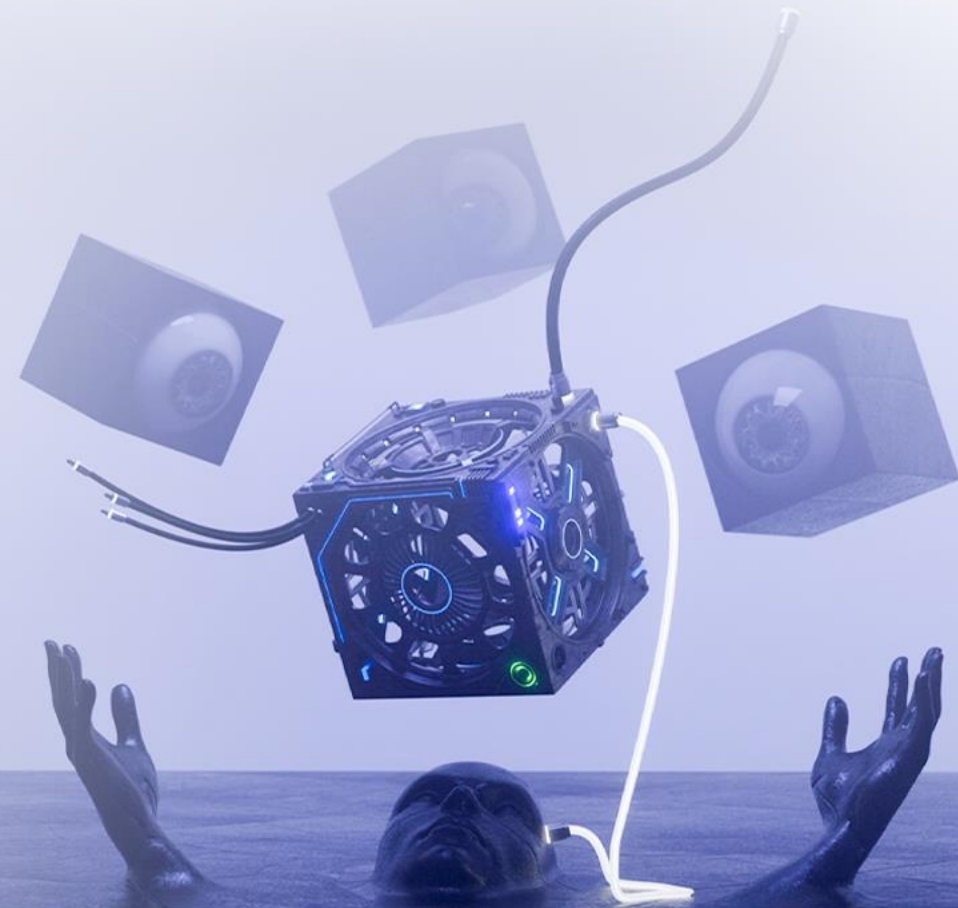


Инфильтрация & эксфильтрация данных через RDP при пентестах

Душенев Денис

Заместитель начальника отдела защищенности по инфраструктурному тестированию





About me

- Более 15 лет работы в различных интеграторах: сопровождение и построение различной ИТ-инфраструктуры, систем безопасности.
- С 2021 в компании ООО «Комплаинс Контрол», где занимаюсь инфраструктурными пентестами

