

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ компьютерной безопасности и криптографии

**ОБНАРУЖЕНИЕ СЕТЕВОГО RDP ТРАФИКА МЕТОДОМ АНАЛИЗА
ЕГО ПОВЕДЕНИЯ**

КУРСОВАЯ РАБОТА

студента 3 курса 331 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Токарева Никиты Сергеевича

Научный руководитель
доцент

Гортинский А. В.

Заведующий кафедрой

Абросимов М. Б.

Саратов 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 Определение RDP	4
1.1 Безопасность протокола RDP.....	4
2 Принцип работы протокола RDP и анализ его поведения	5
3 Обнаружение сеанса удаленного управления.....	9
3.1 Клавиатурный мониторинг	10
3.2 Другие варианты обнаружения RDP-сессии	14
ЗАКЛЮЧЕНИЕ	16
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	17
Приложение А Код keylogger-win.py	18

ВВЕДЕНИЕ

Информация – это сведения об окружающем мире и протекающих в нём процессах, которые зафиксированы на каком-либо носителе. Благодаря протоколам удаленного доступа можно распоряжаться базами данных, информацией, которая хранится на другом устройстве. В недавнем прошлом большинство схем удаленного доступа характеризовалось высокой стоимостью, низкой производительностью, небольшой скоростью передачи данных, недостаточным уровнем защищенности передаваемой информации [1].

Сейчас, когда практически все предприятия перешли на дистанционный формат работы, компании выбирают протокол RDP, так как он прост в настройке и в использовании. Но далеко не все уделяют особое внимание безопасности собственных рабочих мест. Поэтому предприятия могут быть атакованы злоумышленниками.

В данной работе будут разобраны принцип работы RDP, анализ его поведения, а также методы обнаружения.

1 Определение RDP

Протокол RDP (от англ. Remote Desktop Protocol — протокол удалённого рабочего стола) — патентованный протокол прикладного уровня компании Microsoft и приобретен ею у другой компании Polycom, который предоставляет пользователю графический интерфейс для подключения к другому компьютеру через сетевое соединение. Для этого пользователь запускает клиентское программное обеспечение RDP, а на другом компьютере должно быть запущено программное обеспечение сервера RDP [2].

Клиенты для подключения по RDP существуют для большинства версий Microsoft Windows, Linux, Unix, macOS, iOS, Android и других операционных систем. Стоит отметить, что RDP-серверы встроены в операционные системы Windows. По умолчанию подключения, созданные с помощью RDP, используют UDP-порт 3389 и TCP порт 3389, по которым осуществляется передача данных.

1.1 Безопасность протокола RDP

Как уже известно, что для операционной системы Windows постоянно выходят различные обновления, включая обновлений RDS (от англ. Remote Desktop Services — службы удаленных рабочих столов). В связи с этим возникают различные уязвимости при инициализации RDP-сессии. В основном они не связаны непосредственно с протоколом RDP, но касаются службы удаленных рабочих столов RDS и позволяют при успешной эксплуатации путем отправления специального запроса через RDP получить возможность выполнения произвольного кода на уязвимой системе, даже не проходя при этом процедуру проверки подлинности. Достаточно лишь иметь доступ к хосту или серверу с уязвимой системой Windows. Таким образом, любая система, доступная из сети Интернет, является уязвимой при отсутствии установленных последних обновлений безопасности Windows.

Если стоит задача защитить удаленный доступ, то, конечно, необходимо использовать надежный пароль, обновить свое программное обеспечение до последней версии, также можно использовать VPN подключение, чтобы получить IP-адрес виртуальной сети и добавить его в правило исключения брандмауэра RDP. Стоит отметить, что существует много разных способов, чтобы защитить подключение с помощью протокола RDP и более подробно это описано в документации Microsoft.

2 Принцип работы протокола RDP и анализ его поведения

Принцип работы RDP базируется на протоколе TCP. Соединение клиент-сервер происходит на транспортном уровне. После инициализации пользователь проходит аутентификацию. В случае успешного подтверждения сервер передает клиенту управление. Стоит отметить, что под понятием слова «клиент» подразумевается любое устройство (персональный компьютер, планшет или смартфон), а «сервер» — удаленный компьютер, к которому оно подключается.

Протокол RDP внутри себя поддерживает виртуальные каналы, через которые пользователю передаются дополнительные функции операционной системы, например, можно распечатать документ, воспроизвести видео или скопировать файл в буфер обмена.

Далее в работе будет описан процесс установки RDP-сессии, во время которой осуществляется захват трафика с помощью одной известной программы Wireshark. С помощью нее можно достаточно подробно рассмотреть структуру сообщений протоколов.

Для начала будет произведено подключение с помощью «Удаленного рабочего стола». Это средство представляет собой встроенную в Windows программу, предназначенную для удалённого доступа. В качестве клиента и сервера будут выступать компьютеры с операционной системой Windows 10 Professional версии 21H2. Стоит отметить, что программа «Удаленный рабочий стол» может работать только в том случае, если клиент имеет операционную систему Windows, macOS, Android и iOS и сервер может находиться на платформах Windows, сделанных только в редакциях Professional, Enterprise и Ultimate. Поэтому, пользуясь данной программой, не к каждой платформе можно будет подключиться.

