# Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

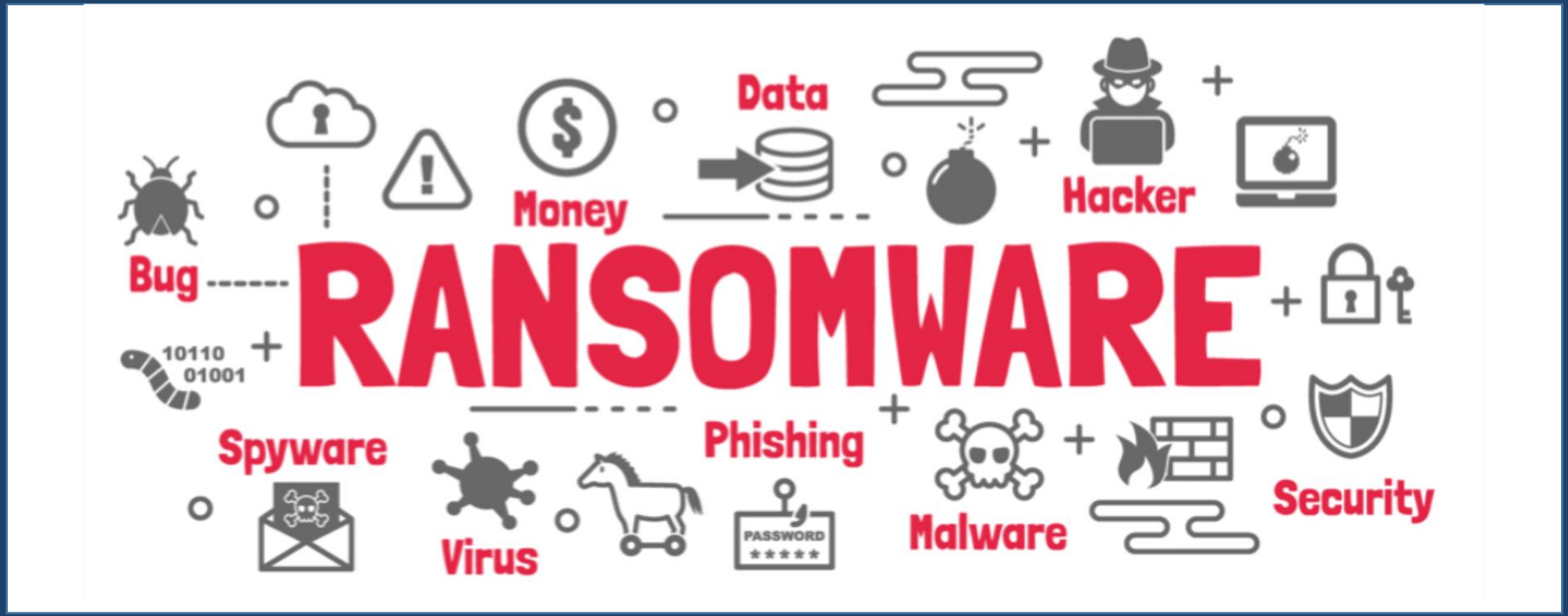
## Разбор поведения злоумышленника по MITRE ATT&CK


