Опять зашифровали? Как это происходит и как от этого защититься

Кадыков Иван
Руководитель продуктового направления

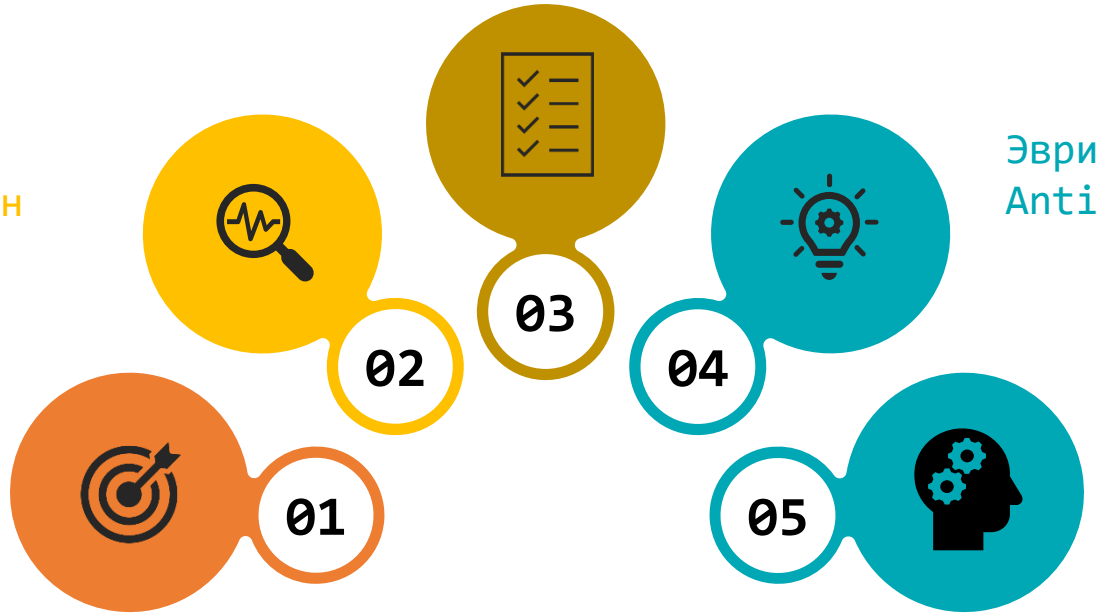
На «светлой» стороне

ViPNet EndPoint Protection

Контроль приложений

Персональный межсетевой экран

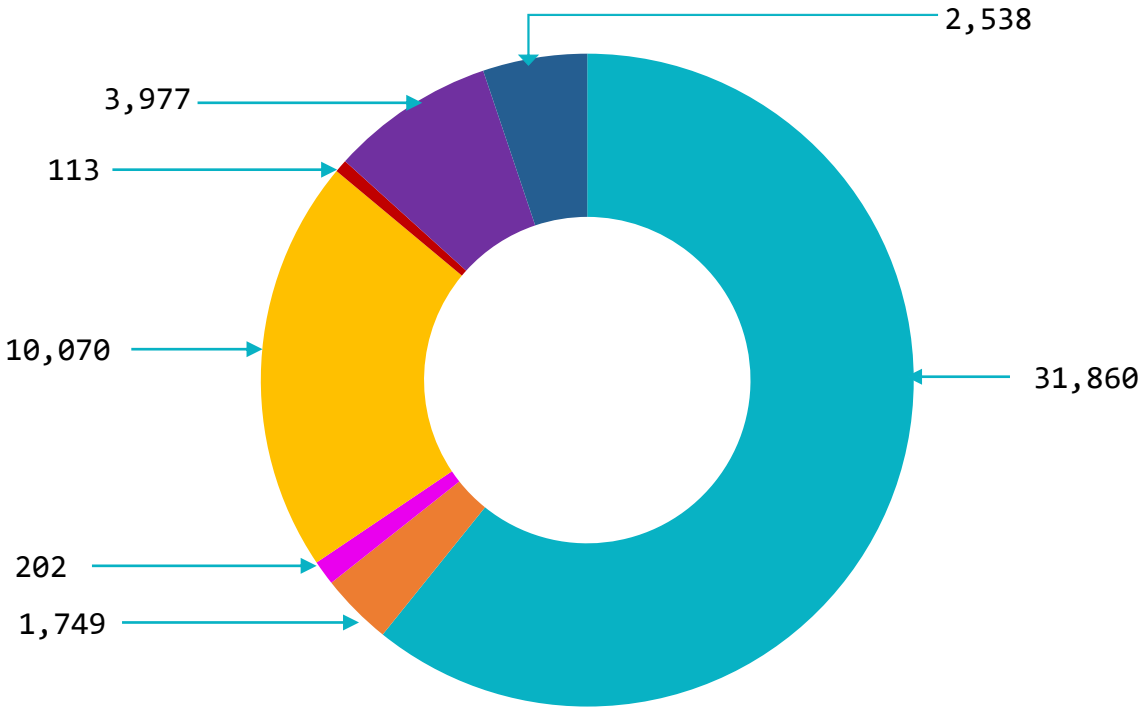
Эвристический Antimalware движок



Система обнаружения и предотвращения вторжений

Модуль поведенческого анализа

Работаем «по правилам» - БРП

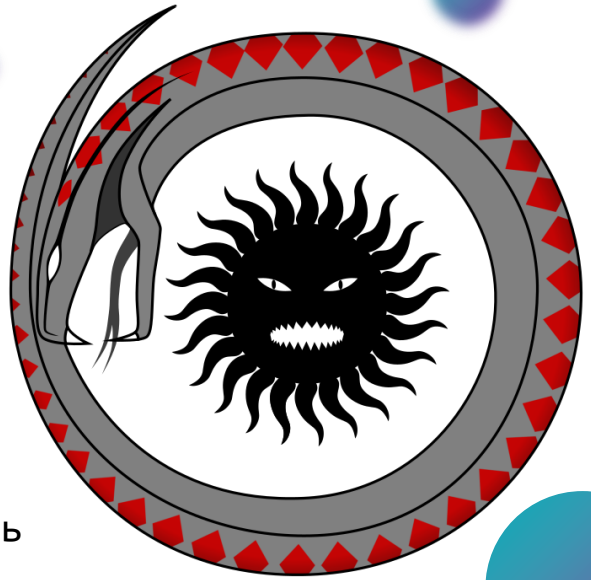


На «тёмной» стороне

- Злоумышленник
- Троян и шифровальщик - CryWiper

Что из себя представляет CryWiper?