Для подключения к удаленному рабочему столу были заданы статические IP-адреса. Клиенту был присвоен статический IP-адрес 192.168.10.254, а серверу — 192.168.10.229, соответственно маска сети 255.255.255.0. После того, как были заданы IP-адреса, необходимо зайти в настройки Windows, чтобы включить возможность подключения к удаленному рабочему столу. Об этом более подробно описано в статьях [3] и [4]. Далее на сервере был произведен запуск анализа трафика с помощью приложения Wireshark. После подключения к удаленному компьютеру программа-анализатор трафика начала «захватывать» пакеты, как показано на рисунке 1, принадлежащие следующим протоколам:

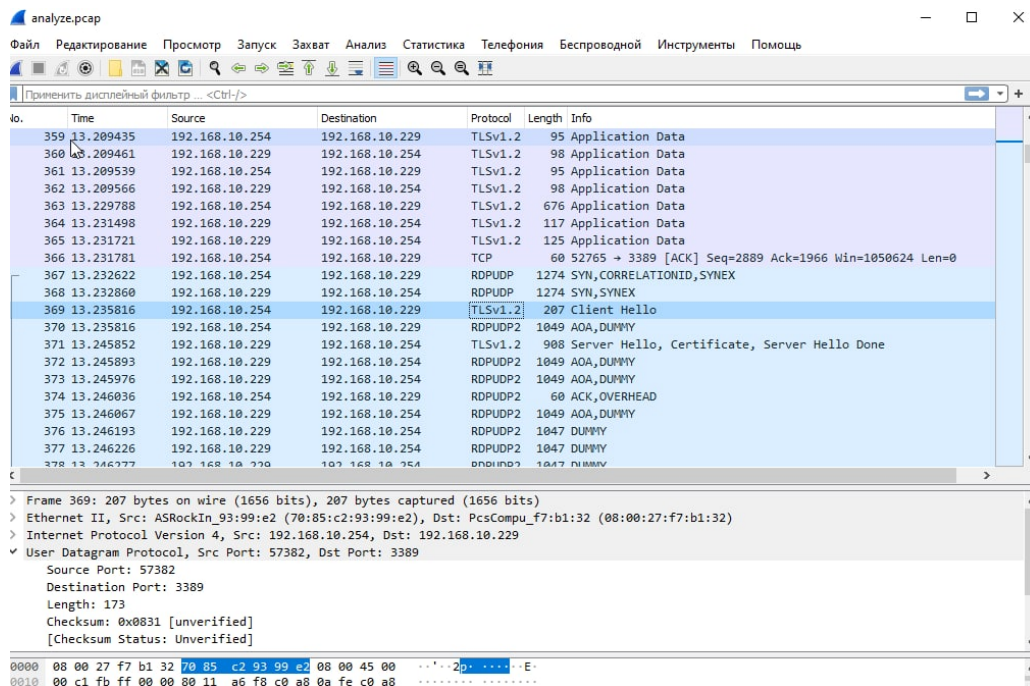


Рисунок 1 – Окно программы Wireshark после захвата трафика

- RDPUDP — протокол RDP, использующий для передачи данных UDP-протокол.
- RDPUDP2 также относится к протоколу RDP. Он был разработан для повышения производительности сетевого соединения по сравнению с соответствующим соединением RDP-UDP [7].
- TLSv1.2 — протокол защиты транспортного уровня, обеспечивающий защищенную передачу между узлами в сети интернет. В данном случае обеспечивает безопасность RDP-сессии.

Во время работы программы Wireshark было найдено достаточное количество пакетов, принадлежащих RDP, которые содержат в себе достаточно интересную информацию. Поэтому стоит рассказать о том, как происходит стандартный способ защиты RDP. Это можно представить в несколько этапов:

1. Клиент объявляет серверу о своем намерении использовать стандартный протокол RDP.
2. Сервер соглашается с этим и отправляет клиенту свой собственный открытый ключ, полученный при шифровании алгоритмом RSA, а также некоторую строку случайных байтов (обычно её называют «random сервером»), генерируемую сервером. На рисунке 2 можно увидеть запись random сервера.

