

«Нас зашифровали!»

Обнаружение и реагирование шаг за шагом

Иван Кадыков
Руководитель продуктового направления

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  infotecs
ФЕСТ



Ransomware – это финальный этап атаки

До шифрования данных
злоумышленник продельывает долгий
и не легкий путь

К сожалению, на этом пути чаще
встречается «помощь» от тех кто
не соблюдает «цифровую гигиену»

Что? Как? Куда? и другие вопросы

- Выбрать жертву?
- Что доставить?
- Как доставить?
- Где взять инструментарий?
- И т.д.



Невозможно остаться незамеченным



Каждый шаг злоумышленника
зачастую фиксируется в системах,
но не все это замечают...



Рассмотрим атаку

- Мы не учим атаковать, мы показываем атаку и учим, как от нее защищаться!
- Все материалы по атакам взяты из открытых источников
- Не стоит повторять атаки дома или на работе!
- А вот средства защиты использовать надо!
- 😊 😊 😊 – всем добра!



Чем «разрушаем?» Ransomware Hellokitty

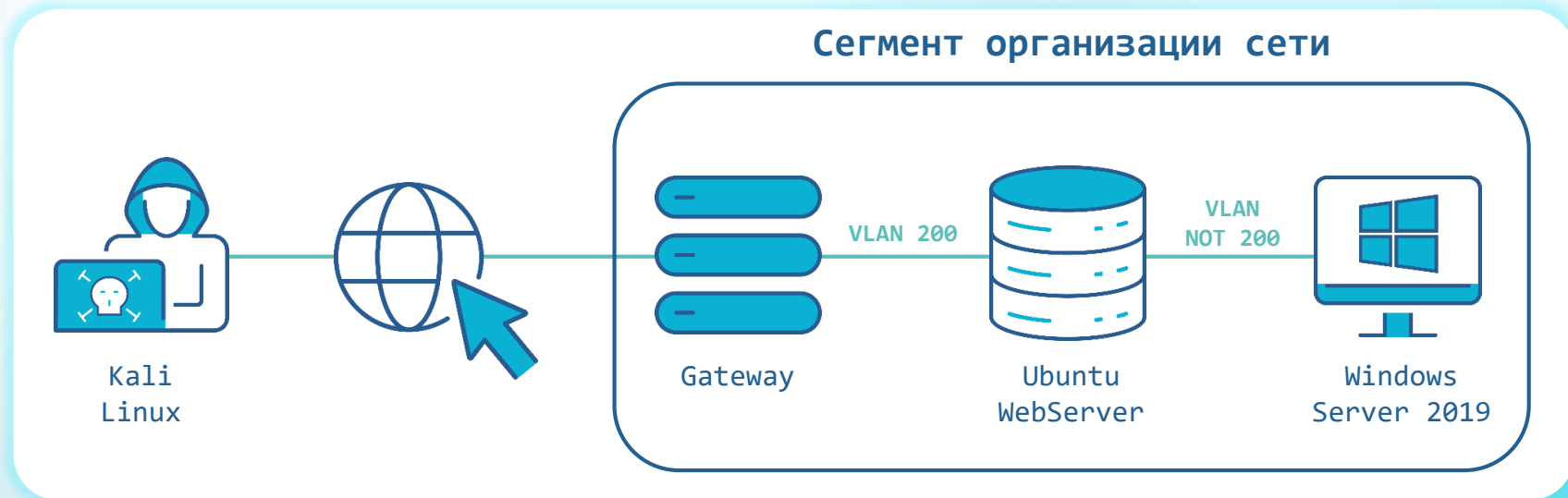
Криптовымогатель шифрует данные пользователей с помощью комбинации алгоритмов AES-256 и RSA, а затем требует выкуп в BTC

Подвергаются шифрованию: документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, архивы и пр.

В конце 2023 года исходный код шифровальщика был слит на хакерском форуме



Схема стенда



На **Ubuntu WebServer** установлен **Apache ActiveMQ** представляет собой масштабируемый брокер сообщений с открытым исходным кодом

Уязвимость **CVE-2023-46604** (CVSS: 10.0) в Apache ActiveMQ позволяет осуществлять удаленное выполнение кода (Remote Code Execution, RCE)



Начинаем!