- Троян-шифровальщик CryWiper – «клиент-серверное приложение»
- Обнаружен – Лабораторией Касперского
- «Шифрует» данные навсегда, но требует выкуп
- Уничтожает данные при помощи случайной последовательности данных
- Запрещает доступ по RDP, чтобы быстро не решить проблему у удалённых сотрудников
- Активно атаковал системы госрганов



MITRE | ATT&CK™

Секундант

Методология для специалистов ИБ

Архитектура стенда и используемые инструменты

ВАЖНО!

- 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!

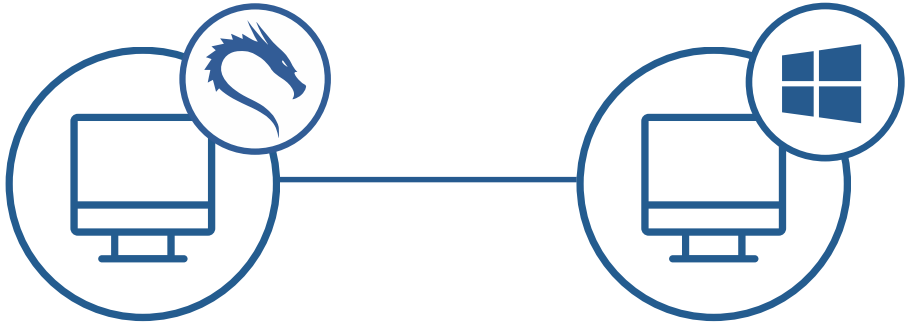
Кратко о «стенде»