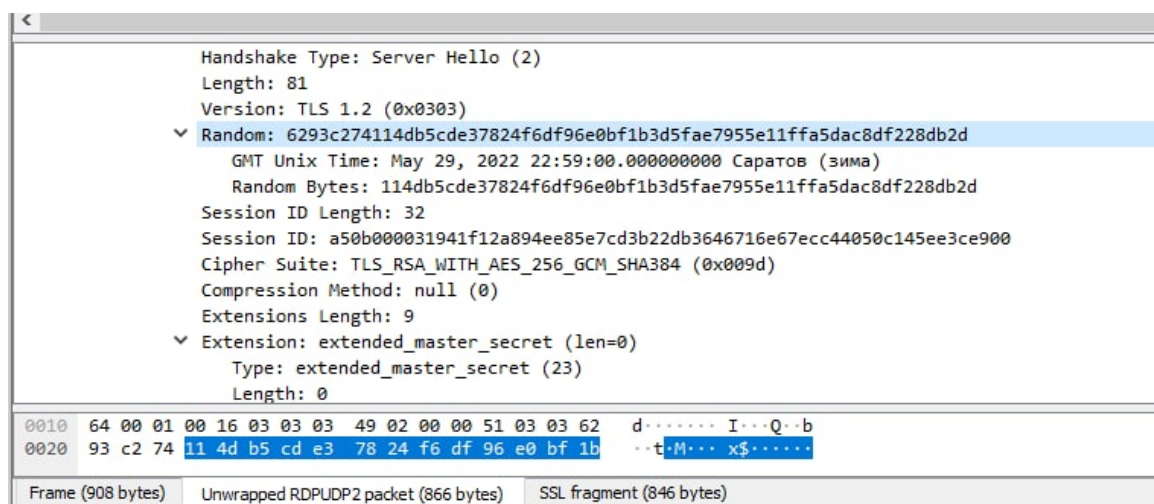


Рисунок 2 – Содержимое пакета, посылаемого от сервера клиенту (запись random сервера)

Совокупность открытого ключа и некоторая строка случайных байтов называется «сертификатом». Данная запись изображена на рисунке 3.

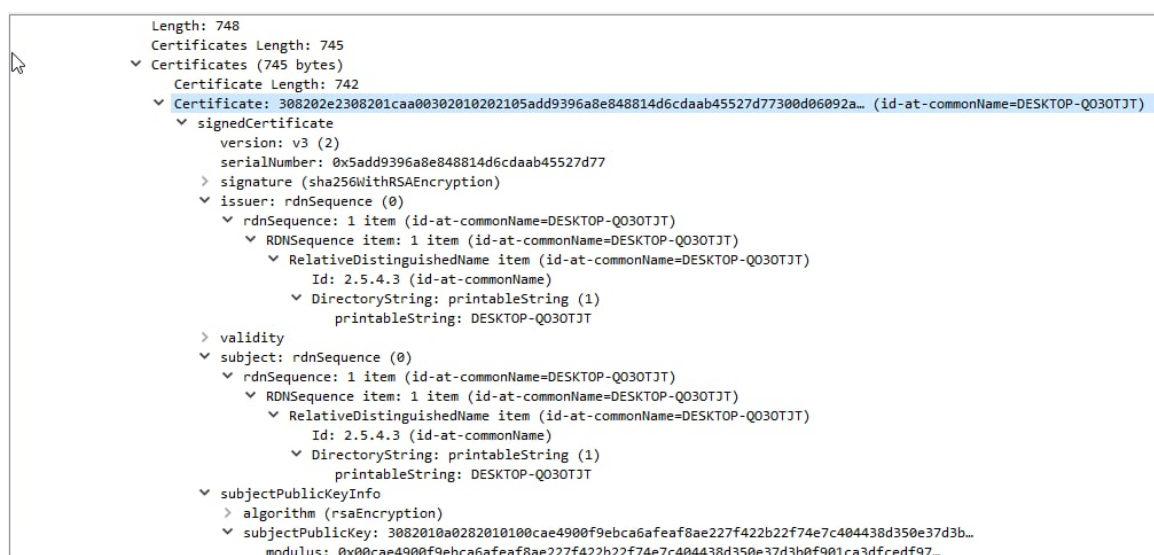


Рисунок 3 – Содержимое пакета, посылаемого от сервера клиенту (запись сертификата)

Сертификат подписывается службой терминалов, например, RDS, с использованием закрытого ключа для обеспечения подлинности.

3. Теперь клиент посылает некоторую строку случайных байтов, которая называется «premaster secret», показанная на рисунке 4.

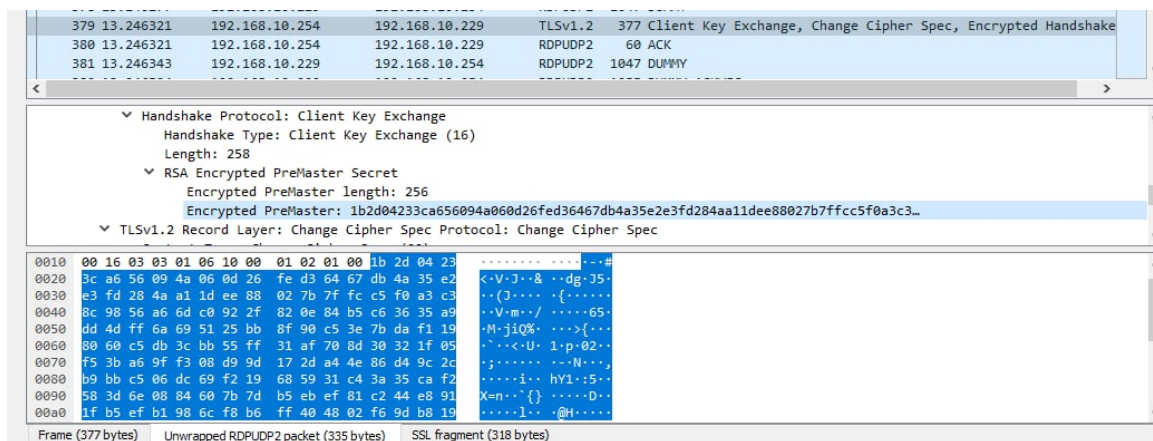


Рисунок 4 – Содержание пакета, посылаемого от клиента серверу (запись premaster secret)

Данная запись шифруется открытым ключом, которая может быть расшифрована сервером только с помощью закрытого ключа службы терминалов.