**Шаг 2. Получение доступа
(эксплуатация CVE-2023-46604)**

T1105 Ingress Tool
Transfer

Шаг 4. Разведка

T1046 Network Service
Discovery (nmap)

Шаг 6. Выполнение атаки

T1574 Hijack Execution Flow: DLL
(DLL Sideload)
TA0004 Privilege escalation
TA0011 Command and Control
T1485 Data Destruction



Шаг 1. Разведка

T1046 Network Service
Discovery (nmap)

**Шаг 3. Загрузка Chisel.
Создание Proxy**

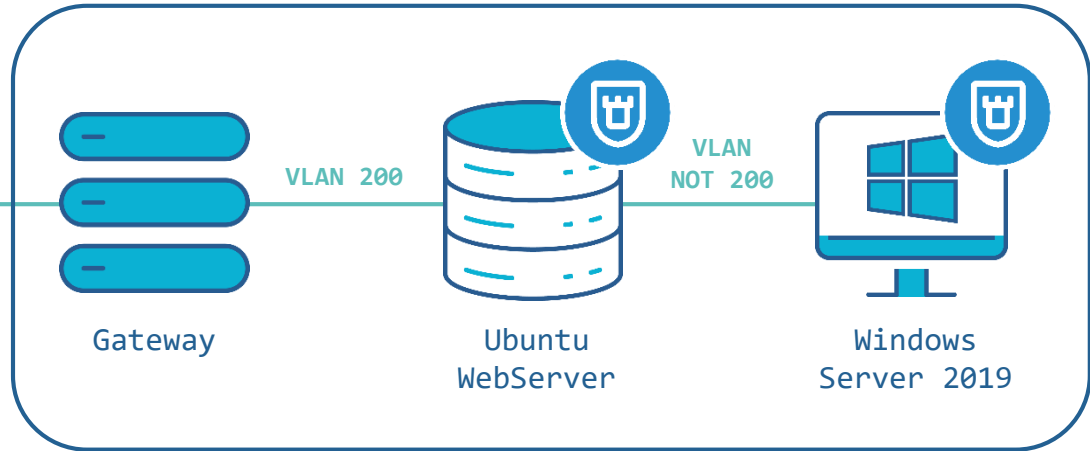
T1105 Ingress Tool Transfer
T1090 Proxy

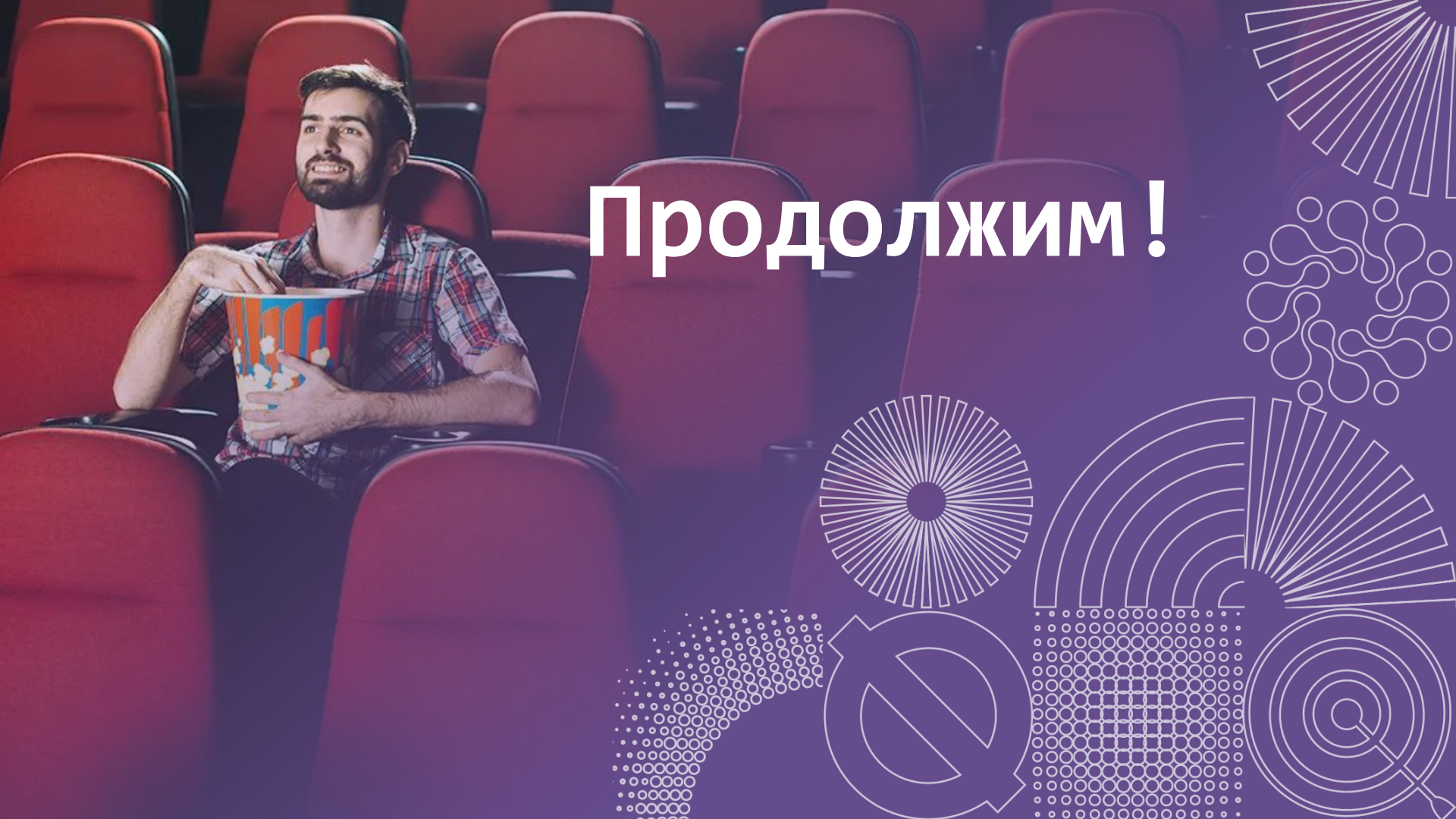
**Шаг 5. Загрузка
библиотеки и HelloKitty**