Кадыков Иван
Руководитель продуктового направления

ТехноФест 2023 infotecs

# О чём пойдёт речь?

# «Болезни» последних шести лет



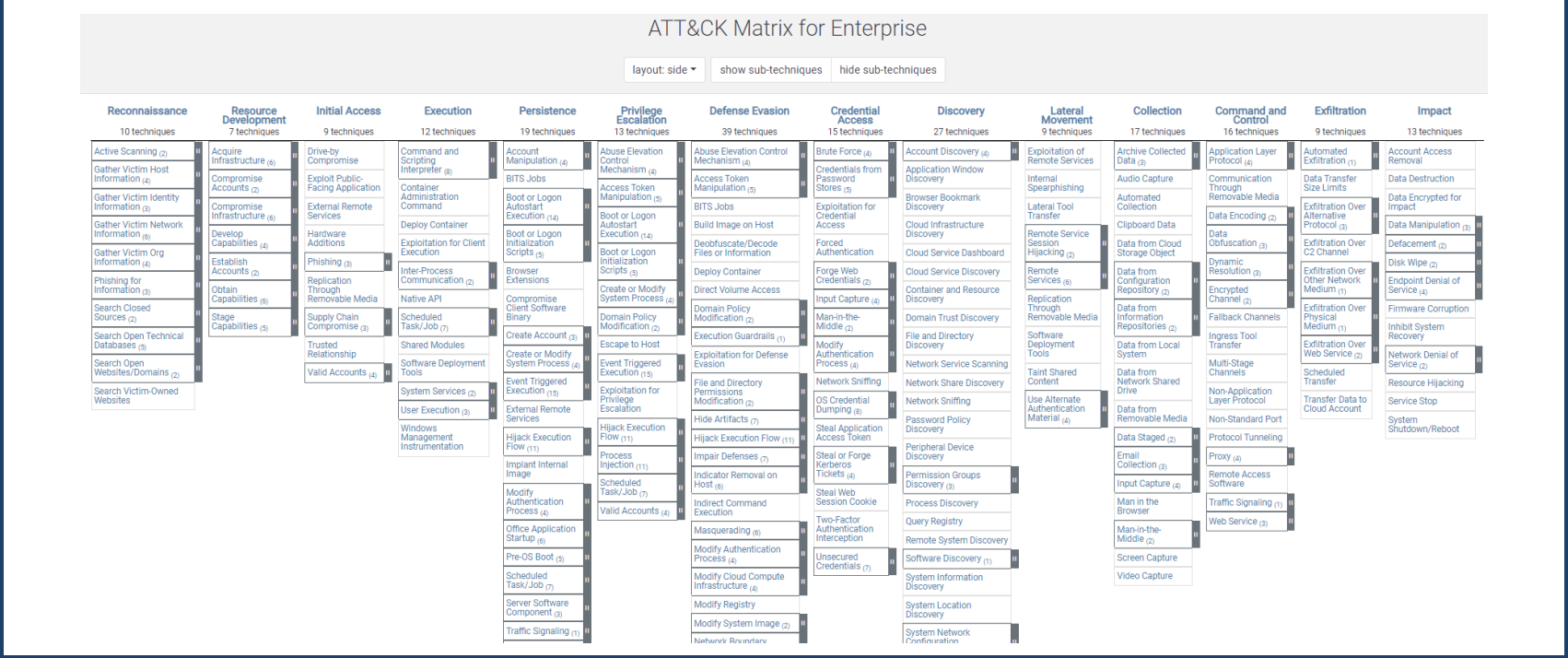

# Kill Chain

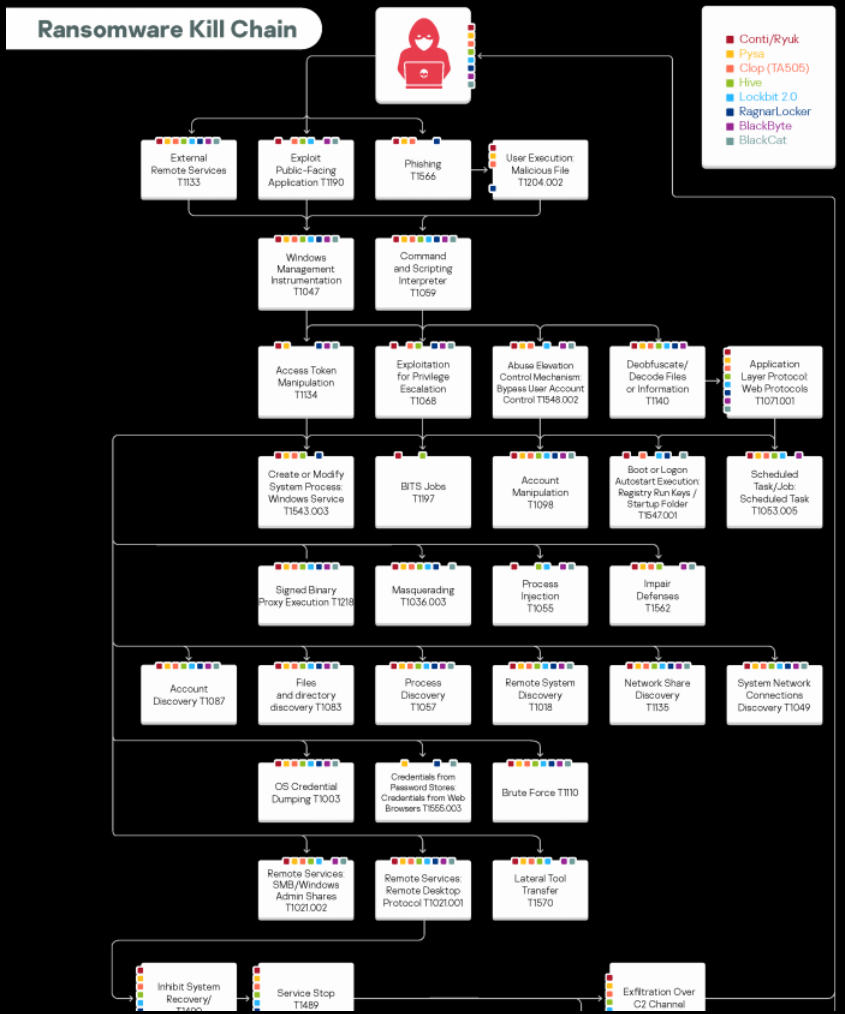
Атаку можно структурировать


**A**dversary
**T**actics
**T**echniques
**&**
**C**ommon
**K**nowledge

# Методология для специалистов ИБ

# Техники — Тактики — Процедуры





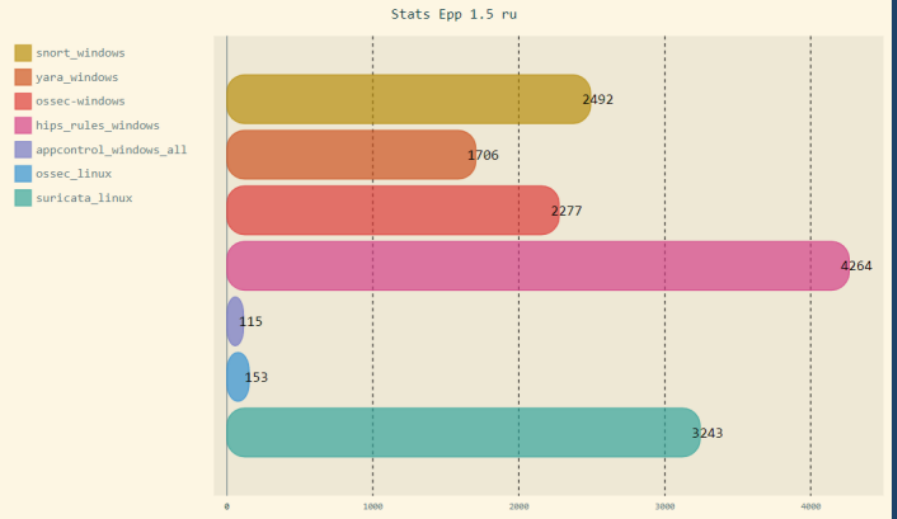