4. Сервер расшифровывает premaster secret с помощью собственного закрытого ключа.
5. В случае успеха клиент и сервер получают свои сеансовые ключи из random сервера и premaster secret. Далее они используются для симметричного шифрования остальной части сеанса.

Теперь после того, как был произведен разбор RDP-сессии можно перейти к её обнаружению.

3 Обнаружение сеанса удаленного управления

Помимо программы «Удаленный рабочий стол» есть и другие приложения, с помощью которых можно установить соединение клиент-сервер. Например:

1. Удаленный рабочий стол Chrome (Chrome Remote Desktop) — удаленный рабочий стол Chrome позволяет пользователям получать удаленный доступ к другому компьютеру через браузер Chrome. С помощью данного приложения можно подключаться к платформам, на которых есть этот браузер. Однако подключение таким образом к телефону невозможно, так как мобильное приложение «Удалённый рабочий стол Chrome» предоставляет доступ к компьютеру.
2. TeamViewer — приложение, позволяющее установить соединение с любым персональным компьютером или сервером всего за несколько секунд. На данный момент это очень популярное приложение, которое позволяет записывать сеансы на видео, общаться участникам в голосовом и текстовом каналах и открывать удалённый доступ только к выбранным приложениям.
3. Remote Utilities — программа для удалённого подключения к компьютерам. Серверная часть Remote Utilities устанавливается только на Windows, зато клиенты доступны на всех популярных платформах.
4. Ammyy Admin — надежный и удобный инструмент для удаленного доступа к компьютеру. Программа позволяет удалённо перезагружать компьютер, входить в систему и менять пользователей. Однако она доступна только для Windows.

Сейчас таких программ, позволяющих подключиться к удаленному рабочему столу, стало достаточно много. И в некоторых приложениях уже не используется RDP. Например, программа Chrome Remote Desktop работает с протоколом HTTP, а TeamViewer вообще использует собственный проприетарный протокол, который не задокументирован. Хотя он немного похож на RDP по назначению, но включает в себя обход преобразования сетевых адресов и имеет немного другие методы аутентификации. Поэтому некоторые программы, созданные для распознавания и перехвата RDP трафика, в данном случае будут бесполезны.

Хорошо, что такие программы, позволяющие устанавливать соединение с рабочим столом, для пользователя имеются в открытом доступе. Что, если существуют такие приложения, о которых пользователь не имеет никакого

представления? Получается, данное программное обеспечение будет являться потенциальной угрозой, так как с помощью него можно подключиться к удаленному рабочему столу без разрешения самого пользователя.

Таким образом, в данной ситуации необходимо проанализировать возможную угрозу, используя различные методы обнаружения RDP-сессии.

3.1 Клавиатурный мониторинг

Одним из таких методов обнаружения является клавиатурный мониторинг. Допустим может возникнуть ситуация, когда злоумышленник уже смог подключиться к удаленному рабочему столу локального пользователя. Его сертификат оказался действительным, и он может полностью взять под свой контроль чужой компьютер. И тогда у локального пользователя остается мало шансов предотвратить утечку информации.

И здесь одним из способов обнаружения RDP-сессии может быть полезен кейлоггер. Это программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д. [6]. В данном случае кейлоггер выполняет следующие задачи:

- регистрирует нажатия клавиш на клавиатуре и мыши компьютера;
- при достижении заданного предела символов отправляет по протоколу SMTP (Simple Mail Transfer Protocol — протокол передачи почты) сообщение на электронную почту;
- создает log-файл, в который делаются записи названия клавиш и их время удержания, а также названия клавиш мыши и их позиция на экране, представленная в виде двух координат.

Чтобы обезопасить свой компьютер от сторонних подключений, локальный пользователь запускает программу кейлоггер, написанную на языке Python. Из рисунка 5 видно, что программа запрашивает логин и пароль от электронной почты, на которую будут отправляться сообщения.

