ПОДДЕЛКА ЗАПРОСОВ СО СТОРОНЫ СЕРВЕРА

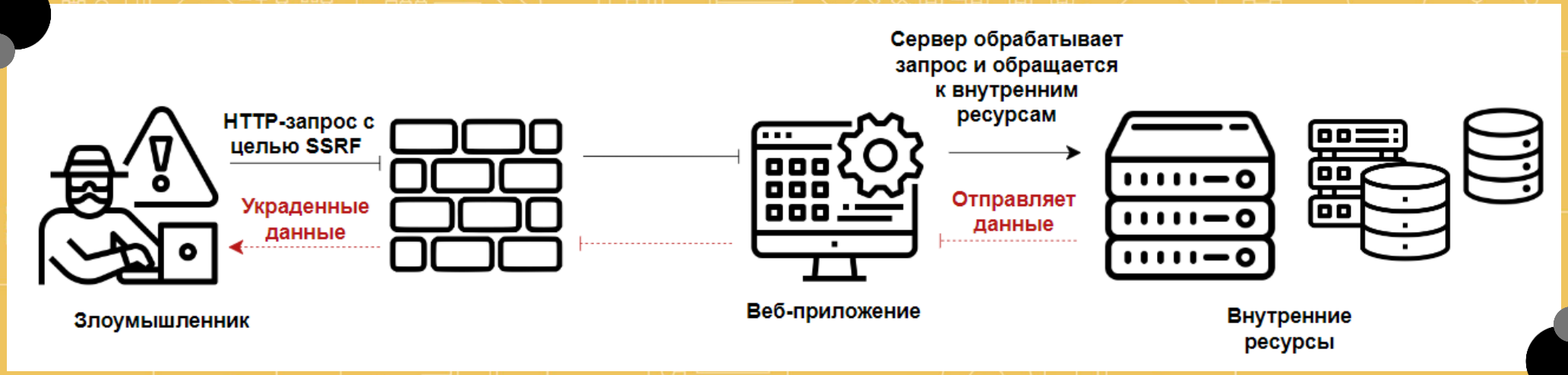
Server-Side Request Forgery

ПОНЯТИЕ SSRF

Подделка запроса на стороне сервера или SSRF – это атака, которая позволяет отправлять запросы от имени сервера к внешним или внутренним ресурсам.

С 2021 года SSRF входит в рейтинг основных угроз безопасности веб-приложений OWASP.

ОБЩАЯ СХЕМА SSRF-АТАКИ

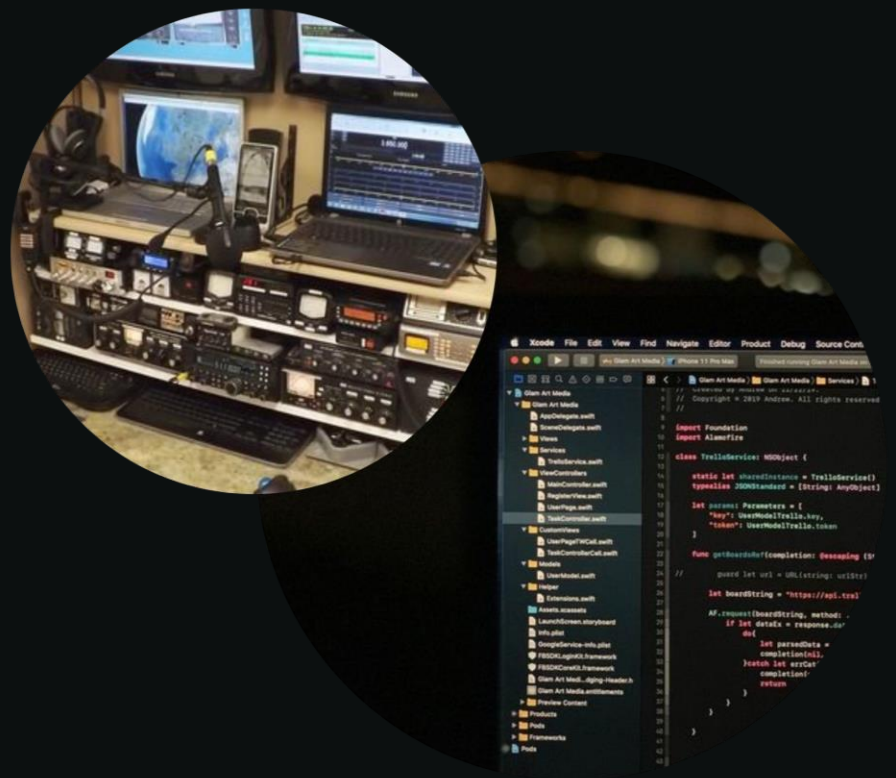


ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ SSRF-АТАК

- разоблачение и кража данных, которые могут включать конфиденциальную личную или корпоративную информацию
- несанкционированное манипулирование конфиденциальными данными
- обход авторизации
- удаленное выполнение кода
- взлом уязвимой системы, чтобы использовать ее доверительные отношения с другими системами

