ANGARA SECURITY

ШИФРОВАЛЬЩИКИ

КАК НЕ ПОТЕРЯТЬ ДАННЫЕ И СОХРАНИТЬ БИЗНЕС

Программы-вымогатели существуют уже три десятилетия. За эти годы они эволюционировали из гипотетической угрозы в один из наиболее разрушительных инструментов современных кибератак.

Мировая статистика демонстрирует устойчивый рост атак с использованием программ-вымогателей: в первом квартале 2025 года их количество увеличилось на 126% по сравнению с аналогичным периодом в 2024 году. Согласно данным Positive Technologies, в 2024 — первой половине 2025 года в странах СНГ на долю шифровальщиков приходилось 44% всех вредоносных атак на организации с использованием вредоносного ПО (ВПО). При этом около 90% таких атак инициировались преступниками, мотивированными финансовой выгодой.

О ПРОГРАММАХ-ВЫМОГАТЕЛЯХ

Программа-вымогатель — это вредоносное ПО, которое блокирует доступ к системе или файлам до тех пор, пока жертва не заплатит выкуп. Блокировка доступа к системе может происходить по-разному, в зависимости от вида атаковавшего ВПО.

Основные виды программ-вымогателей

БЛОКИРОВЩИКИ

- Ограничивают доступ к устройству и не позволяют жертве использовать компьютер, при этом не повреждают пользовательские файлы.
- Менее опасны, так как блокировку можно обойти.

ВАЙПЕРЫ

- Уничтожают данные на диске без возможности восстановления.
- Иногда это происходит из-за ошибок в коде вредоноса, но чаще — умышленно, чтобы навредить бизнесу.

ШИФРОВАЛЬЩИКИ

- Шифруют пользовательские файлы и переименовывают их, добавляя специфическое для данного ВПО расширение.
- Без ключа расшифровки (дешифратора) восстановить данные невозможно.
- Некоторые варианты ВПО шифруют загрузочную запись (MBR), из-за чего система не запускается.

Заражение программой-вымогателем

Заражение программой вымогателем

Вредоносное ПО уничтожает или шифрует файлы

От жертвы требуют оплатить выкуп за востановление данных

ПОЧЕМУ ЗЛОУМЫШЛЕННИКИ ИСПОЛЬЗУЮТ ШИФРОВАЛЬЩИКИ

Это самый популярный способ вымогательства благодаря своей эффективности: жертвы, опасаясь безвозвратной потери данных, часто соглашаются платить за дешифратор.

Даже после оплаты нет гарантии, что данные восстановят.
Лучшая защита — комплексные превентивные меры и резервные копии.

Начало эры вымогателей

Первая известная атака с использованием программы-вымогателя произошла в конце 1980-х. Вредоносный троян AIDS заражал компьютеры через дискеты, якобы содержащие информацию о борьбе со СПИДом. Преступники использовали простое симметричное шифрование и требовали от жертв отправить выкуп почтовым переводом, чтобы вернуть доступ к данным.

Эволюция: от массовых атак к точечным

С появлением криптовалют в 2010-х злоумышленники получили возможность получать выкуп в больших суммах анонимно.

2013–2016: Spray and Pray

Преступники стремились заразить как можно больше случайных пользователей, требуя с них небольшие суммы в качестве выкупа. Но такой подход требовал огромного охвата для прибыли и постепенно устарел.

После 2016: Big Game Hunting (BGH)

Вымогатели перешли на целевые атаки против крупных компаний, способных заплатить миллионы. Это повысило доходы и дало больше рычагов давления.

