

Инфильтрация&эксфильтрация данных через RDP при пентестах

Душенев Денис
Савостин Владимир

About me

- COMPLIANCE CONTROL LLC
- ДУШЕНЕВ ДЕНИС / САВОСТИН ВЛАДИМИР
- ИНФРАСТРУКТУРНЫЕ ПЕНТЕСТЫ

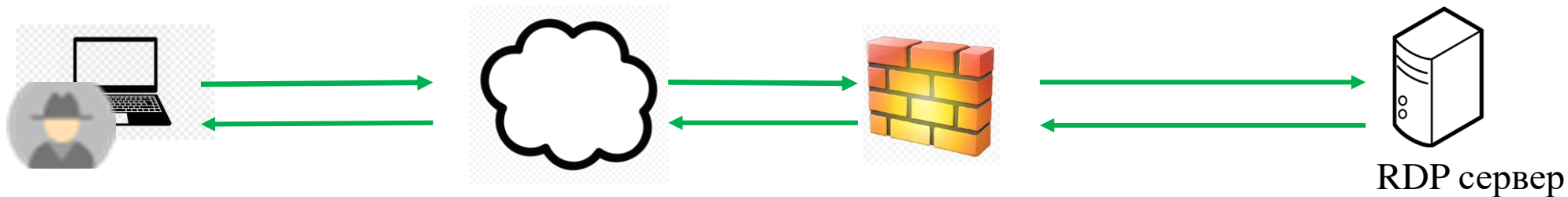
О чем будем говорить

- Случай из практики: пентест по модели «Нелояльный сотрудник»
- Как мы обошли ограничения на копирование файлов при работе по RDP
- Возможные риски для организацией
- Как обнаружить инфильтрацию файлов на удаленный RDP сервер

«Нелояльный» сотрудник

- Запрет на буфер обмена
- Запрет подключения сетевых дисков

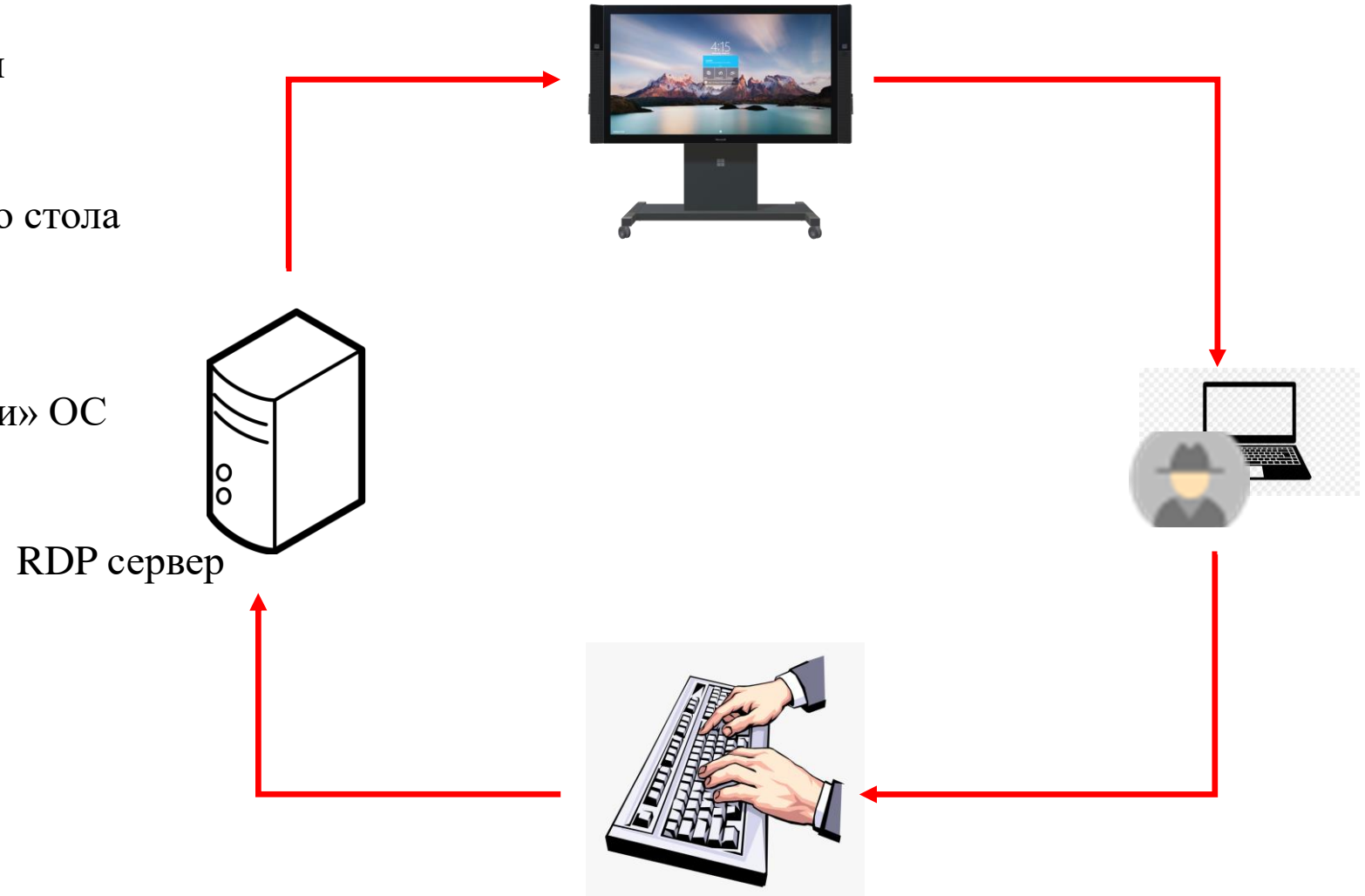
- Удаленное подключение
- Доступ к рабочему месту по RDP
- Доступ к внутренним ресурсам организации
- AV защита
- DLP