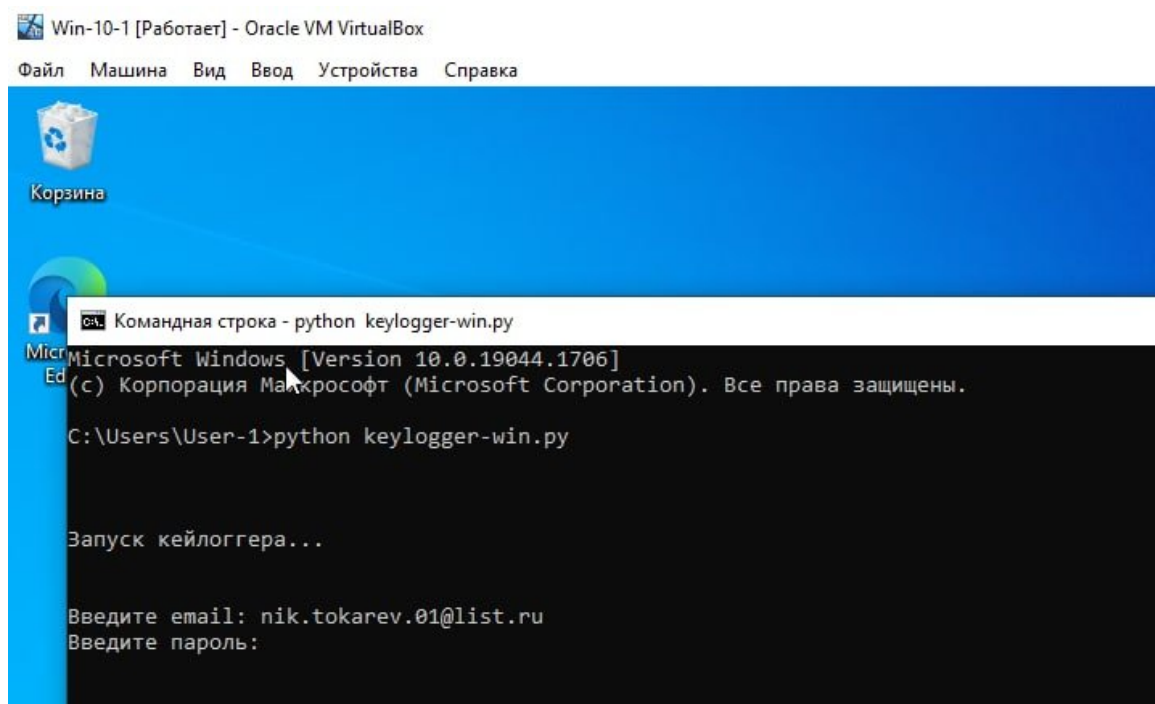


Рисунок 5 – Окно программы при работе кейлоггера

Допустим злоумышленник уже знает IP-адрес и имя пользователя компьютера, и ему удалось подключиться к удаленному рабочему столу. На рисунке 6 показано подключение к удаленному рабочему столу, а именно к компьютеру с IP-адресом 192.168.10.229. Стоит отметить, что здесь подключение производится через известное приложение для удаленного рабочего стола устройства Windows. Конечно, злоумышленник будет использовать программу, сигнатура которой никому другому неизвестна. Поэтому программа «Подключение к удаленному рабочему столу» используется в качестве примера.

На рисунке 6 показан ввод различной информации при успешно установленной RDP-сессии.