У атакующего:

- Kali linux
- JNDI-Exploit
- Apache Server
- Crywiper (сервер)

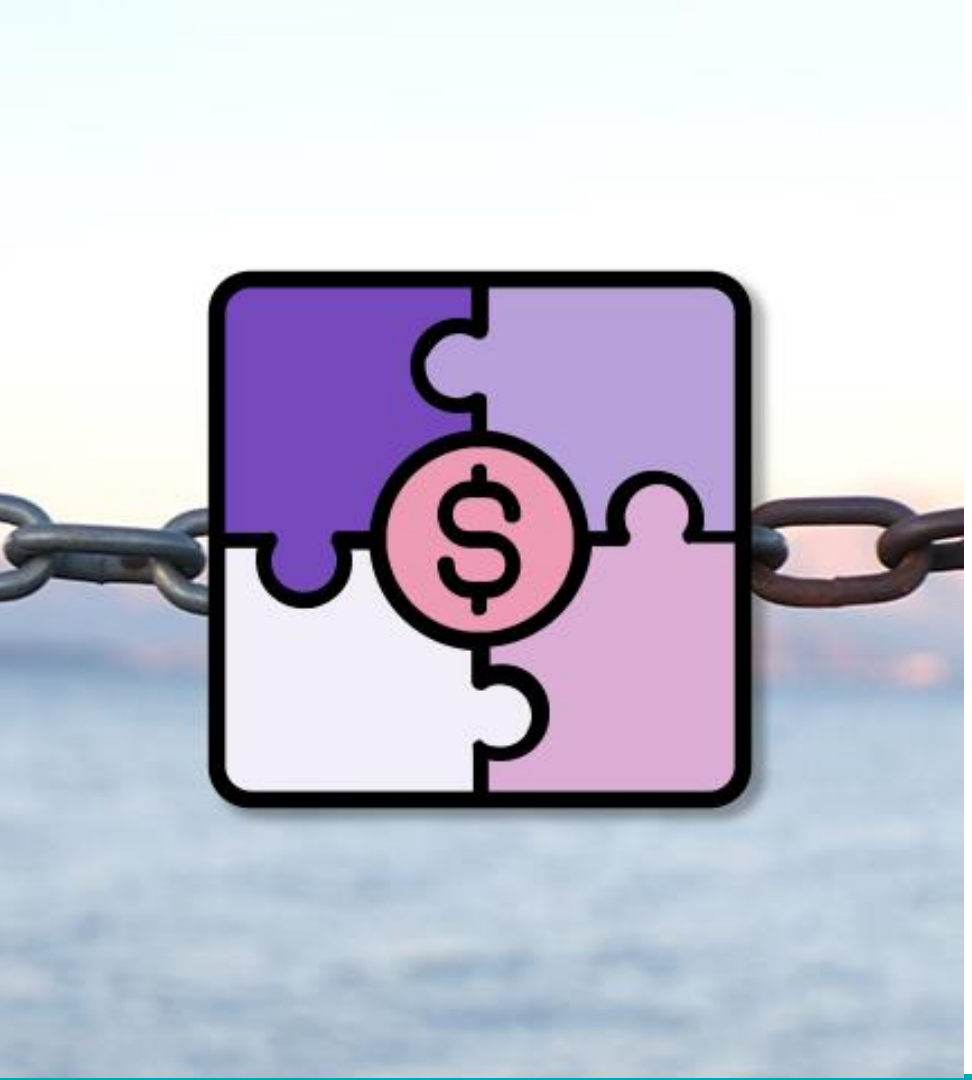
У пользователя:

- Обычная ОС Windows
- не закрытая уязвимость log4j в java-приложении (может быть любая другая уязвимость и приложение…)



