работы с этими функциями он использует PID-ы выбранных процессов, которые он предварительно получил с помощью CreateToolhelp32Snapshot.

Шифрование: Две подпрограммы под названием "LoadLibrary_EncodeString" и "Encode_Func" отвечают за выполнение процедуры

шифрования.



```
mov     ecx, 1388h      ; dwMilliseconds
call    cs:Sleep
call    LoadLibrary_EncodeString
lea     ecx, [r12+2]
call    Encode_Func
lea     r11, [rsp+0B8060h+var_20]
xor     eax, eax
mov     rbx, [r11+30h]
mov     rsi, [r11+38h]
mov     rdi, [r11+40h]
mov     rsp, r11
pop     r15
pop     r14
pop     r13
pop     r12
pop     rbp
retn
```

Рис. 7. Исключенные процессы

Вначале Ryuk загружает строку, которая позже будет использоваться для деобфускации всего, что необходимо: импорты, DLL, команды, файлы и CSP. Первый импорт, который он деобфускирует в регистре R4, LoadLibrary. Это будет использоваться позже для загрузки необходимых DLL. [5]

```
Ocultar FPU

RAX   000000000000006B    'k'
RBX   00007FF653C964B4    ttqum.00007FF653C964B4
RCX   0000000000000048    'H'
RDX   000000000000000B
RBP   00000016D6644950
RSP   00000016D6644910
RSI   000000000000000C
RDI   00007FF653CA3E4C    ttqum.00007FF653CA3E4C

R8    7EFEFEFEFEFEFEFF
R9    7EFEFEFEFEFEFEFF
R10   0000000000000000
R11   8101010101010100
R12   00007FF653CA35D0    "PIuHRaAZnrukOjfsAIYRNIGtOAWqGH
R13   0000000000000001
R14   00007FF653CA3E40    "LoadLibraryA"
R15   0000000000000044    'D'

RIP   00007FF653C8470A    ttqum.00007FF653C8470A

RFLAGS   0000000000000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus C0000018 (STATUS_CONFLICTING_ADDRESSES)
```

Рис.8. Динамическая деобфускация

Ryuk продолжает загружать команды, которые он выполнит позже, чтобы отключить резервные копии, точки восстановления и безопасные режимы загрузки

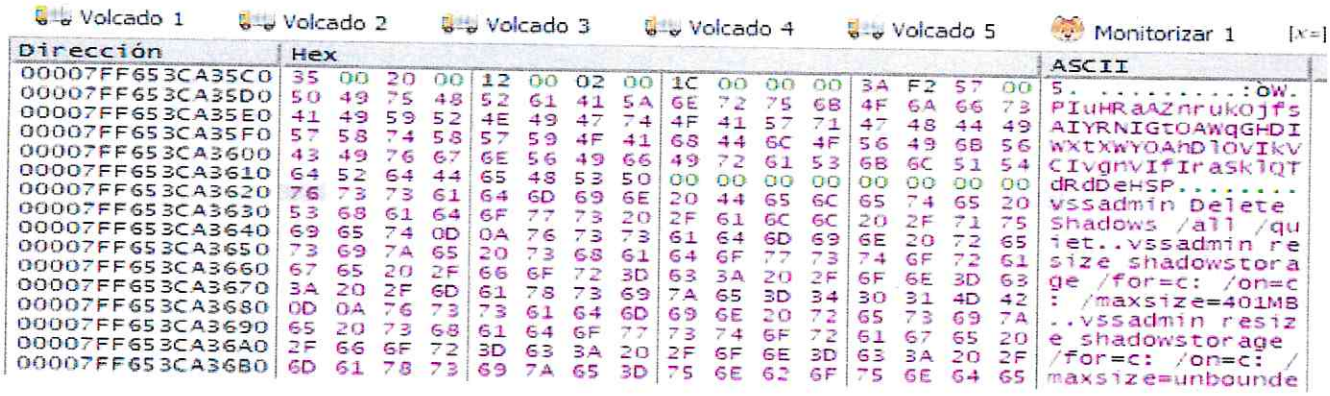


Рис. 9. Загрузка команд

Затем он загружает локацию, куда он бросит 3 файла: Windows.ba run.sct и start.bat. Эти 3 файла используются для проверки привилегий, которым обладают каждая из локаций. Если требуемые привилегии недоступны, Ryu останавливает выполнение. Он продолжает загружать строки, соответствующи трем файлам. Первая, DECRYPT_INFORMATION.html, содержит информацик необходимую для восстановления файлов. Вторая, PUBLIC, содержит открыты ключ RSA. Третья, UNIQUE_ID_DO_NOT_REMOVE, содержит зашифрованны ключ, который будет использоваться в следующей подпрограмме для выполнени шифрования. Наконец, он загружает необходимые библиотеки вместе с требуемым импортами и CSP (Microsoft Enhanced RSA и AES Cryptographic Provider).

После того как вся деобфускация завершена, он переходит к выполнени действий, требуемых для шифрования: перебор всех логических дисков выполнение того, что было загружено в предыдущей подпрограмме, усилени присутствия в системе, заброска файла RyukReadMe.html, шифрование, перебо всех сетевых дисков, переход на обнаруженные устройства и их шифрование.