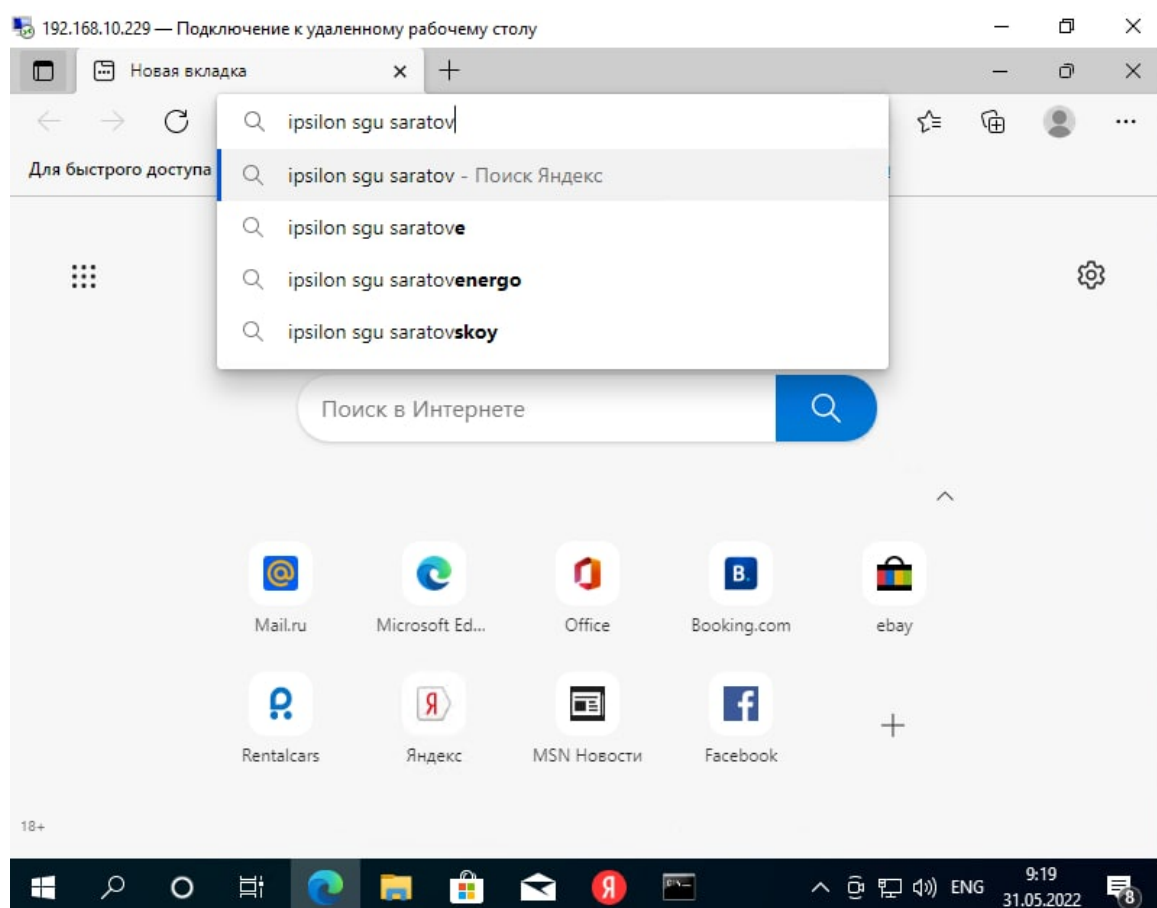


Рисунок 6 – Демонстрация работы с удаленным рабочим столом

Допустим злоумышленник решил попытаться зайти на сайт ippsilon.sgu.ru, зная логин и пароль некоторого пользователя, как показано на рисунке 7.

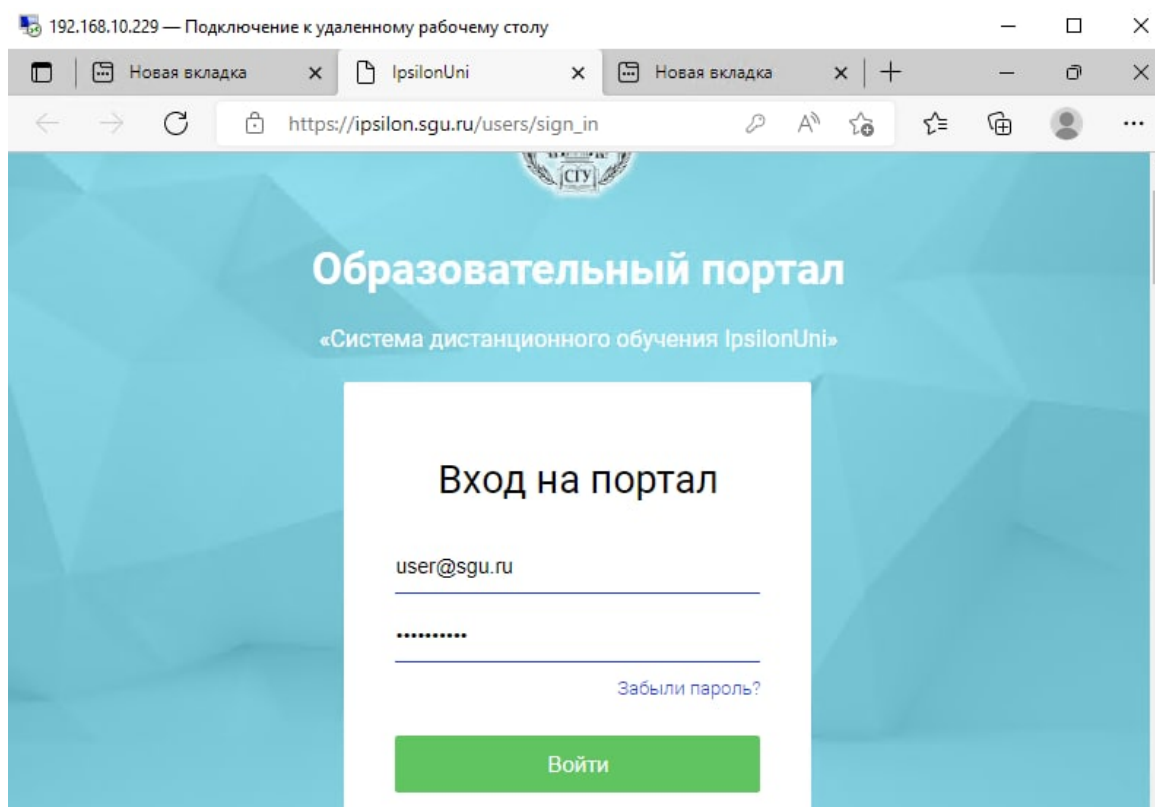


Рисунок 7 – Ввод логина и пароля, осуществляемый на сайте ippsilon.sgu.ru

И после набора определенного количества символов осуществляется отправка письма на электронную почту. На рисунке 8 видно, что письмо доставлено на введенную локальным пользователем почту.

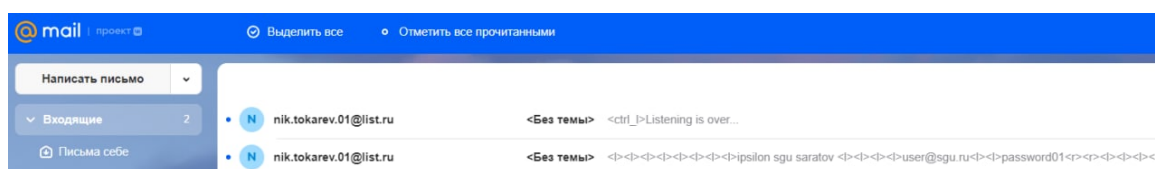


Рисунок 8 – Получение электронного письма

На рисунке 9 показано содержимое сообщения. Записи «<l>» и «<r>» обозначаются нажатия левой и правой кнопки мыши соответственно.