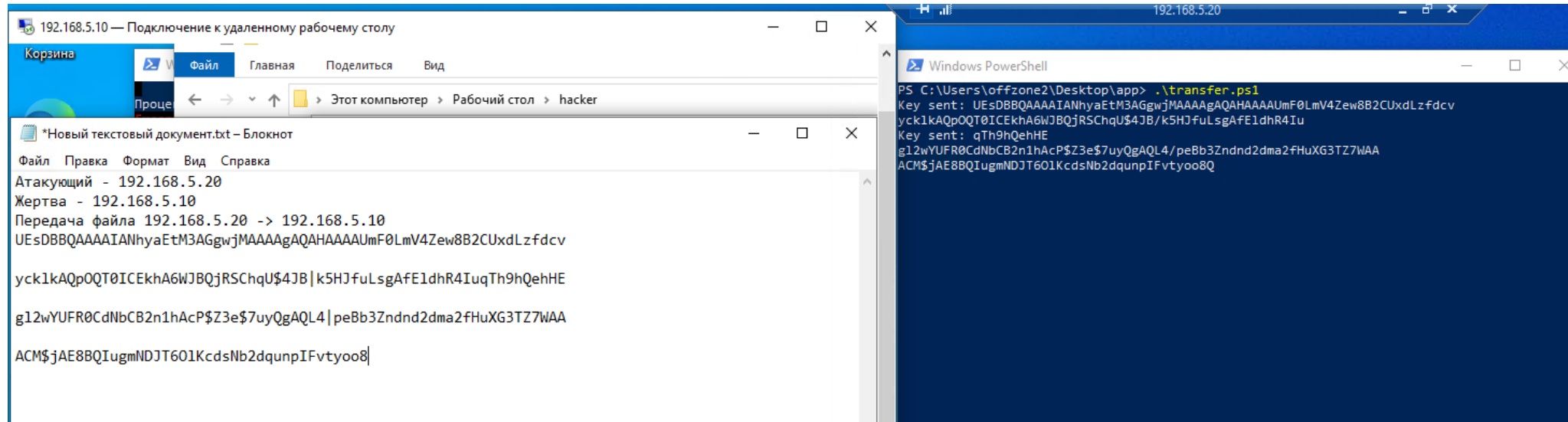
- Блокировка HTTP и DNS tunneling
- Анализ MAIL, IM etc.
- Запрет на подключение к внешним ресурсам

Копирование файлов.