**COMPLIANCE
CONTROL**



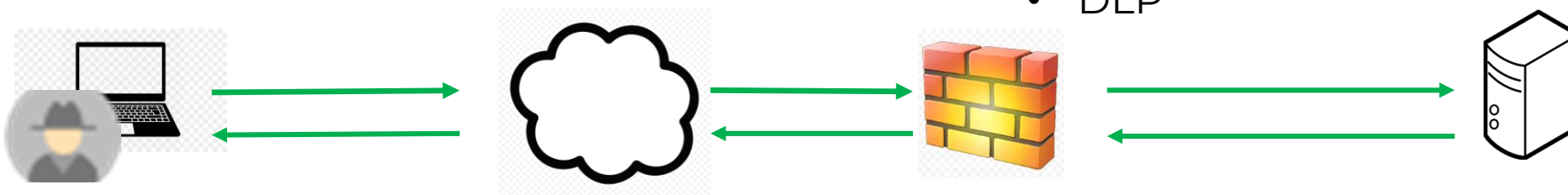
О чем поговорим

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



«Нежелательный» сотрудник

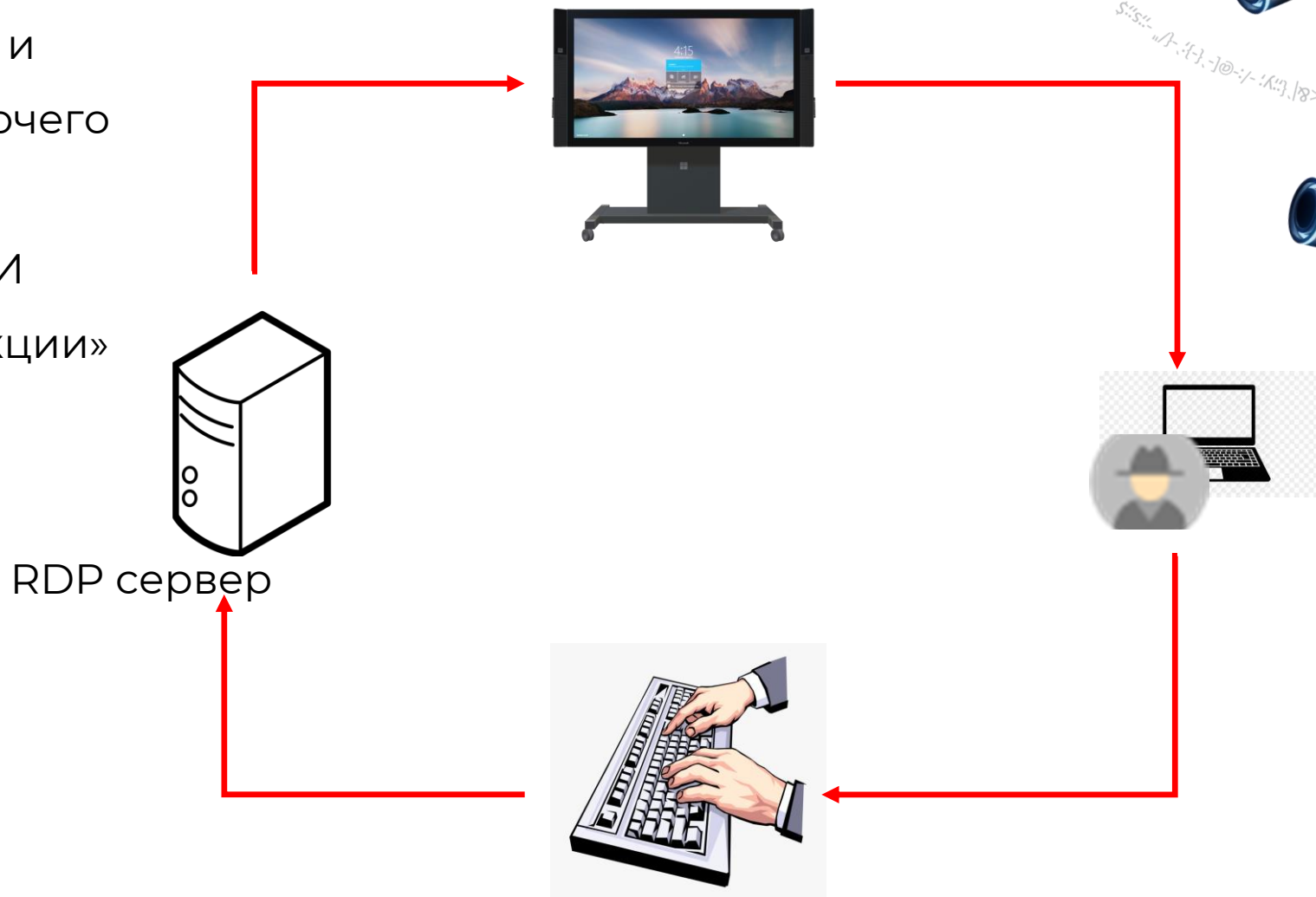
- Запрет на буфер обмена
- Запрет подключения сетевых дисков
- Удаленное подключение
- Доступ к рабочему месту по RDP
- Доступ к внутренним ресурсам организации
- AV
- DLP