# Тактики, техники и процедуры Ransomeware группировок

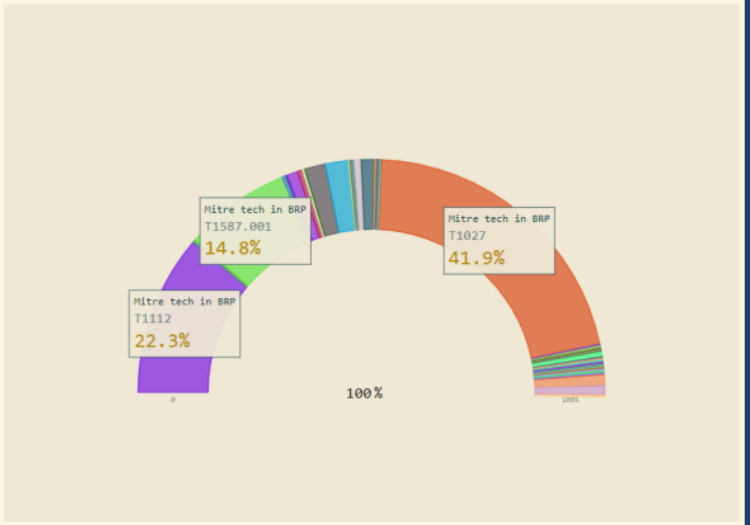
Исследования АО «Лаборатория Касперского»

Изображение взято с https://securelist.ru/modern-ransomware-groups-ttps/105553/ По ссылке можно получить полный отчёт.

# «Методика оценки угроз безопасности информации». ФСТЭК России

# ViPNet EndPoint Protection




# Небольшая статистика

**БРП:**

- Регулярно обновляем