T1105 Ingress Tool Transfer

Схема стенда. Добавим ViPNet EPP для защиты

Сегмент организации сети



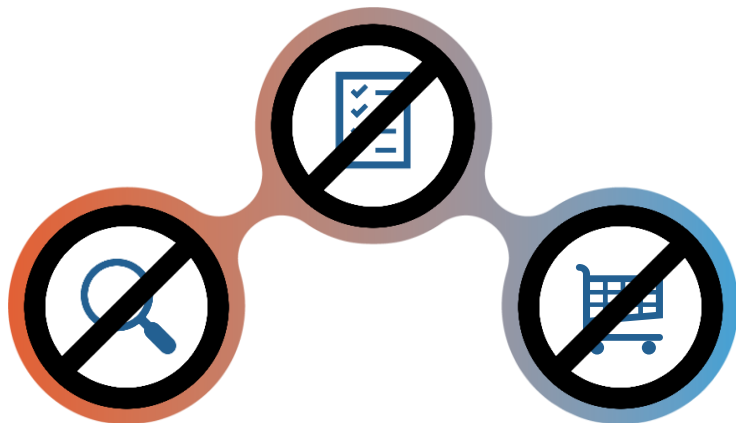


Продолжим!

На Web-сервере

~~Шаг 2. Получение доступа (эксплуатация CVE-2023-46604)~~

Обнаружена и заблокирована попытка
эксплуатации уязвимости (HIPS)



~~Шаг 1. Разведка~~

При работе FW на Web-сервере будет обнаружен и заблокирован nmap

~~Шаг 3. Загрузка Chisel. Создание Proxy~~

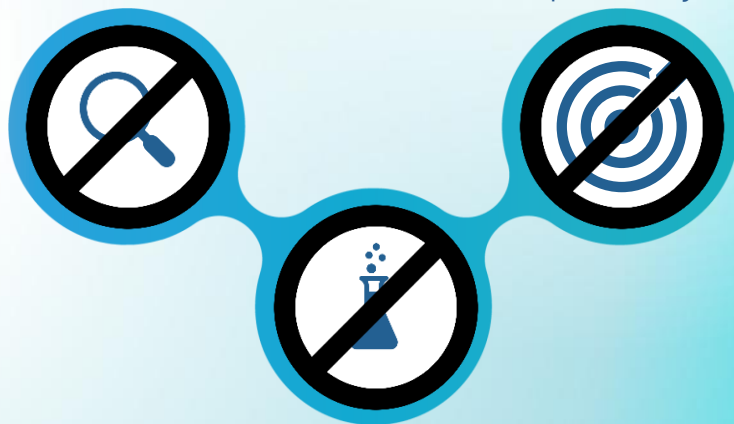
Обнаружено появление
chisel и создание
Proxy

~~Шаг 4. Разведка~~

FW в действии

~~Шаг 6. Выполнение атаки~~

Application control
в действии – обнаружен
и заблокирован запуск службы



~~Шаг 5. Загрузка библиотеки и HelloKitty~~

Обнаружена загрузка библиотеки,
файла inn

На Windows Server

Network:

- 3252853 "AM EXPLOIT [ET] Possible Apache ActiveMQ < v5.18.3 RCE Server Response (CVE-2023-46604)"
- 2049045 "ET EXPLOIT Apache ActiveMQ Remote Code Execution Attempt (CVE-2023-46604)"
- 3203947 "ET SCAN NMAP -f -sV var1"
- 2033342 "ET POLICY Chisel SOCKS Proxy Startup Observed"

Host:

- 870146 "Обнаружена активность Bash Stageless Reverse TCP"
- 870181 "Обнаружено использование утилиты "wget", связанной с загрузкой файлов из сети"
- 880005 "Обнаружена успешная аутентификация под "root"
- 902764 "Linux_TCP Tunneling Chisel"
- 500006 "Открытие RDP сеанса"
- 300799 "Использование утилиты curl"
- 200951 "Обнаружено повышение привилегий до SYSTEM через StorSvc"
- 902763 "Windows_Ransomware_HelloKitty"

ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного