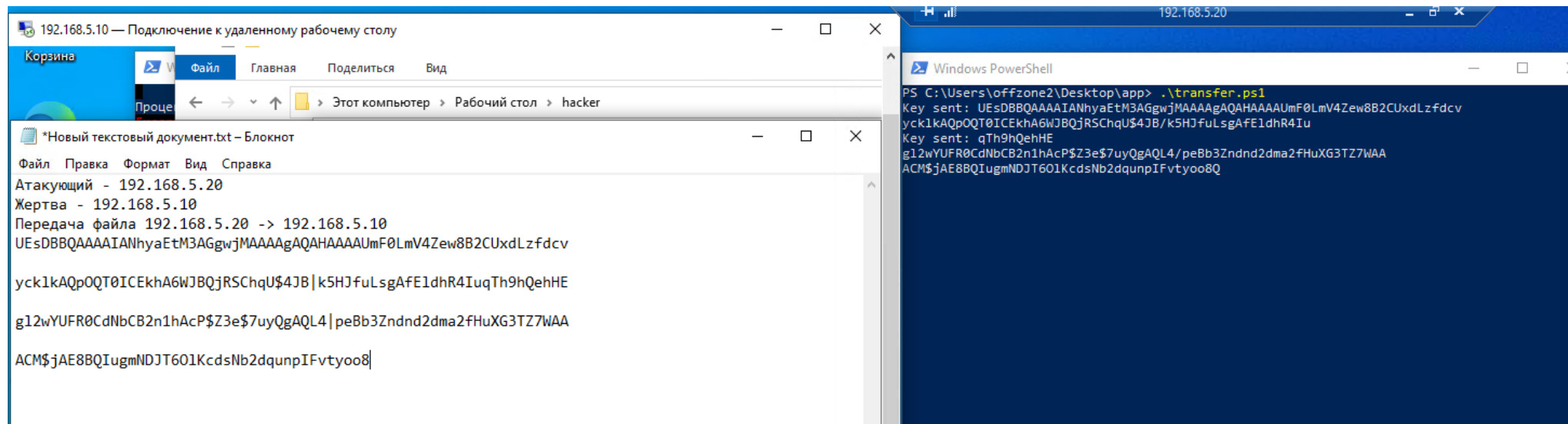
- Блокировка HTTP и DNS tunneling
- Анализ MAIL, IM etc.
- Запрет на подключение к внешним ресурсам

Копирование файлов

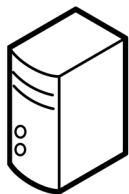
- Используем разрешенные каналы передачи: клавиатурный ввод и отображение удаленного рабочего стола
- Обходим периметральные СЗИ
- Не используем «опасные функции» ОС