- Актуализируем правила
- Обновляем информацию по уязвимостям

# Давайте попрактикуемся

**Продукт:**

ViPNet EndPoint Protection

**Знания:**

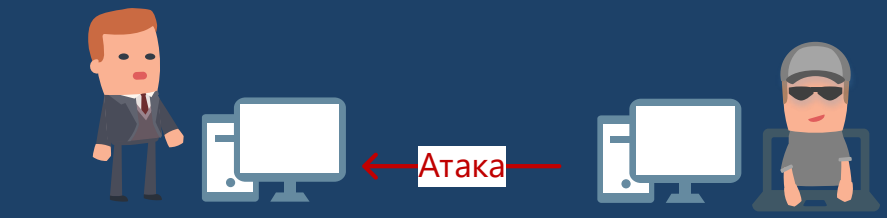
MITRE ATT&CK

# 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! ☺ ☺ ☺

# Сценарий 1. Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

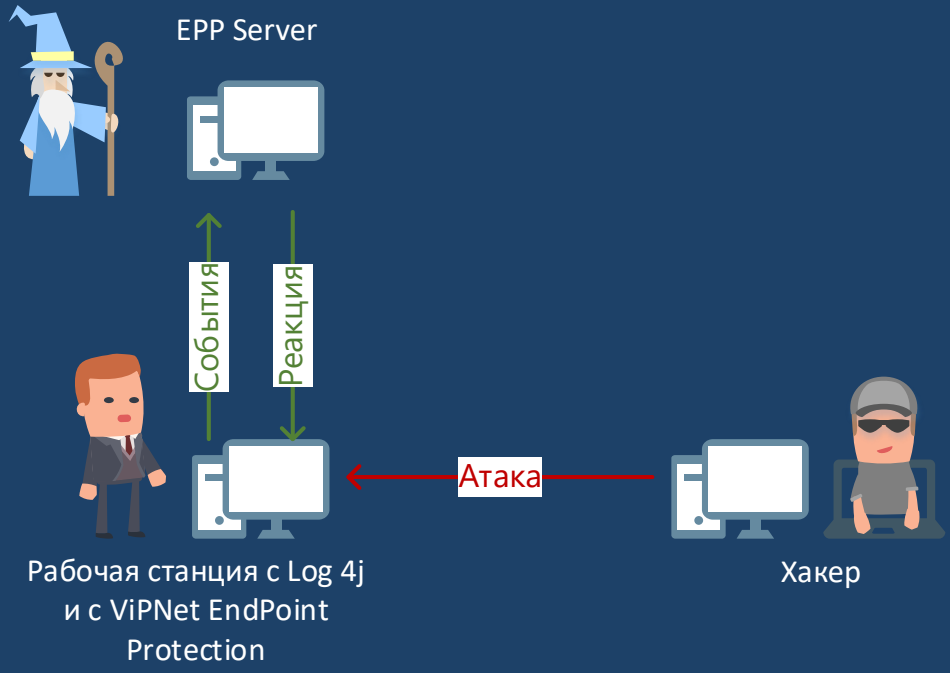
# Что за атака?