Рабочая станция атакующего с Kali Linux

Рабочая станция сотрудника с Java-приложением и незакрытой уязвимостью log4j

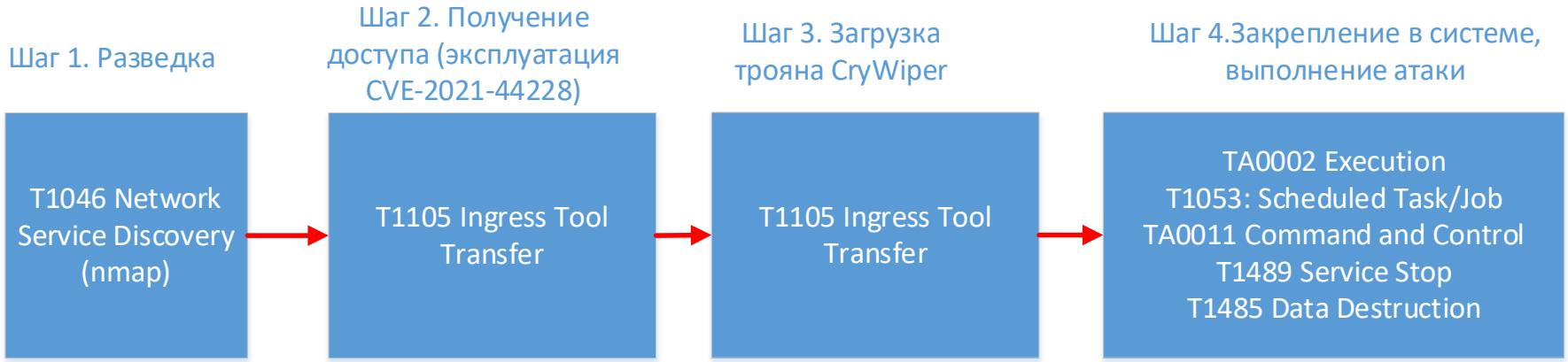


Задачи атакующего

- Провести разведку
- Выбрать средство атаки
- Выбрать средство доставки
- Доставить средство атаки
- Закрепиться в системе
- Выполнить атаку

Поехали!