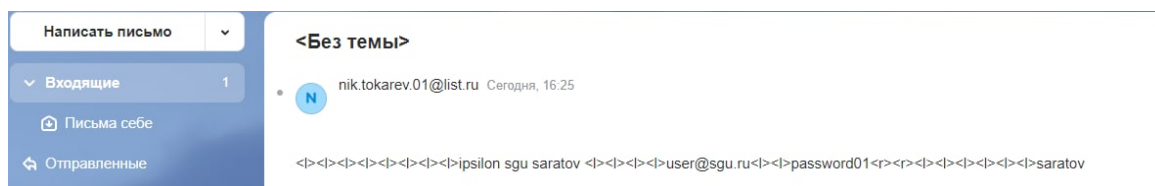
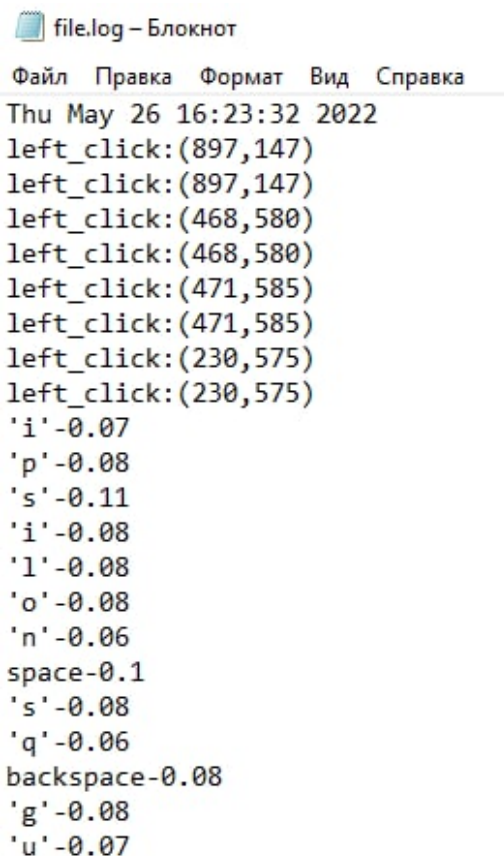


Рисунок 9 – Содержимое электронного письма

Получив письмо, пользователь может начать действовать, пытаясь изолировать злоумышленника от интернета или просто зайдя под своей учетной за-

писью на своем устройстве. Таким образом RDP-сессия будет предотвращена. При закрытии консоли или нажатии комбинации клавиш *Ctrl + f5*, программа завершает свою работу и в итоге получается log-файл, показанный на рисунке 10.



```
file.log – Блокнот
Файл  Правка  Формат  Вид  Справка
Thu May 26 16:23:32 2022
left_click:(897,147)
left_click:(897,147)
left_click:(468,580)
left_click:(468,580)
left_click:(471,585)
left_click:(471,585)
left_click:(230,575)
left_click:(230,575)
'i'-0.07
'p'-0.08
's'-0.11
'i'-0.08
'l'-0.08
'o'-0.08
'n'-0.06
space-0.1
's'-0.08
'q'-0.06
backspace-0.08
'g'-0.08
'u'-0.07
```

Рисунок 10 – Содержимое файла file.log

Возможно ситуация, в которой злоумышленнику удастся получить контроль над удаленным рабочим столом, маловероятна. Однако это не исключено. Ведь RDP блокирует текущую сессию, где компьютер в данный момент работает, не позволяя двум пользователям видеть действия другого. В таком случае локальному пользователю будет сложно остановить утечку данных, так как он не знает, когда была установлена RDP-сессия. Поэтому представленный в работе кейлоггер здесь может оказаться полезным.

3.2 Другие варианты обнаружения RDP-сессии

В Windows существуют логи RDP подключений, которые позволяют администраторам терминальных RDS серверов получить информацию о том, какие пользователи подключались к серверу, когда сеанс был начат или завершен. Информация об этих событиях содержится в журналах Windows. Ее можно

просмотреть, открыв коллекцию средств администрирования — «Управление компьютером», позволяющая управлять локальным или удаленным компьютером. Открыв «Просмотр событий» необходимо рассмотреть следующее:

- Network Connection — установка сетевого подключения к серверу от RDP клиента пользователя;
- Authentication — успешная или неуспешная аутентификация пользователя на сервере;
- Session Disconnect/Reconnect — события отключения/переподключения сессии имеют разные коды в зависимости от того, что вызвало отключение пользователя (отключение по неактивности, выбор пункта Disconnect в сессии, завершение RDP сессии другим пользователем или администратором и т.д.);
- Logon и Logoff — RDP вход в систему и выход из системы.

В перечисленных событиях необходимо анализировать значения EventID. Благодаря им, можно узнать некоторую информацию о возможных подключениях. В основном просмотр логов RDP подключений осуществляется уже после того, как произошла какая-либо утечка информации. Благодаря просмотру событий пользователь может предотвратить будущие атаки злоумышленников, однако он уже не сможет вернуть похищенные данные, которые производились в результате установки посторонних RDP-сессий.

