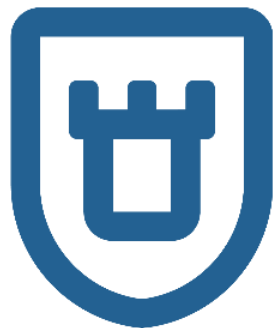


Опять зашифровали? Как это происходит и как от этого защититься

Кадыков Иван
Руководитель продуктового направления



На «светлой» стороне



VIPNet
EndPoint
Protection

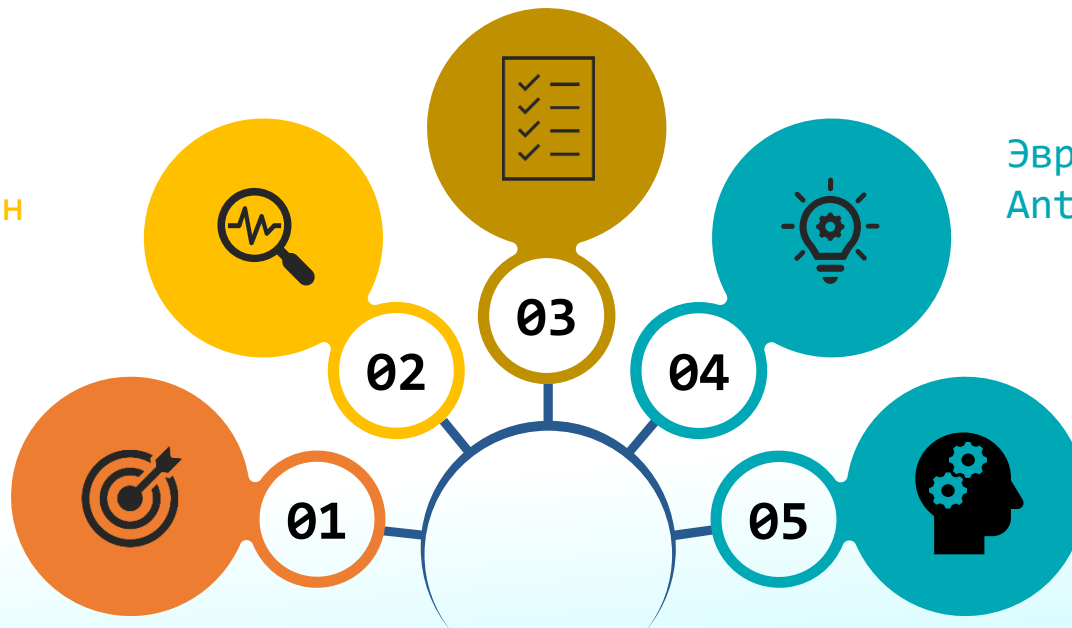


VIPNet EndPoint Protection

Контроль приложений

Персональный
межсетевой экран

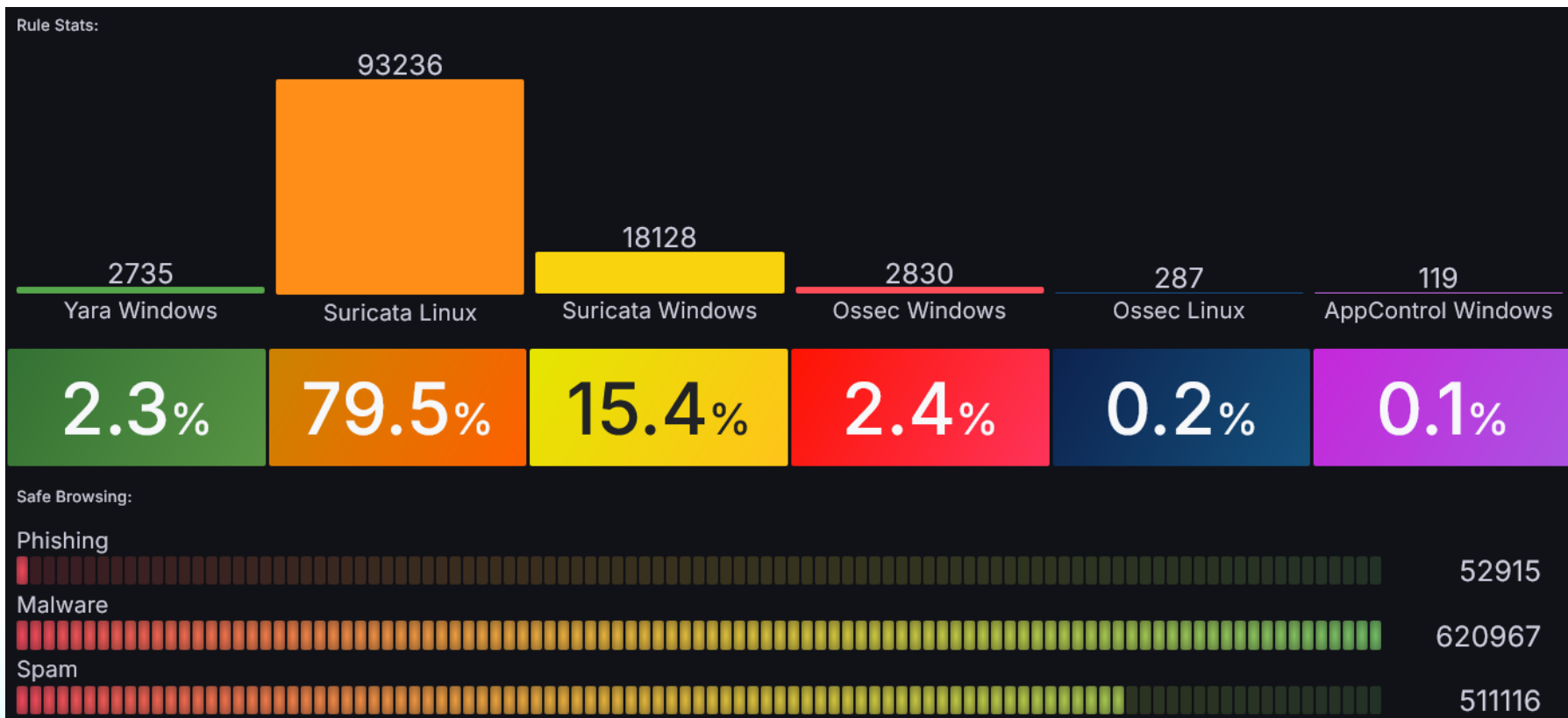
Система
обнаружения и
предотвращения
вторжений



Эвристический
