Меня атаковал шифровальщик. Что делать?



Практический гайд от Экспертного центра безопасности Positive Technologies

Можно ли расшифровать данные без оплаты выкупа?

Скорее всего — нет, но это не означает, что всё потеряно

Для части семейств шифровальщиков существуют публичные дешифраторы или известные ключи

Иногда злоумышленники допускают ошибки в реализации шифрования, и это даёт шанс на восстановление. Но в большинстве современных атак используются стойкие схемы — рассчитывать на «лёгкий» выход не стоит.

Чтобы оценить вашу конкретную ситуацию, необходимо:

- проанализировать образец шифровальщика
- собрать первичную информацию об инциденте
- изучить записку о выкупе



Стоит ли платить выкуп?

Это сложный вопрос, и однозначного ответа нет

С одной стороны, операторы шифровальщиков — это бизнес

Им важна репутация, поэтому многие действительно предоставляют ключи после оплаты. С другой — гарантий никто не даёт. Бывают технические сбои, бывают просто нечестные группировки.

Есть и морально-этическая сторона

Оплачивая выкуп, вы финансируете дальнейшую деятельность злоумышленников и поддерживаете их мотивацию продолжать атаки.

Наш совет:

Прежде чем принимать решение об оплате, проконсультируйтесь со специалистами — возможно, ситуация не так безнадёжна, как кажется



Что делать прямо сейчас: 6 шагов

Независимо от того, будете ли вы проводить расследование, первые действия одинаковы

1. Отключите сеть от интернета и смежных инфраструктур. В крайнем случае — ограничьте доступ по белым спискам.
2. Выгрузите логи сетевых подключений, VPN и средств защиты информации — они понадобятся при расследовании.
3. Проведите инвентаризацию ресурсов, доступных извне: один из них мог стать точкой входа.
4. Не переустанавливайте и не выключайте скомпрометированные системы — вы можете уничтожить следы.
5. Будьте осторожны с восстановлением из бэкапов — они тоже могут быть скомпрометированы.
6. Сохраните файл шифровальщика, если он доступен — он нужен для анализа.

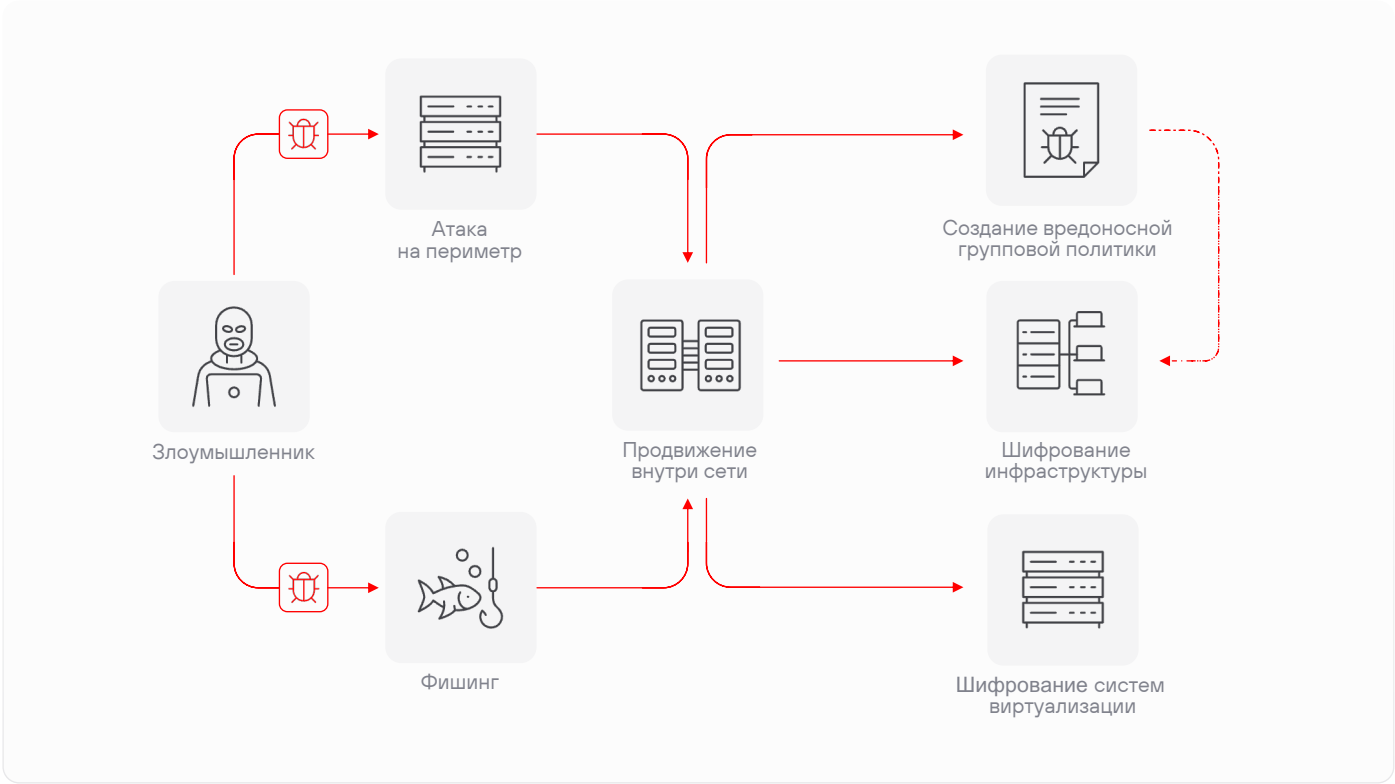
Зачем проводить расследование?