СЦЕНАРИЙ 1: Проверка портов на внутренних серверах

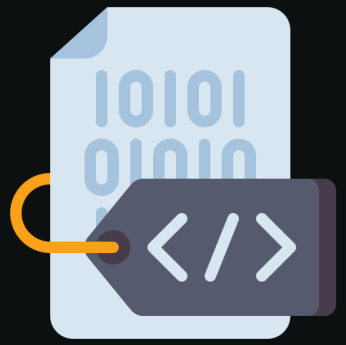
Если сетевая архитектура не сегментирована, злоумышленники могут составить карту внутренних сетей и определить, открыты или закрыты порты на внутренних серверах, основываясь на результатах успешного подключения или на времени, которое было затрачено на подключение или отклонение запроса



СЦЕНАРИЙ 2: Раскрытие конфиденциальных данных

Злоумышленники могут получить доступ к локальным файлам или внутренним службам для получения конфиденциальной информации, такой как file:///etc/passwd и http://localhost:28017/

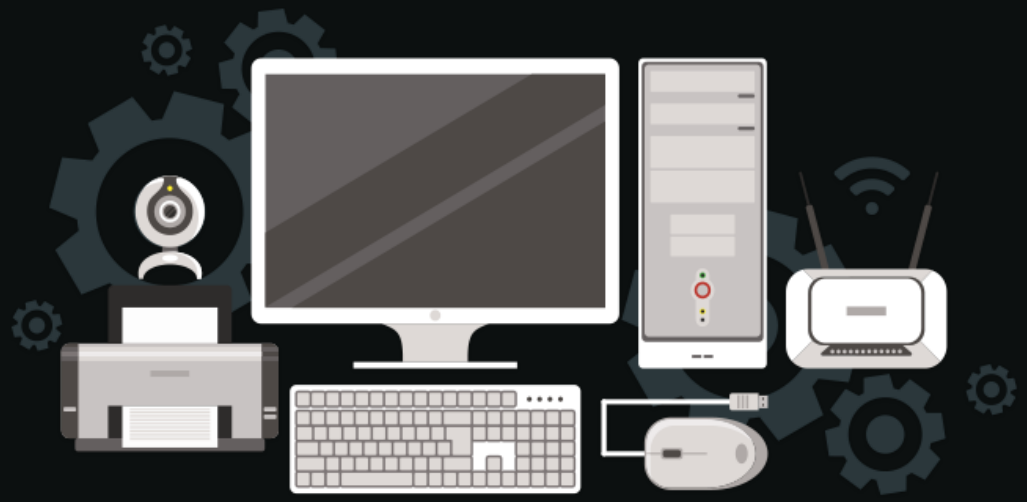
СЦЕНАРИЙ 3: Доступ к хранилищу метаданных облачных сервисов



Хранилища метаданных имеют стандартный IP-адрес вида: http://169.254.169.254/. Злоумышленник может как прочитать метаданные, чтобы получить конфиденциальную информацию, так и попытаться внести в них изменения.

СЦЕНАРИЙ 4: Компрометация внутренних служб

Злоумышленник может злоупотреблять внутренними службами для проведения дальнейших атак, таких как удаленное выполнение кода или отказ в обслуживании.