Antimalware движок

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**



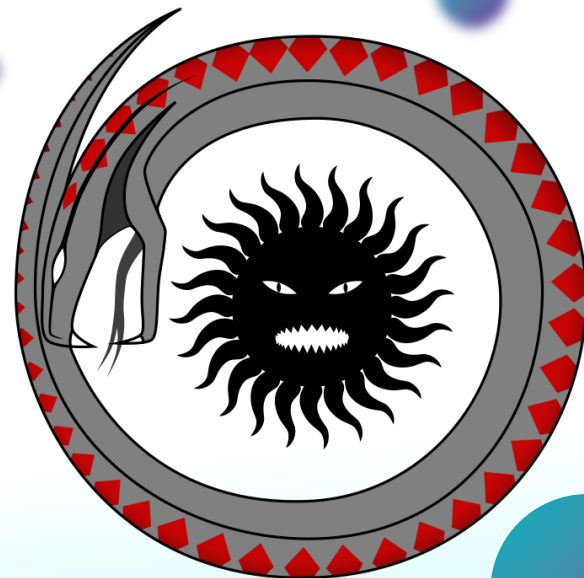
Уничтожает данные при помощи случайной
последовательности данных



Запрещает доступ по RDP, чтобы быстро
не решить проблему у удалённых сотрудников



Активно атаковал **системы госорганов**



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!

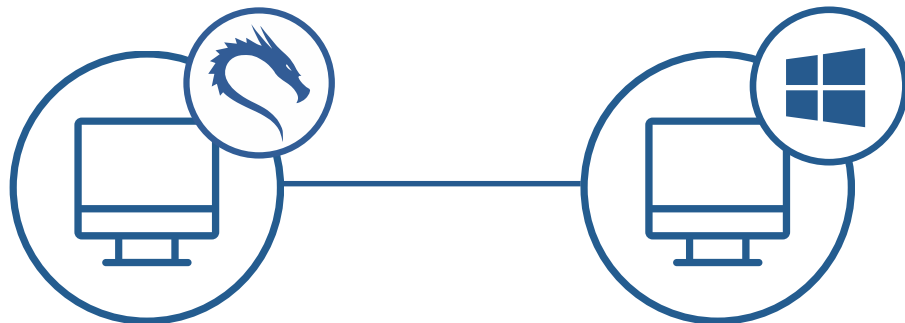
Кратко о «стенде»