А теперь «языком» MITRE

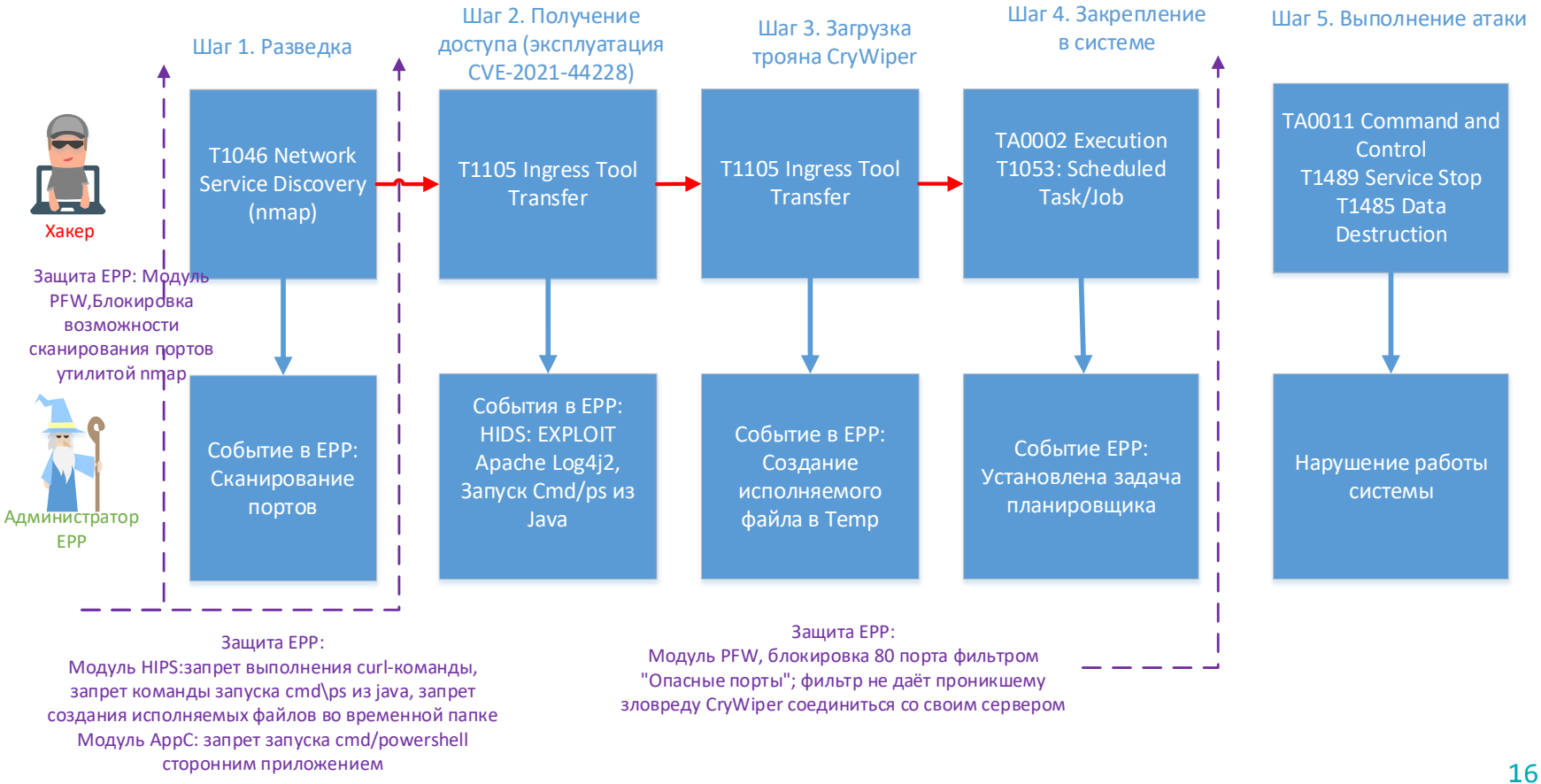


В нашей схеме появляется ViPNet EndPoint Protection

Рабочая станция атакующего
с Kali Linux

Рабочая станция сотрудника
с Java-приложением и
незакрытой уязвимостью log4j.
С установленным ViPNet
EndPoint Protection

Продолжаем!


Шаг 1. Разведка
Шаг 2. Получение доступа (эксплуатация CVE-2021-44228)
Шаг 3. Загрузка трояна CryWiper
Шаг 4. Закрепление в системе
Шаг 5. Выполнение атаки
Хакер
T1046 Network Service Discovery (nmap)
T1105 Ingress Tool Transfer
T1105 Ingress Tool Transfer
TA0002 Execution T1053: Scheduled Task/Job
TA0011 Command and Control T1489 Service Stop T1485 Data Destruction
Защита EPP: Модуль PFW,Блокировка возможности сканирования портов утилитой nmap
Событие в EPP: Сканирование портов
События в EPP: HIDS: EXPLOIT Apache Log4j2, Запуск Cmd/ps из Java
Событие в EPP: Создание исполняемого файла в Temp
Событие EPP: Установлена задача планировщика
Нарушение работы системы
Администратор EPP
Защита EPP:
Модуль HIPS:запрет выполнения curl-команды, запрет команды запуска cmd\ps из java, запрет создания исполняемых файлов во временной папке
Модуль AppC: запрет запуска cmd/powershell сторонним приложением
Защита EPP:
Модуль PFW, блокировка 80 порта фильтром "Опасные порты"; фильтр не даёт проникшему зловреду CryWiper соединиться со своим сервером

ТЕХНО 2024 infotecs ФЕСТ

Кадыков Иван
Руководитель продуктового направления

Подписывайтесь на наши соцсети