Отправляем файл на сервер: xdotool

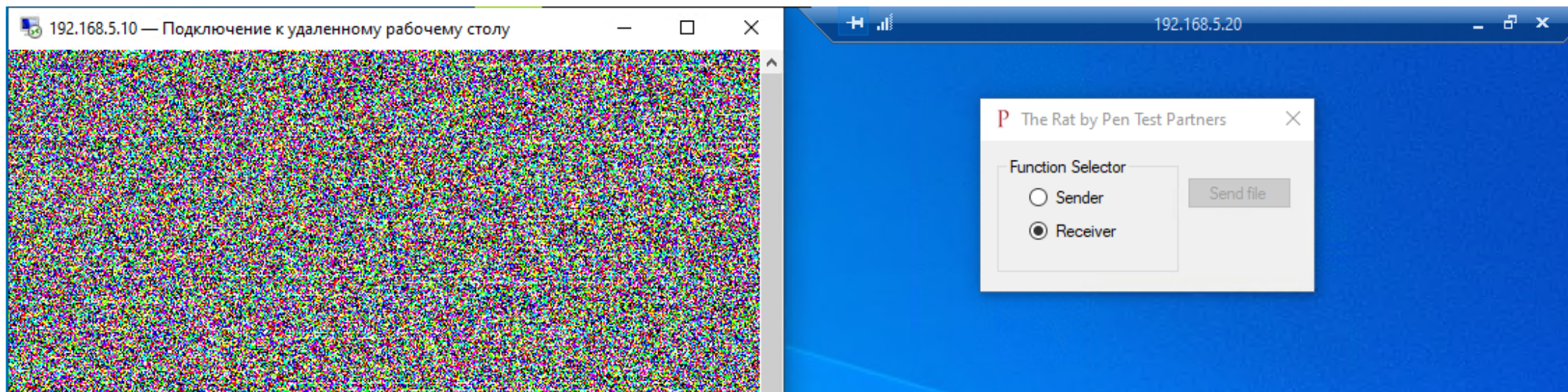


RDP сервер



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

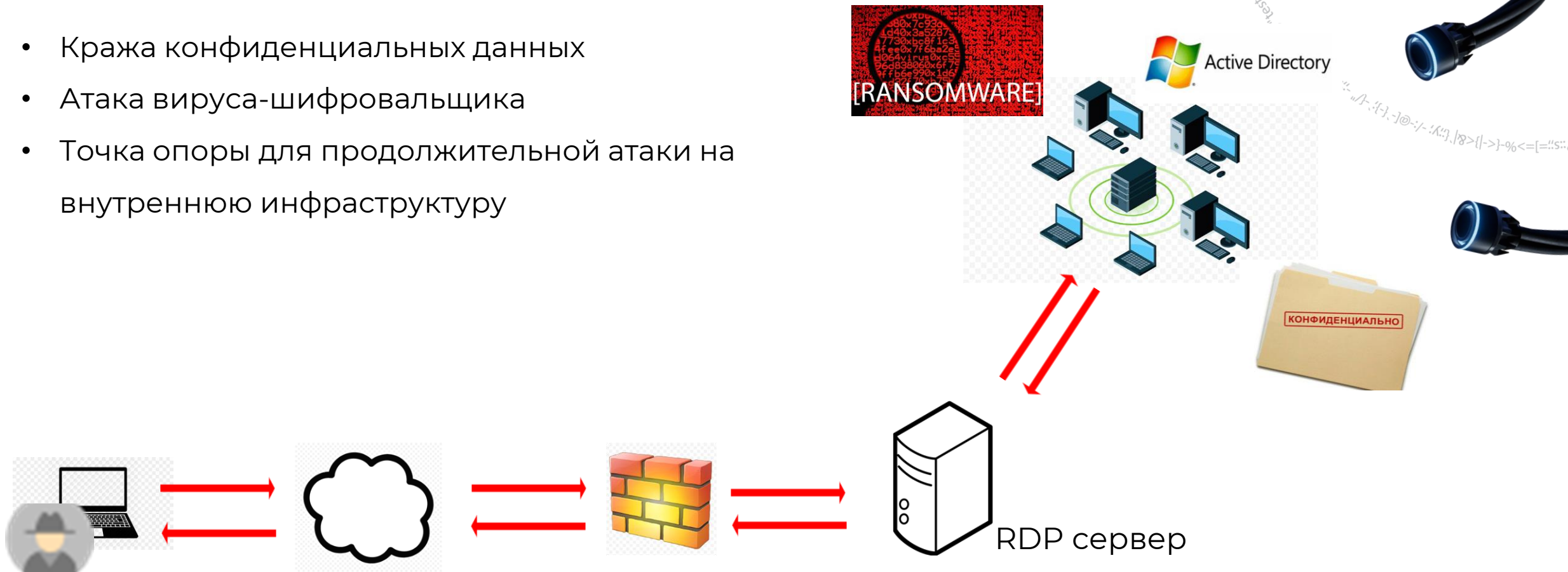
Копируем файл на свой компьютер: RAT



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

Возможные сценарии атаки

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



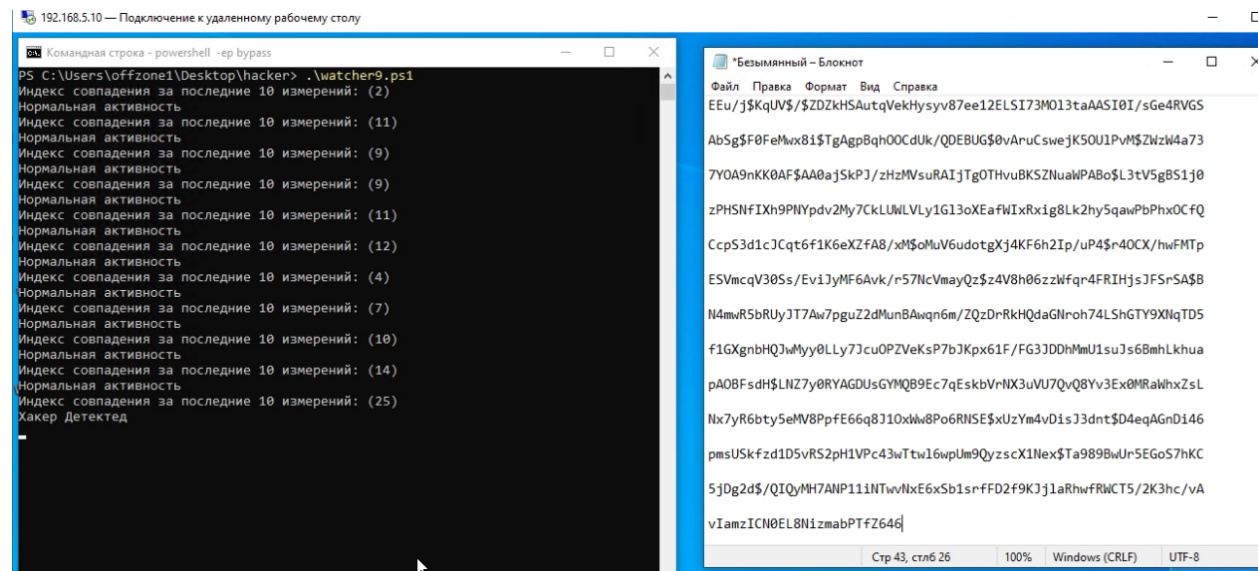
Как бороться: ищем аномалии клавиатурного ввода



Идея: человек не машина!



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



The screenshot shows two windows. The left window is a PowerShell terminal titled '192.168.5.10 — Подключение к удаленному рабочему столу'. It shows the execution of a script named 'antiXdotool.ps1' which outputs a series of 'Индекс совпадения за последние 10 измерений' (Index of coincidence for the last 10 measurements) and 'Нормальная активность' (Normal activity) for various keyboard inputs. The right window is a Notepad application titled '*Безымянный - Блокнот' showing a long string of random characters, likely generated by the script to demonstrate keyboard activity analysis.

Ссылки и дополнительные материалы



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

1. `transfer.ps1` - Скрипт для автоматизации передачи файлов с помощью `xdotool.exe`
2. `antiXdotool.ps1` - Скрипт для обнаружения использования `xdotool` для копирования файлов на удаленный сервер. Это концепция, которая не предназначена для использования в производственных средах.

Videos:

1. <https://youtu.be/nPPUjF3eZoE> - Демонстрация использования `transfer.ps1` и `RAT.exe` для копирования файлов между удаленным RDP-сервером и вашим хостом. Позволяет обойти ограничения на копирование файлов при работе с RDP.
2. <https://youtu.be/crZMIEZVyQ8> - Демонстрация использования `antiXdotool.ps1` для обнаружения использования `xdotool.exe` при копировании конфиденциальных данных с удаленного RDP-сервера на локальный хост.



Дополнительные ссылки:

1. Для работы `transfer.ps1` требуется:
<https://github.com/ebanlard/xdotool-for-windows>
<https://github.com/ebanlard/wmctrl-for-windows>
2. Утилита RAT:
<https://github.com/pentestpartners/PTP-RAT/tree/master>

**COMPLIANCE
CONTROL**

Q&A

