МКБ

Ransomware Расследование и реагирование

Вячеслав Касимов

Апрель, 2023

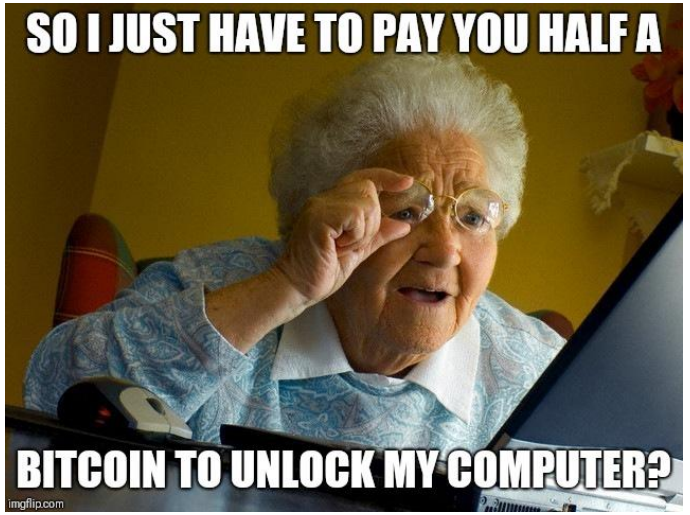
Ransomware – вообще не миф

1) Это крайне неприятно
2) Если не подготовлены, то можете остаться без бизнеса вовсе
3) Итого: лучше готовиться

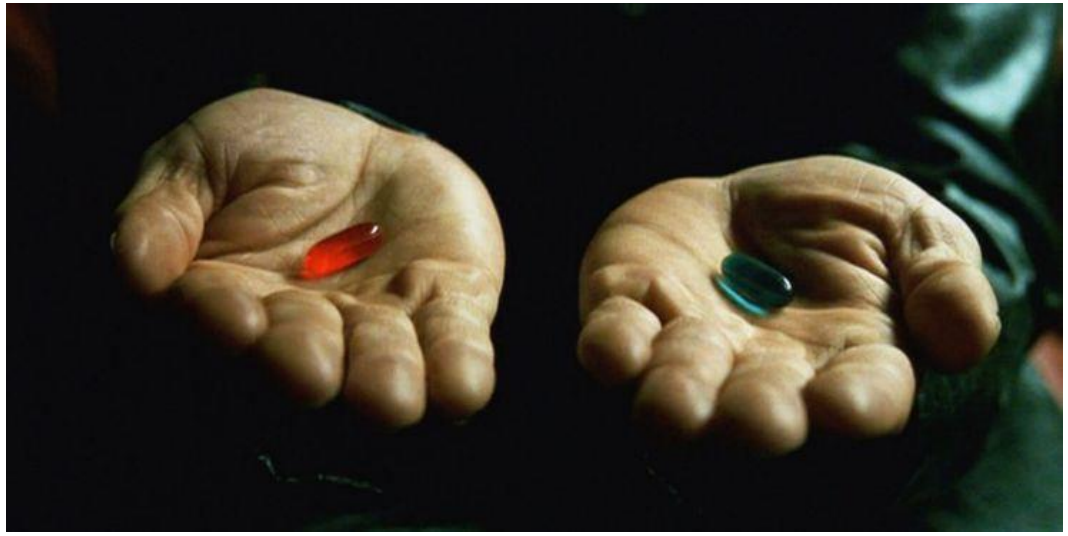
Немного фактов:

63% целенаправленных атак заканчиваются шифрованием инфраструктуры

Ransomware **не обязательно писать**.
Bitlocker и powershell/sh вполне сгодятся



Итак, Ransomware влетел в вашу инфрастуктуру



Платить по реквизитам, которые увидите (но это не точно)

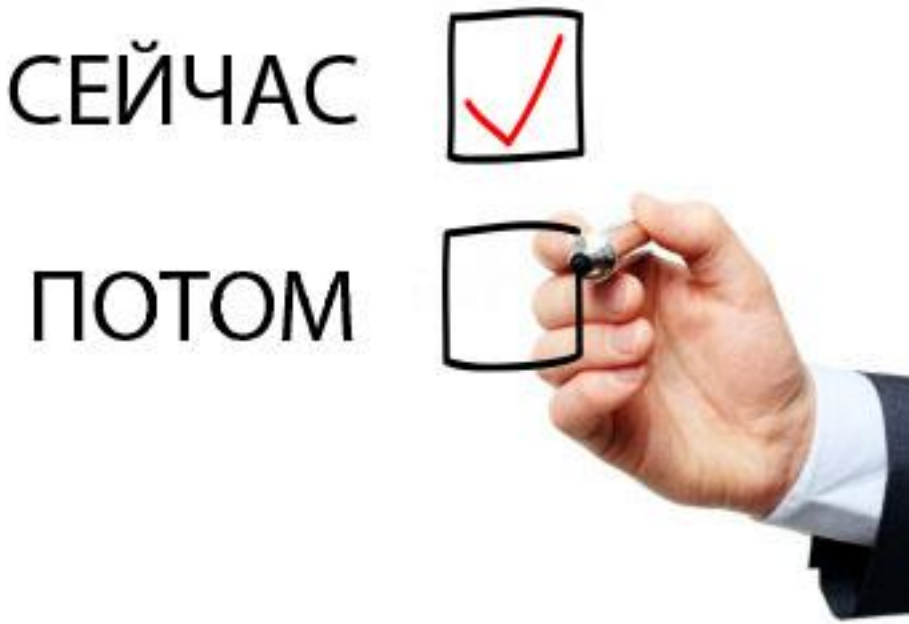
VS

Реагировать и восстанавливаться

Начало

Прежде всего определяем приоритеты:

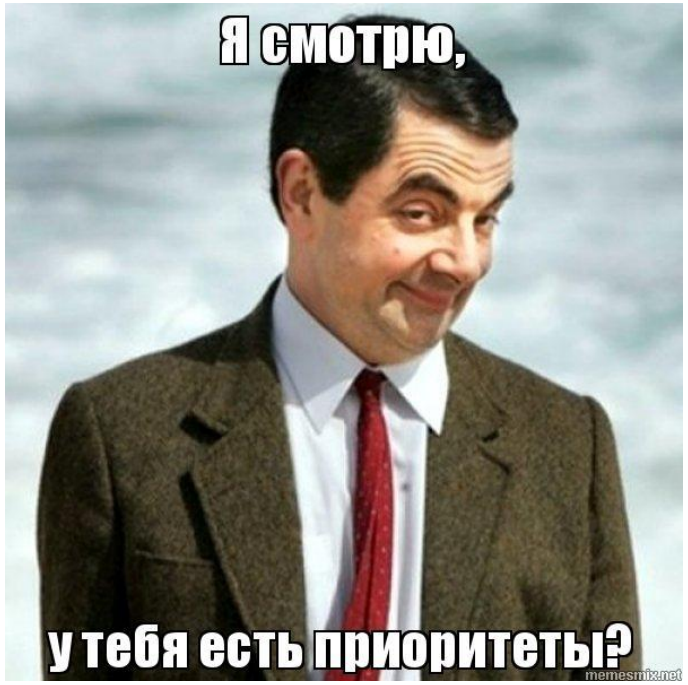
1) Восстановление работоспособности?
2) Восстановление данных?
3) Прекращение вредоносного воздействия?



Начало. Правильные ответы внезапно есть

Прежде всего определяем приоритеты:

1) Прекращение вредоносного воздействия
2) Восстановление работоспособности
3) Восстановление данных



Продолжаем. Куда бежать?

С очень высокой вероятностью вам потребуется эксперт в части форензики

Что если нет?

Тогда нужны стримы:

1) Идентифицировать точку проникновения и управления шифровальщиками
2) Попробовать выцепить ключи шифрования
3) Попробовать восстановиться из бэкапов
4) Заняться восстановлением из того, что осталось после шифровальщика

Продолжаем. Основные инструменты

Если сами зачем-то занимаетесь форензикой, то:

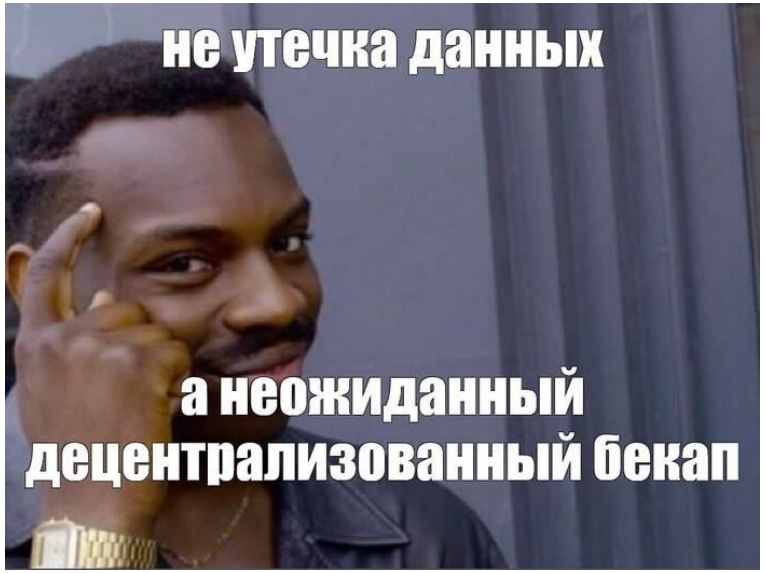
1) FTK imager
2) Registry Recon
3) volatility/RAM Capturer
4) Wireshark
5) Логи (чем больше, тем лучше)
6) Кейлоггер в DLP
7) IDA Pro

Действительно важно

1) Остановить внешнюю атаку (прекратить удаленный доступ или распространение ransomware)
2) Отреверсить ransomware, чтобы понять где может жить ключ
3) Запустить sample в контролируемой среде, чтобы на ней попытаться получить ключ
4) Попробовать найти ключ в памяти или временных файлах зашифрованной машины
5) Помнить, что если пришли хактивисты или киберармия, то, возможно, лучше потратить время на восстановление из бэкапов

Восстанавливаемся

1) Бэкапы – ваше все. Если их нет, то шансы крайне низки
2) Volume shadow copy может помочь
3) Попытаться восстановиться из частей одинаковых файлов
4) (внезапно) если данные утекли, то кажется минимум 1 бэкап у вас есть



Помните, крайне важно иметь отделенную от инфрастуктуры систему резервного копирования!

МКБ

Спасибо
за внимание!