ОСНОВНАЯ КЛАССИФИКАЦИЯ АТАК

Атаки вслепую

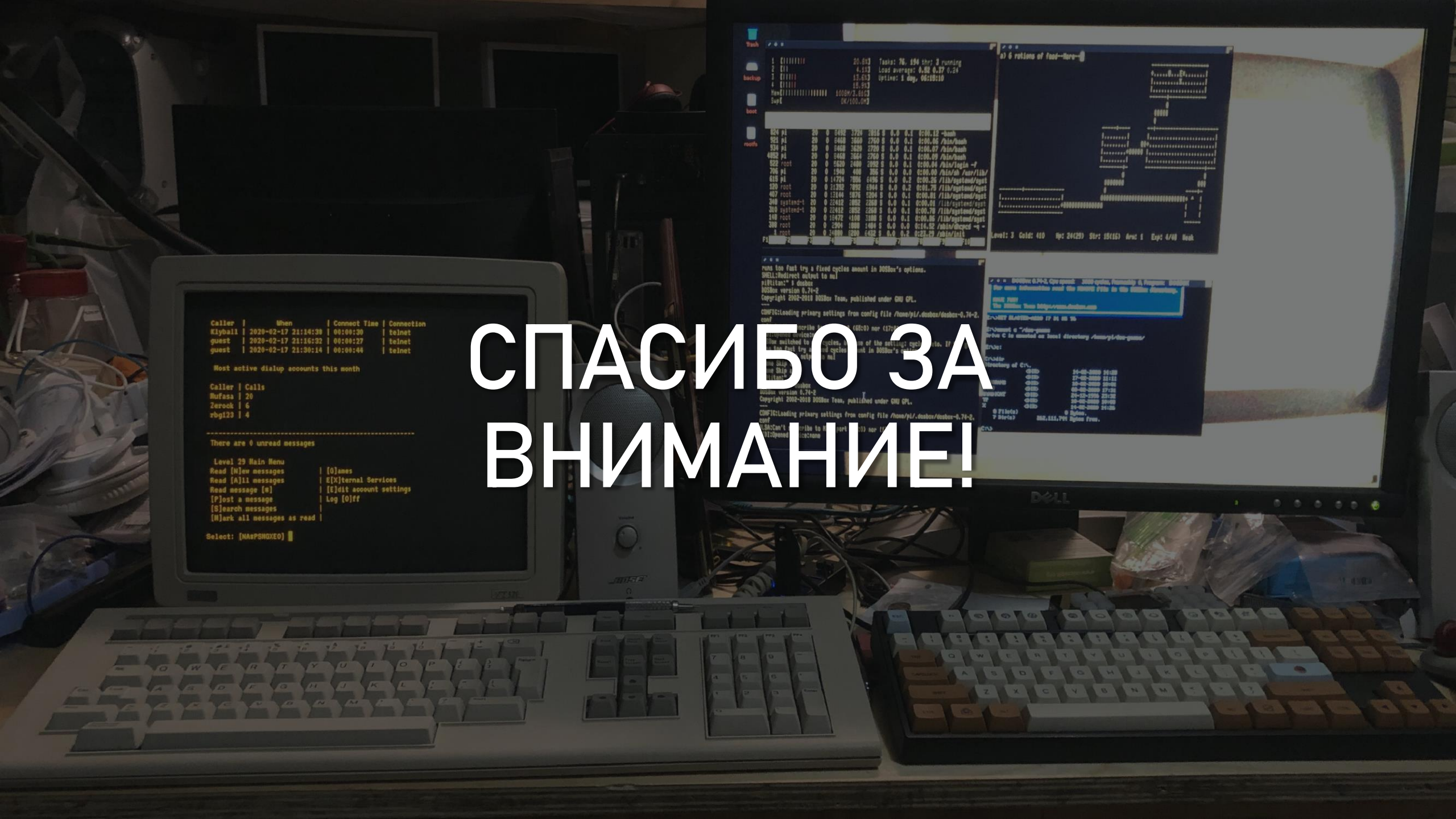
Никакие данные не возвращаются при его успешном или неудачном выполнении. Основное внимание здесь уделяется выполнению незаконного действия, а не незаконному извлечению некоторых данных

Атаки с конкретной целью

Субъект угрозы может получать выходные данные или обратную связь от сервера. По полученным визуальным данным легко определить, была ли атака успешной или неудачной

РЕКОМЕНДАЦИИ ПО ПРЕДОТВРАЩЕНИЮ АТАК

- проверка и очистка всех входных данных, предоставленных пользователем, и использование схемы URL-адреса;
- проверка согласованности URL-адресов, чтобы избежать таких атак, как повторная привязка DNS.
- применение политики брандмауэра «запретить по умолчанию» для фильтрации трафика;
- валидация доменных имен;
- четкое понимание того, как используемые библиотеки обрабатывают адреса;
- отключение поддержки перенаправлений HTTP-запросов


Caller | When | Connect Time | Connection
Klyball | 2020-02-17 21:14:38 | 00:00:30 | telnet
guest | 2020-02-17 21:16:32 | 00:00:27 | telnet
guest | 2020-02-17 21:30:14 | 00:00:44 | telnet
Most active dialup accounts this month
Caller | Calls
Mufasa | 20
Zerock | 6
rbg123 | 4
There are 0 unread messages
Level 29 Main Menu
Read [N]ew messages | [O]ames
Read [A]ll messages | E[X]ternal Services
Read message [#] | [E]dit account settings
[P]ost a message | Log [O]ff
[S]earch messages
[M]ark all messages as read
Select: [NASPSNQXEO]
СПАСИБО ЗА ВНИМАНИЕ!