- Используем разрешенные каналы передачи: клавиатурный ввод и отображение удаленного рабочего стола
- Обходим периметральные СЗИ
- Не используем «опасные функции» ОС

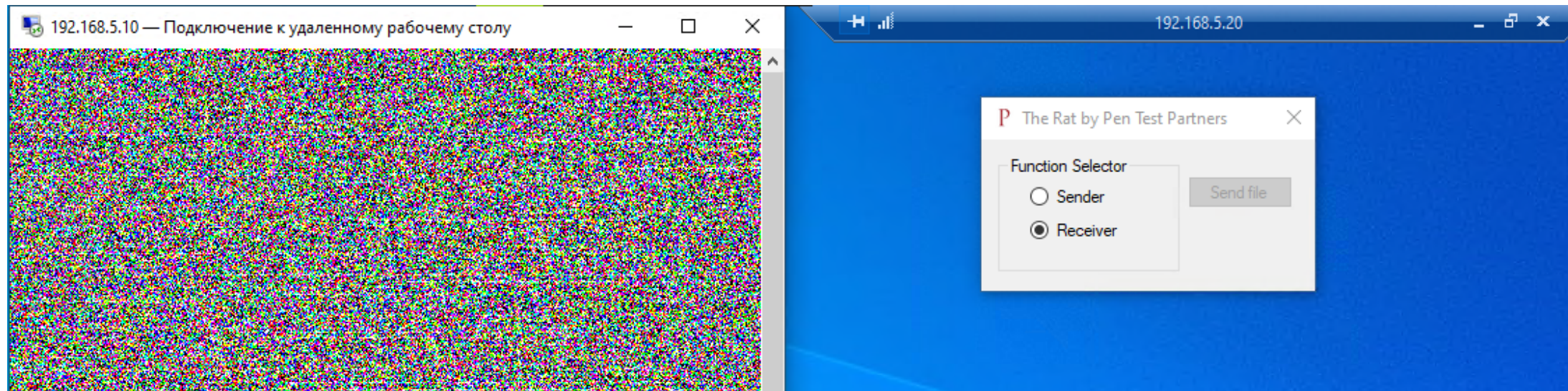


Отправляем файл на сервер: xdotool



1. .exe файл кодируем в формат base64
2. Используем xdotool - позволяет выполнить эмуляцию нажатия клавиш.
3. Автоматизируем копирование файла – скрипт transfer.ps1
4. Разбиваем кодированный файл на блоки и передаем в текстовый редактор на удаленном RDP сервере
5. На сервере – декодируем полученный файл из base64 в .exe

Копируем файл на свой компьютер: RAT

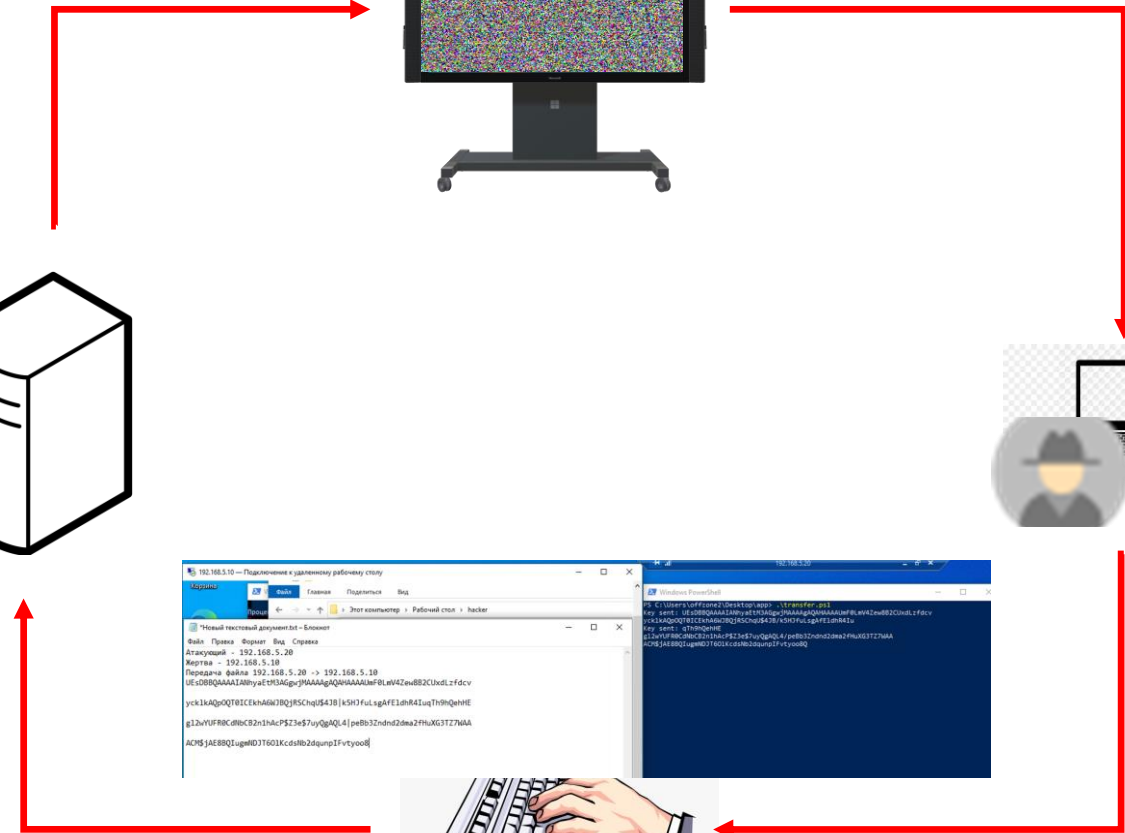
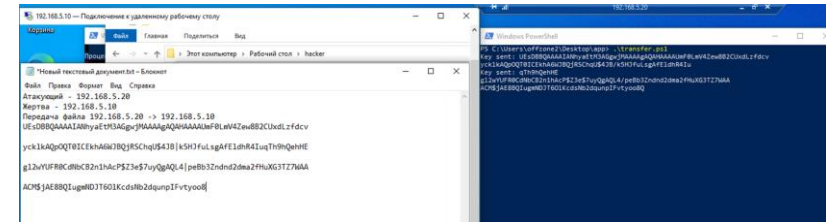
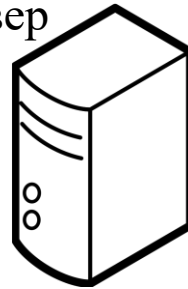