У атакующего:

- Kali linux
- JNDI-Exploit
- Apache Server
- Cpuwiper (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

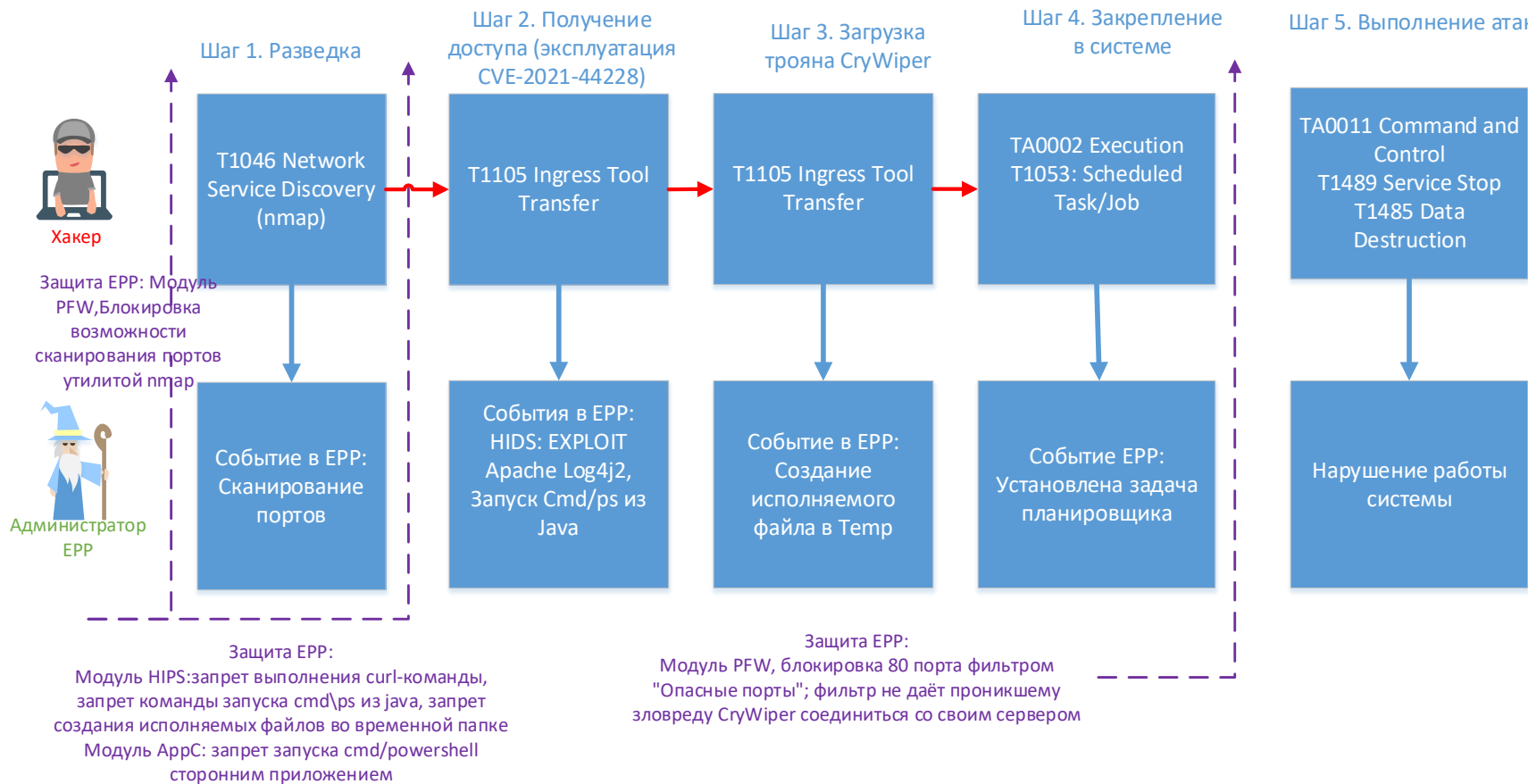


Рабочая станция атакующего
с Kali Linux

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



Продолжаем!



ТЕХНО infotecs Фест

Подписывайтесь
на наши соцсети,
там много интересного