Все начинается с загрузки "cmd.exe" и записи открытого RSA-ключа. Затем о получает все логические диски с помощью GetLogicalDrives и отключает вс резервные копии, точки восстановления и безопасные режимы загрузки. После этог он усиливает свое присутствие в системе и записывает первы файл RyukReadMe.html в TEMP. Чтобы иметь возможность выполнить эти ж действия на всех устройствах, он использует "icacls.exe". И, наконец, он начинае

шифрование файлов за исключением файлов "*.exe", "*.dll", системных файлов других локаций, указанных в виде зашифрованного белого списка. Для этого о использует импорты: CryptAcquireContextW (где указано использование AES RSA), CryptDeriveKey, CryptGenKey, CryptDestroyKey и т.д. Такж предпринимается попытка расширить свое действие на обнаруженные сетевы устройства с помощью WNetEnumResourceW и затем зашифровать их. [3]

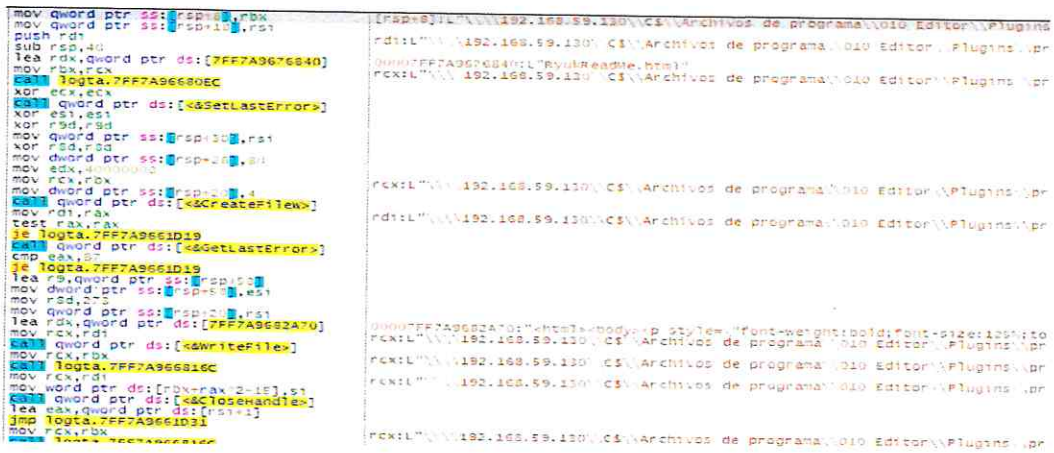


Рис. 10. Шифрование системных файлов

Противодействовие программе-вымогателю Ryuk.

Для того чтобы защитить систему и данные от Ryuk необходимо прежде всего[6]:

- Повысить киберграмотность сотрудников, чтобы исключить фишинг как возможный вектор проникновения преступников в систему. На сегодняшний день именно фишинг является средством для получения учётных данных сотрудников и внедрения вредоносного ПО в корпоративные сети.
- Обновить контроллеры домена, чтобы защитить их от использования Zerologon, который используется для получения доступа на уровне домена.
- Рассмотреть возможность полного отключения административных ресурсов или блокирования доступа через брандмауэры, поскольку Ryuk

пытается шифровать файлы с помощью административных ресурсов Windows (C$ и т. п.).

- Отключить PowerShell с помощью групповой политики, поскольку это добавит ещё один уровень защиты, учитывая широкое использование PowerShell в атаках вредоносного ПО в сети.
- Всегда регулярно создавать резервные копии всех данных, чтобы обеспечить доступ к ним даже в случае успешной атаки вымогателя.
- По возможности сделать файлы доступными только для чтения большинству пользователей, если только им не требуется разрешение на чтение/запись. Переводить файлы на сетевых ресурсах старше определённого периода (в идеале от трёх до шести месяцев) в режим «только чтение». [6]

Заключение

В результате выполнения практики были реализованы поставленные цели и задачи:

- Изучено, чем является программа-вымогатель Ryuk;
- Выяснено на кого и на что нацелена программа-вымогатель Ryuk;
- Изучена работа программы-вымогателя Ryuk. Из-за чего происходит заражение системы и с помощью чего шифруются данные;
- 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: 03.08.2021)
2) Основные направления деятельности АО «НПО «Эшелон». – Режим доступа: https://npo-echelon.ru/about (дата обращения: 03.08.2021)
3) Руководство по программе-вымогателю Ryuk. – Режим доступа: https://habr.com/ru/post/497696/ (дата обращения: 03.08.2021)
4) Руководство по программе-вымогателю Ryuk. – Режим доступа: https://www.enigmasoftware.com/ru/ryukransomware-udaleniye/ (дата обращения: 03.08.2021)
5) Руководство по противодействию программе-вымогателю Ryuk. – Режим доступа: https://securelist.ru/story-of-the-year-2019-cities-under-ransomware-siege/95280/ (дата обращения: 03.08.2021)
6) Руководство по противодействию программе-вымогателю Ryuk. – Режим доступа: https://habr.com/ru/company/trendmicro/blog/546546/ (дата обращения: 03.08.2021)