1. RAT использует кодирования данных с использованием значений цвета отдельных пикселей (3 бита на пиксель)
2. Работает в режиме передачи и в режиме приема данных
3. После завершения передачи, приемник декодирует полученную информацию

Основные моменты

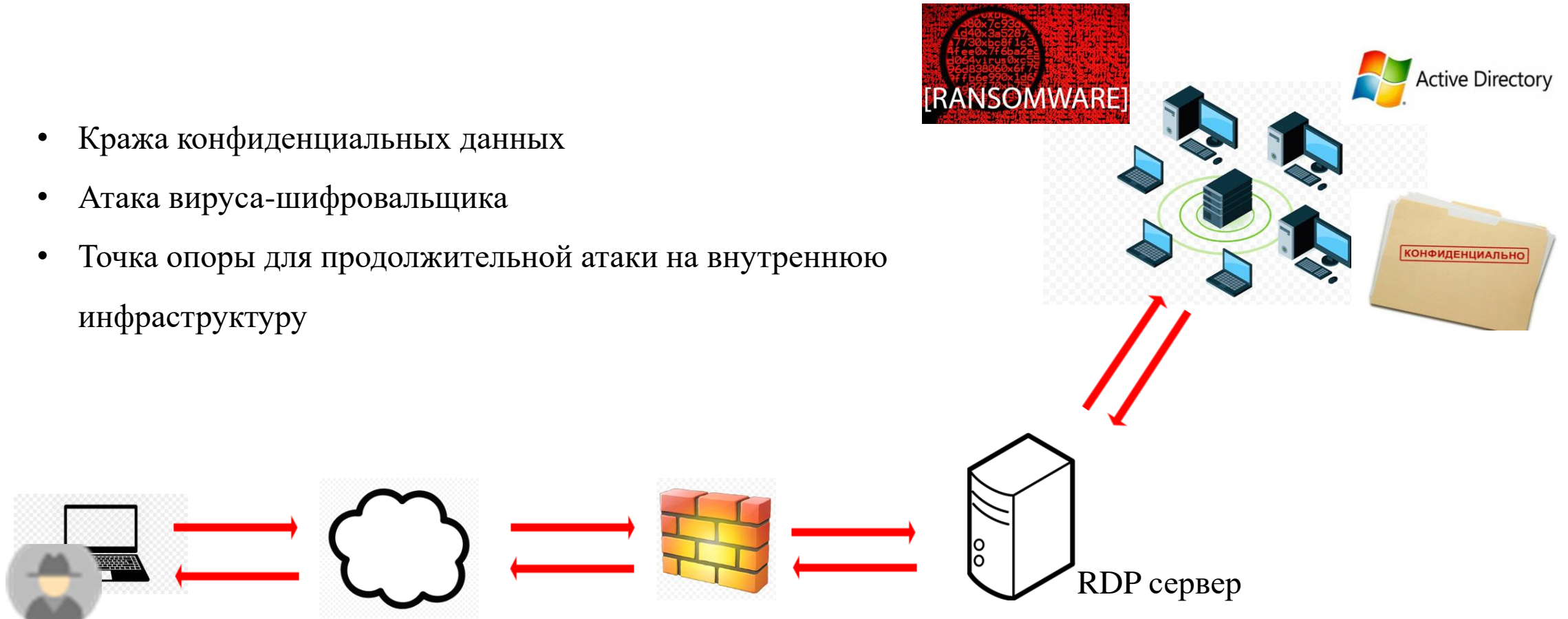
- Передаем файлы со скоростью порядка 10 кбит/мин
(Архив с утилитой RAT передаем за 12-14 минут)
- Забираем файлы со скоростью 1,6 Мбит/сек
- Не используем опасные функции ОС
- Обходим периметральные СЗИ
- Локальные средства защиты могут препятствовать записи на диск и запуску передаваемых файлов