- Злоумышленник будет использовать известную уязвимость в Log4j, точнее **CVE-2021-44228**
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI)
- Запустим калькулятор через cmd

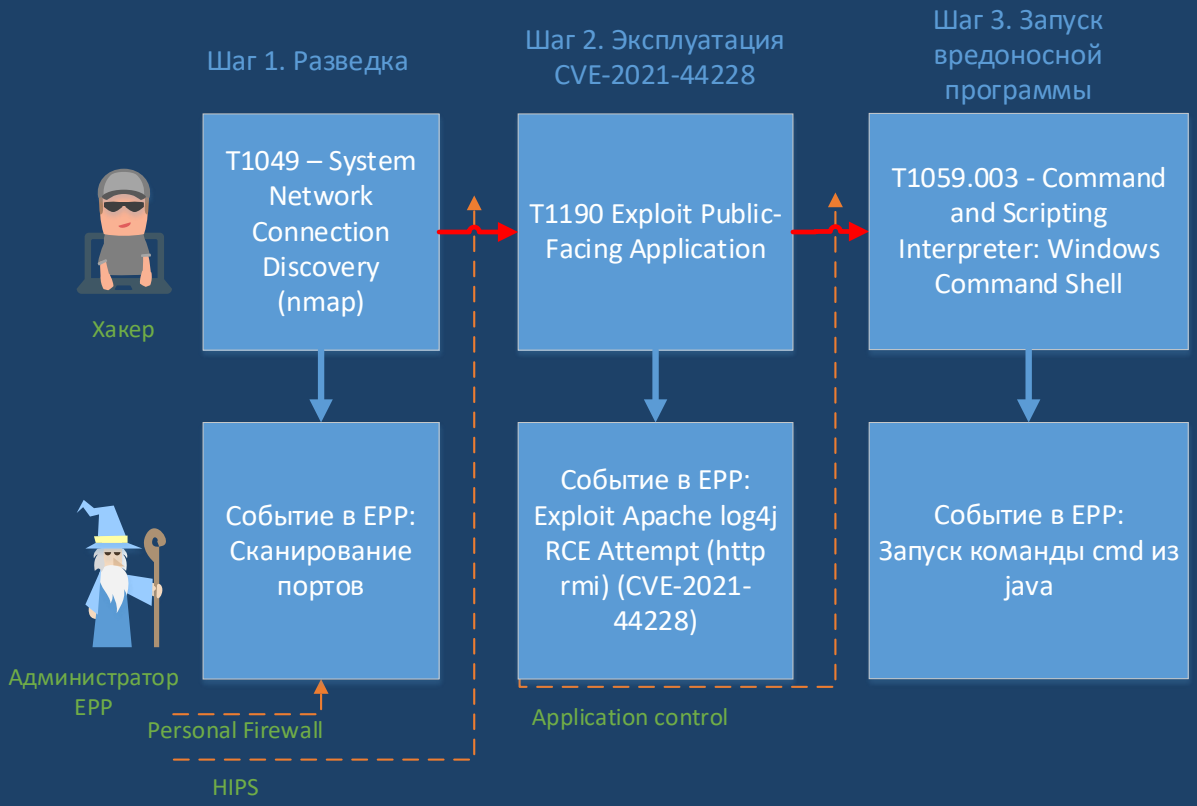

# Демонстрируем атаку!

# В инфраструктуре появился ViPNet EndPoint Protection




# Повторно