ЗАКЛЮЧЕНИЕ

На основании проведенной работы можно предположить, что RDP далеко не самый защищенный протокол. Хотя корпорация Microsoft регулярно выпускает обновления для своего программного обеспечения. Однако RDP-сессия становится уязвимой из-за упущений в безопасности, например, из-за некорректной конфигурации сервисов или установки устаревших обновлений системы. В таком случае злоумышленник может использовать такие просчеты в своих целях. Конечно, далеко не за всем можно уследить и не всегда получается предвидеть возможную угрозу. Но лучше попробовать предположить возможное решение данной проблемы, вместо того чтобы вообще о ней не думать.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Книга Ибе О.С. «Компьютерные сети и службы удаленного доступа» / пер. с англ. - Москва, издательство: «ДМК Пресс», Яз. рус.
- 2 Удалённый рабочий стол RDP: как включить и как подключиться по RDP [Электронный ресурс] / URL:<https://hackware.ru/?p=11835> (дата обращения 03.05.2022), Яз. рус.
- 3 How to use remote desktop [Электронный ресурс] / URL: <https://support.microsoft.com/en-us/windows/how-to-use-remote-desktop-5fe128d5-8fb1-7a23-3b8a-41e636865e8c> (дата обращения 27.05.2022), Яз. англ.
- 4 Статья «Как исправить ошибку удаленного рабочего стола не удастся подключиться к удаленному компьютеру» [Электронный ресурс] / URL: <https://okdk.ru/kak-ispravit-oshibku-udalennogo-rabochego-stola-ne-udaetsya-podkljuchitsya-k-udalennomu-kompjuteru/> (дата обращения 27.05.2022), Яз. рус.
- 5 Документация Remote Utilities «RDP» [Электронный ресурс] / URL: <https://www.remoteutilities.com/support/docs/rdp/> (дата обращения 27.05.2022), Яз. англ.
- 6 Статья в википедии «Кейлоггер» [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/Кейлоггер> (дата обращения 28.05.2022), Яз. рус.
- 7 Документация Microsoft «Протоколы» [Электронный ресурс] / URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpeudp2/d8bf9a56-90f3-4608-8f98-9600ed69876b (дата обращения 28.05.2022), Яз. рус.
- 8 Статья «Wireshark Tutorial: Decrypting RDP Traffic» [Электронный ресурс] / URL: https://unit42-paloaltonetworks-com.translate.goog/wireshark-tutorial-decrypting-rdp-traffic/?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=op,wapp (дата обращения 28.05.2022), Яз. англ.

ПРИЛОЖЕНИЕ А

Код keylogger-win.py

```
import time
import getpass
import smtplib
from pynput.keyboard import Key, Listener
from pynput import mouse

print('\n\n')
print('Запуск кейлоггера...\n\n')

# # Ввод логина и пароля электронной почты, на которую
# # будут отправляться письма
email = input('Введите email: ')
password = getpass.getpass(prompt='Введите пароль: ')
server = smtplib.SMTP_SSL('smtp.list.ru', 465)
server.login(email, password)

# Определение глобальных переменных
cur_log = ''
word = ''
email_char_limit = 100
is_ctrl = False
is_exit = False
path = 'C:/file.log'
time_press = 0.0

# Регистрация клавиши при нажатии
def press_elem(event):
    global email
    global cur_log
    global word
    global email_char_limit
    global is_ctrl
    global is_exit
    global time_press
    if event == Key.ctrl_l:
        is_ctrl = True
    if event != Key.ctrl_l and event != Key.f5:
        is_ctrl = False
    if event == Key.f5 and is_ctrl:
        is_exit = True
        cur_log += word + 'Listening is over...'
        send_log()
        return False
    if event == Key.space or event == Key.enter:
        word += ' '
```

```

    cur_log += word
    word = ''
    if len(cur_log) >= email_char_limit:
        send_log()
        cur_log = ''
elif event == Key.shift_l or event == Key.shift_r:
    return
elif event == Key.backspace:
    word = word[:-1]
else:
    event = str(event)
    check = event.find('Key')
    if check != -1:
        event = event.replace('Key.', '')
        word += '<' + event + '>'
    else:
        word += event[1:-1]

event = str(event)
check = event.find('Key')
if check != -1:
    event = event.replace('Key.', '')
time_press = time.time()
with open(path, 'a+') as f:
    f.write('{}-'.format(event))

# Регистрация клавиши после нажатия
def release_elem(event):
    tmp = round(time.time() - time_press, 2)
    with open(path, 'a+') as f:
        f.write('{}\n'.format(tmp))

# Регистрация нажатия мыши
def on_click(x, y, button, pressed):
    global word
    if is_exit:
        return False
    click = str(button).replace('Button.', '') + '_click'
    word += '<' + click[0] + '>'
    with open(path, 'a+') as f:
        f.write('{}\n'.format(click + ':(' + str(x) + ',' + str(y) + ')'))

# Отправка данных на электронную почту
def send_log():
    server.sendmail(email, email, cur_log)

```

```
# Определение переменных для прослушивания клавиатуры и мыши
keyboard = Listener(on_press = press_elem, on_release = release_elem)
mouse = mouse.Listener(on_click = on_click)

if __name__ == '__main__':
    with open(path, 'a+') as f:
        f.write('{}\n'.format(time.ctime()))
    keyboard.start()
    mouse.start()
    mouse.join()
    keyboard.join()
```