RDP сервер



Возможные сценарии атаки

- Кража конфиденциальных данных
- Атака вируса-шифровальщика
- Точка опоры для продолжительной атаки на внутреннюю инфраструктуру



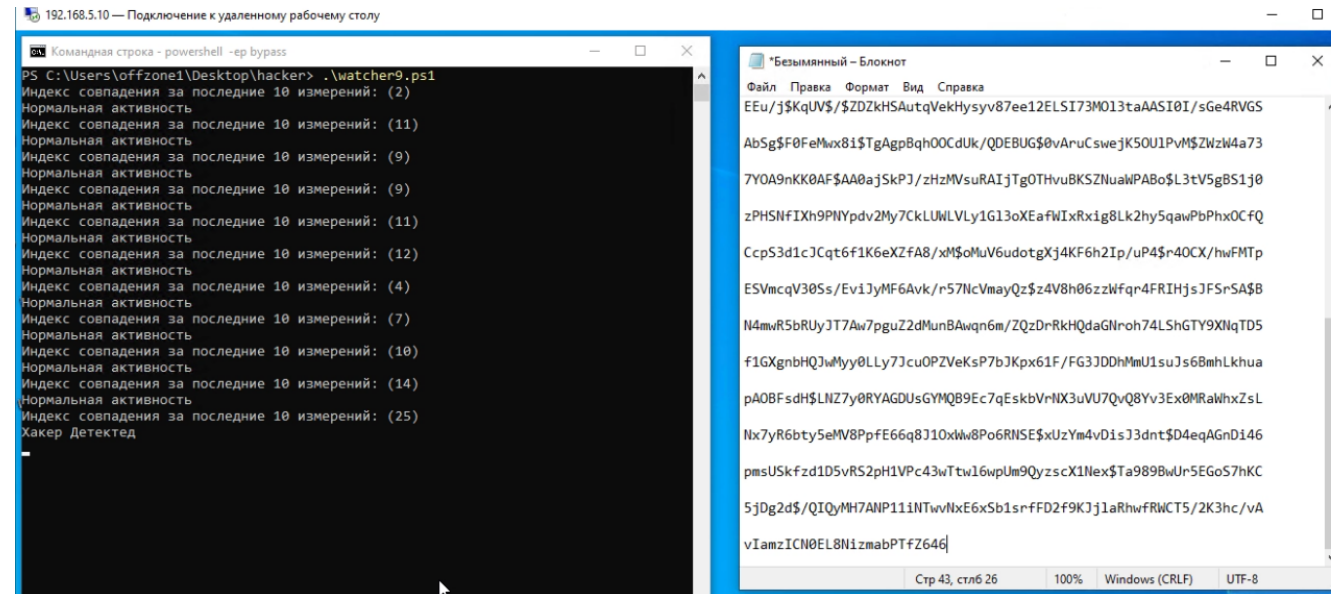
Как бороться: ищем аномалии клавиатурного ввода



Идея: человек не машина!