Если злоумышленник однажды попал
в вашу инфраструктуру — велика вероятность,
что он всё ещё там и потенциально может вернуться



Большинство атак с шифровальщиками — это не случайность, а управляемые многоэтапные операции

Злоумышленники изучают вашу сеть, ищут ключевые системы, получают привилегированные учётные записи — и нередко выгружают данные ещё до шифрования, чтобы потом угрожать их публикацией



Расследование позволяет:

Восстановить путь злоумышленника и найти исходный вектор атаки

Обнаружить точки закрепления, которые он мог оставить

Выяснить, какие данные были выгружены и куда

Как работает расследование с PT ESC



Как это выглядит на практике

Мы работаем удалённо — это позволяет подключиться быстро, без потери времени на организационные вопросы

1 Первичный сбор данных

Мы высылаем утилиту для снятия данных и подсказываем, с каких хостов начать в первую очередь. Обычно это Windows-серверы, подвергшиеся шифрованию, и контроллеры домена.

2 Оперативный анализ

Уже на этом этапе мы начинаем давать значимую информацию: какие техники использовал злоумышленник, какие серверы управления нужно заблокировать на периметре, где искать следы дальше.

3 Углублённое исследование

После локализации инцидента проводим детальный анализ: оцениваем масштабы, ищем оставшиеся точки закрепления, восстанавливаем полную картину атаки.

4 Финальный отчёт

Вы получаете документ с описанием инцидента, выявленными недостатками в безопасности инфраструктуры и конкретными рекомендациями по их устранению. Если в процессе удастся найти способ расшифровки или восстановления данных — эта информация тоже войдёт в отчёт.

Не уверены, что атака закончилась?

Иногда компании восстанавливаются из резервных копий — и считают инцидент закрытым. Но если злоумышленник закрепился в системе до создания бэкапа, он никуда не ушёл.

В таких случаях имеет смысл провести ретроспективный анализ инфраструктуры — даже без активного инцидента. Это позволяет обнаружить следы компрометации, которые не были замечены в процессе самостоятельного восстановления инфраструктуры, и убедиться, что в системе больше никого нет.

Команда PT ESC готова помочь — на любом этапе: от первых часов инцидента до глубокого разбора того, что произошло



Связаться с нами

Напишите нам:
secserv@ptsecurity.com

Присоединяйтесь к нам:
t.me/ptescalator

Узнайте больше:
ptsecurity.com/services/esc/