атакуем, с включенным ViPNet EndPoint Protection

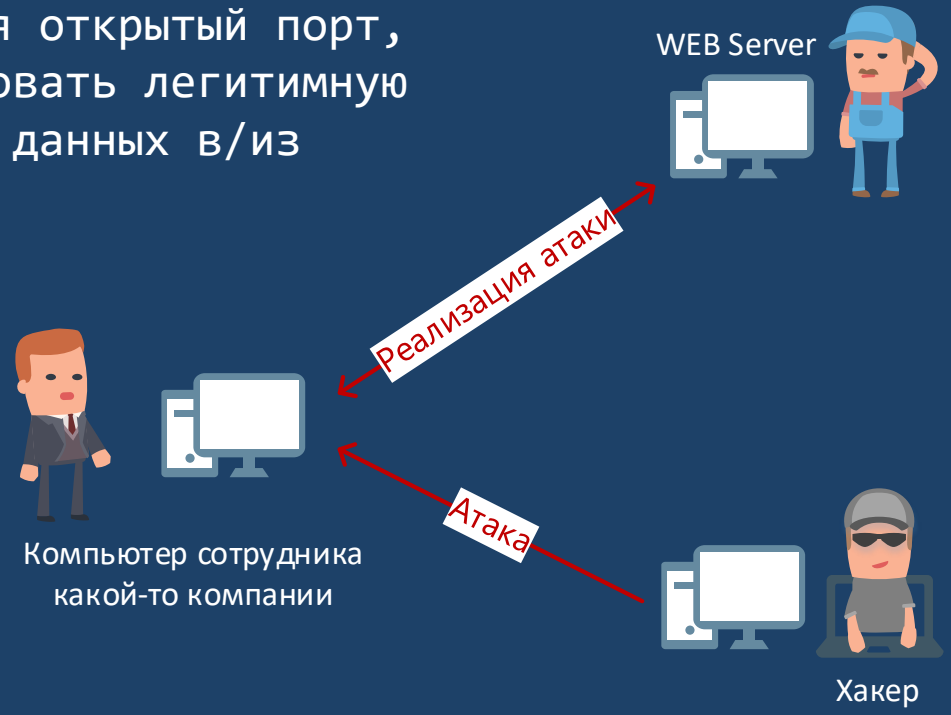
# Пошаговый разбор. Как противодействовать хакеру



# Сценарий 2. Загрузка вредоносной программы через открытый порт 22 (ssh) с использованием Resolve DNS.

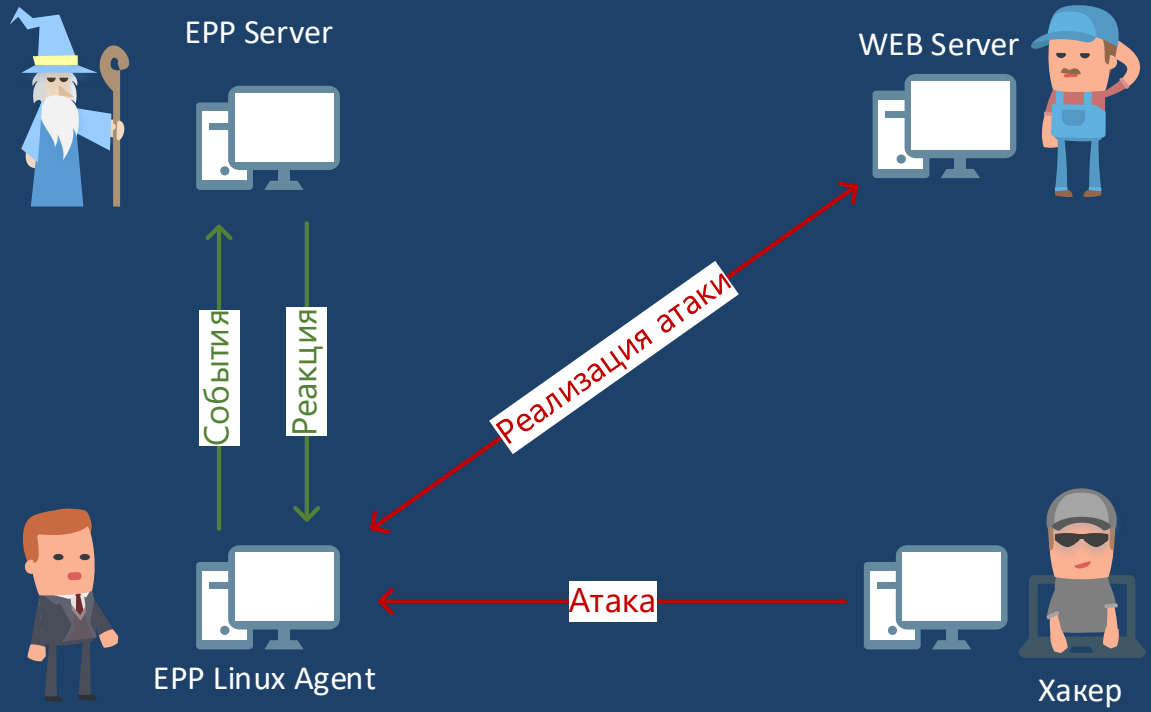
# Что за атака?

Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.

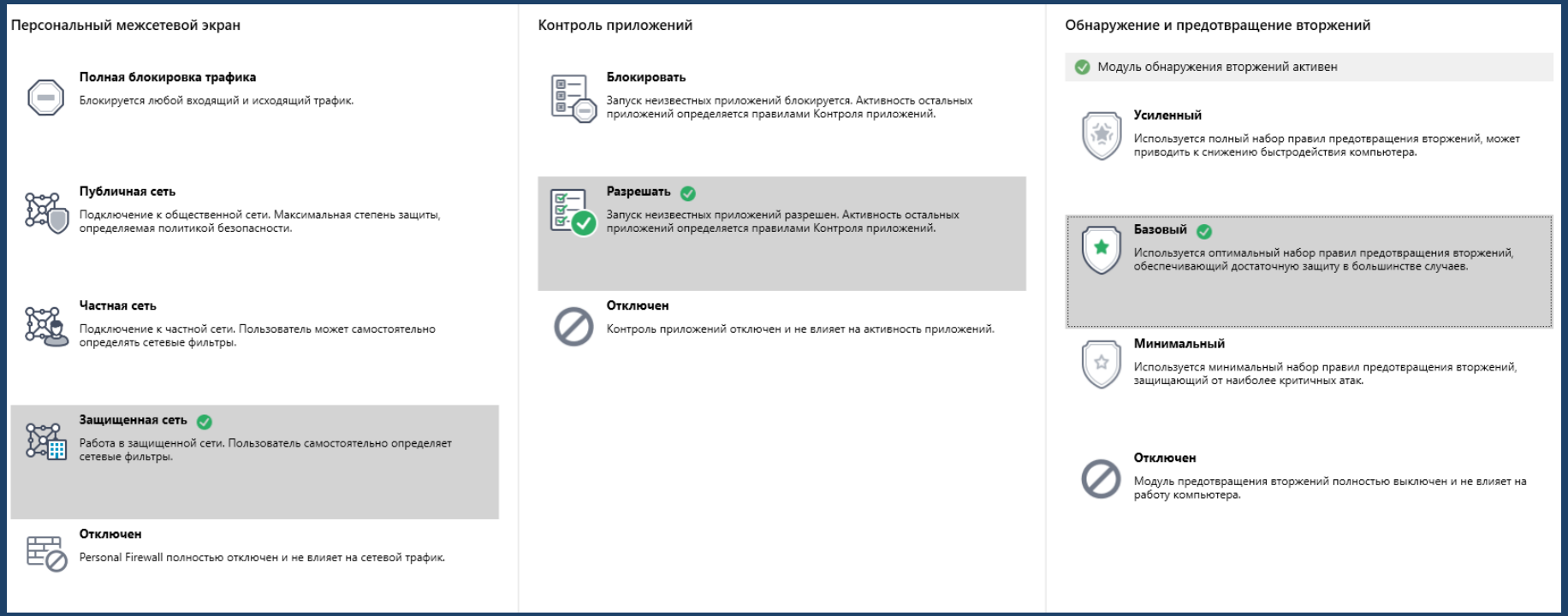



# Демонстрируем атаку!

# В инфраструктуре появился ViPNet EndPoint Protection

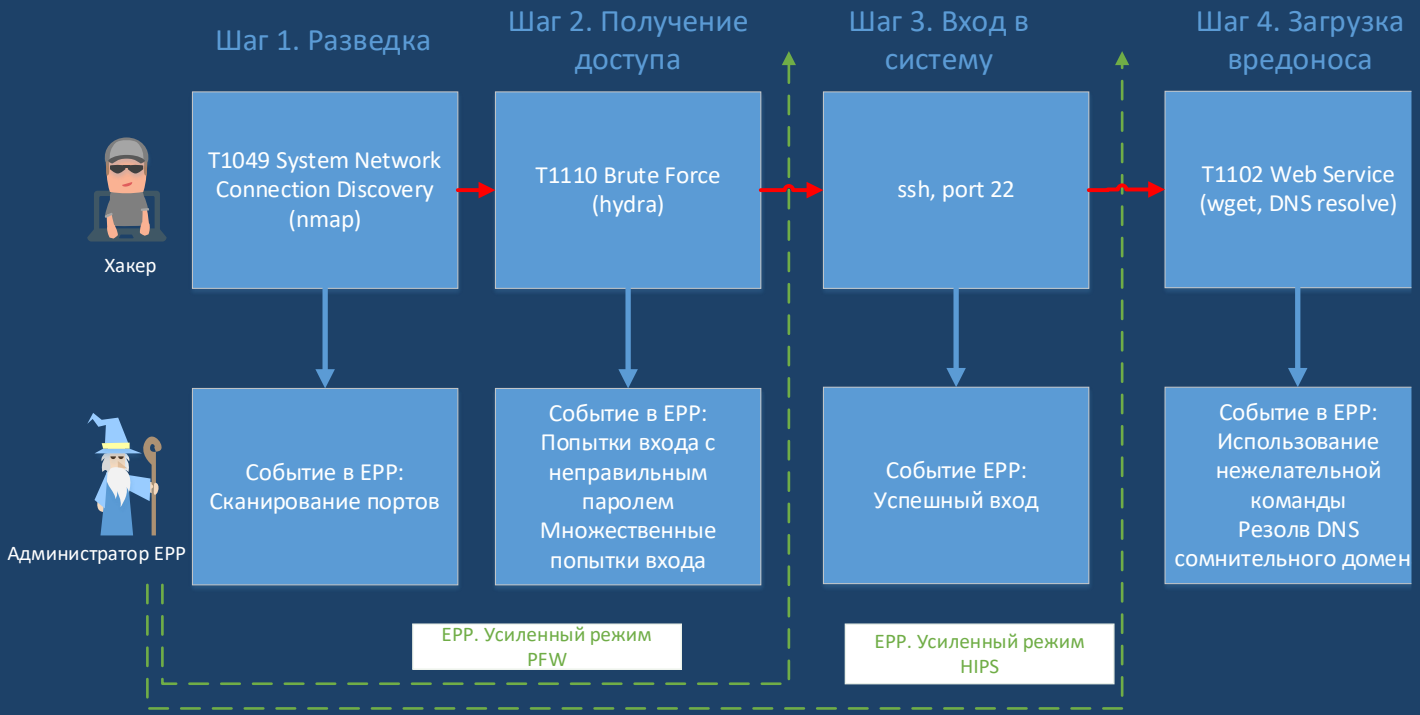


# Что же должно быть включено в EPP?




# Повторно атакуем, с включенным ViPNet EndPoint Protection

# Пошаговый разбор. Как противодействовать хакеру



ТЕХНО 2023 infotecs ФЕСТ

# Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363