- Оцениваем равномерность темпа ввода данных с помощью клавиатуры
- Концепция реализована в antiXdotool.ps1



192.168.5.10 — Подключение к удаленному рабочему столу

Командная строка - powershell -ep bypass

```
PS C:\Users\offzone1\Desktop\hacker> .\watcher9.ps1
Индекс совпадения за последние 10 измерений: (2)
Нормальная активность
Индекс совпадения за последние 10 измерений: (11)
Нормальная активность
Индекс совпадения за последние 10 измерений: (9)
Нормальная активность
Индекс совпадения за последние 10 измерений: (9)
Нормальная активность
Индекс совпадения за последние 10 измерений: (11)
Нормальная активность
Индекс совпадения за последние 10 измерений: (12)
Нормальная активность
Индекс совпадения за последние 10 измерений: (4)
Нормальная активность
Индекс совпадения за последние 10 измерений: (7)
Нормальная активность
Индекс совпадения за последние 10 измерений: (10)
Нормальная активность
Индекс совпадения за последние 10 измерений: (14)
Нормальная активность
Индекс совпадения за последние 10 измерений: (25)
Хакер Детектед
```

*Безымянный – Блокнот

Файл Правка Вид Справка

EEu/j\$KqUV\$/\$ZDZkHSAutqVekHysyv87ee12ELSI73M013taAASI0I/sGe4RVGS
AbSg\$f0FeMux81\$tGAgpBqh00CdUk/QDEBUG\$0vAruCsweJk50U1PvM\$ZW4a73
7Y0A9nKK0AF\$AA0aJskPj/zHzMVsuRAIjTg0THvuBKSZINUaWPABo\$L3tV5gBS1j0
zPHSNfIXh9PNYpdv2My7CkLUWLVLy1G13oXEafWixRxig8Lk2hy5qawPbPhxOCfQ
CcpS3d1cJcqt6f1K6eXZfA8/xM\$0MuV6udotgXj4KF6h2Ip/uP4\$r40CX/hwFMTp
ESVmcqV305s/Ev1JyMF6Avk/r57NcVmayQz\$z4V8h06zzWfqr4FRIHjsJFSrSA\$B
N4mwR5bRUyJT7Aw7pguZ2dMunBAwqn6m/ZQzDrRkHQdaGNroh74LShtY9XNqTD5
f1GXgnbHQJwMyy0LLy7Jcu0PZVeKsP7bJkpx61F/FG3DDHmU1suJs6BmhLkhua
pA0BFsdH\$LNZ7y0RYAGDUsgYMQB9Ec7qEskbVrMX3uU7QyQ8Yv3Ex0MRaWhxZsL
Nx7yR6bty5eMV8PpfE66q8J10xIw8Po6RINSE\$xUzYm4vD1sJ3dnt\$D4eqAGnD146
pmsUSkfzd1D5vRS2pH1Vpc43wTtw16wpUm9QyzscX1Nex\$Ta989BwUr5EGoS7hKC
5jDg2d\$/QIQyMH7ANP111NTwvNxE6xSb1srFFD2f9KJj1aRhwFRWCT5/2K3hc/vA
vIamzICN0EL8N1zmabPTfZ646

Стр 43, стр 6 26 100% Windows (CRLF) UTF-8

Ссылки и дополнительные материалы



<https://github.com/dram-beep/4offZone2024>

1. transfer.ps1 - Script for automating file transfer using xdotool.exe
2. antiXdotool.ps1 - Script for detecting the use of xdotool to copy files to a remote server. This is a concept and is not intended for use in production environments.

Videos:

1. <https://youtu.be/nPPUjF3eZoE> - Demonstration of using transfer.ps1 and RAT.exe to copy files between a remote RDP server and your host. Bypasses file copy restrictions when working with RDP.
2. <https://youtu.be/crZMIEZVyQ8> - Demonstration of using antiXdotool.ps1 to detect the use of xdotool.exe for copying confidential data from a remote RDP server to a local host.



Additional Links:

1. For transfer.ps1 to work:
<https://github.com/ebranlard/xdotool-for-windows>
<https://github.com/ebranlard/wmctrl-for-windows>
2. For RAT to work:
<https://github.com/pentestpartners/PTP-RAT/tree/master>