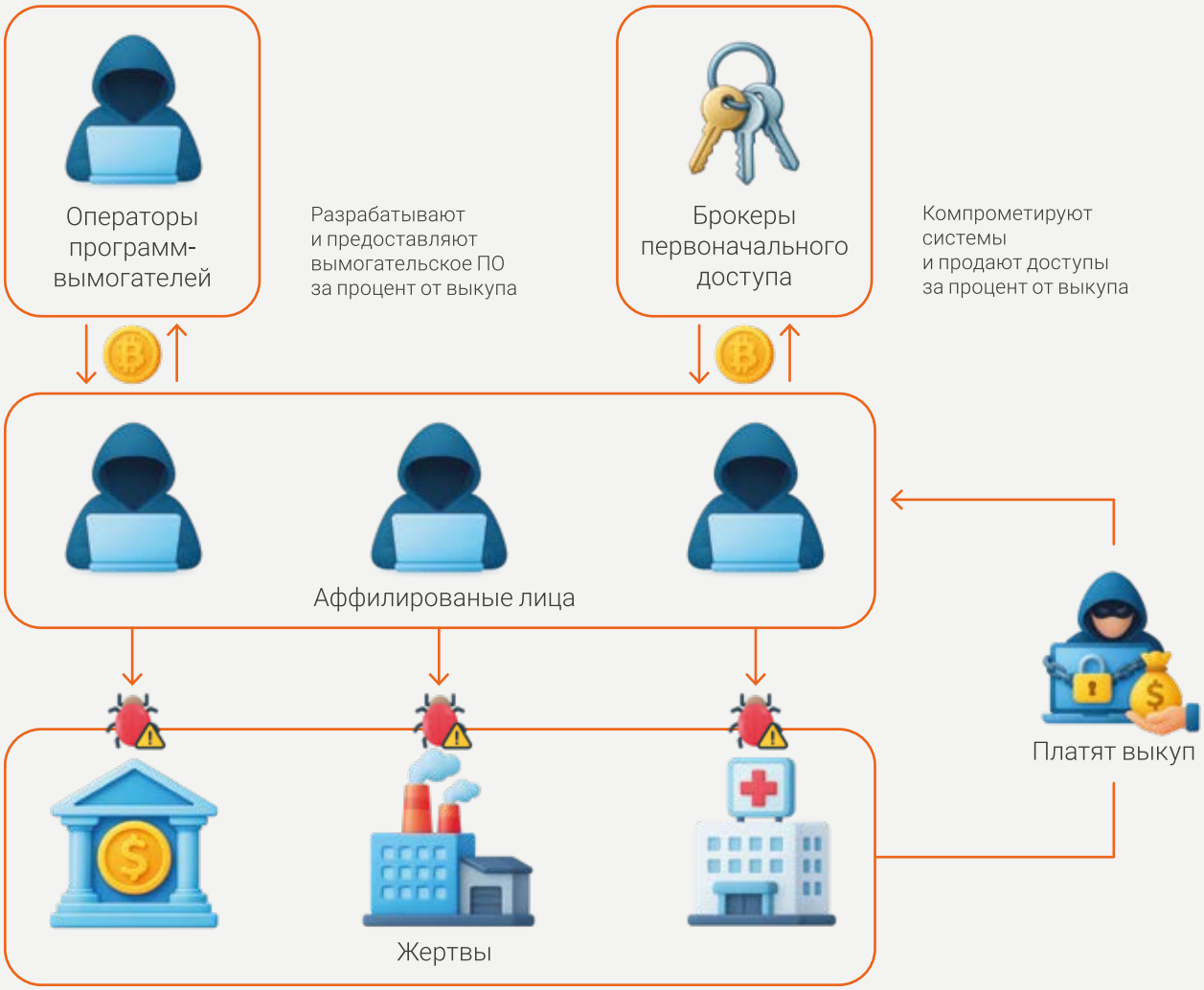
Организованная преступность и RaaS

Сегодня атаки часто проводят организованные группировки (Organized Criminal Group, OCG), преследующие разные мотивы. Но, помимо членов той или иной группировки, в атаке косвенным образом задействованы множество других лиц.

Обычно выделяют 4 ведущие роли в организации и проведении атак с вымогательским ПО:
1. Операторы создают вымогательское ПО и сдают его в аренду.
2. Партнеры (аффилиаты) проводят атаки, делясь прибылью с операторами.
3. Брокеры доступа (Initial Access Brokers, IABs) взламывают корпоративные сети и продают к ним доступ.
4. Поставщики криптовалютных услуг и дропперы помогают отмывать деньги и обналичивать выкуп.

Бизнес-модель взаимодействия между операторами ВПО и аффилированными лицами называется Ransomware-as-a-Service. Данная модель работает по схеме легального сервиса, у которого существуют различные варианты подписок (единовременная выплата, выплата процента от выкупа, ежемесячная подписка). Кроме аренды ВПО, аффилиатам могут предлагаться услуги шантажа жертвы, проведения переговоров с организациями-жертвами, покупки доступа к организации с последующей атакой на нее.

Роли злоумышленников в атаках с вымогательским ПО



Помимо RaaS, злоумышленники часто используют утекшее в открытый доступ ВПО (например, LockBit или Babuk), что позволяет даже неопытным хакерам реализовывать атаки без навыков разработки.

Почему RaaS выгодно?

- RaaS делает киберпреступность устойчивой — арест операторов не останавливает атаки аффилиатов.
- Аффилиаты получают готовые инструменты и профессиональную поддержку.
- У злоумышленников появляется возможность быстро выйти на рынок киберпреступности, не обладая глубокими техническими навыками.
- Жертвам сложнее противостоять хорошо организованным атакам.

Кибервымогательство эволюционировало в полноценную индустрию с чертами сложной экосистемы, где каждый участник играет специализированную роль. Борьба с ней требует не только технологической защиты, но и международного сотрудничества.

КАК РАБОТАЮТ ПРОГРАММЫ-ВЫМОГАТЕЛИ

Злоумышленники-вымогатели используют разные способы проникновения в систему жертвы.
В контексте атак вида «Spray and Pray» чаще всего используются:

- Пиратское ПО — нелицензионные программы могут содержать вирусы.
- Поддельные сайты — мошенники создают фальшивые страницы, продвигают их через рекламу или манипулируют поисковой выдачей.

В случае целевых атак топ векторов первоначального доступа состоит из таких методов, как:

- Целевой фишинг – почтовые рассылки содержат вредоносные вложения или фишинговые ссылки, предназначенные специально для атакуемой компании и направленные на конкретных сотрудников.
- Эксплуатация уязвимостей публично доступных служб и приложений – использование незакрытых уязвимостей в VPN, RDP, веб-интерфейсах и другом ПО, доступном из Интернета.
- Эксплуатация скомпрометированных легитимных учетных данных при подключении через публично доступные RDP-серверы – скомпрометированные доступы могут быть куплены злоумышленниками у брокеров первоначального доступа. Для компрометации учетных данных применяется брутфорс, но также используются стилеры и трояны-загрузчики.

Кроме того, злоумышленники часто используют метод «Trusted Relationship», чтобы получить доступ к целевой организации через компрометацию ее доверенных партнеров.

Методы получения первоначального доступа

Брокеры доступа

Организованные группировки (атакующие)

Основные методы и инстументы

Эксплуатация уязвимостей

Получение легитимных учетных записей

Использование вредоностного ПО

Брутфорс учетных записей для удаленного доступа

Стилеры

Трояны-загрузчики

Способы распространения ВПО

Фишинговые рассылки

Нелицензионное ПО

Отравление поисковой выдачи

ЧТО ПРОИСХОДИТ ПОСЛЕ ПОЛУЧЕНИЯ ПЕРВОНАЧАЛЬНОГО ДОСТУПА?

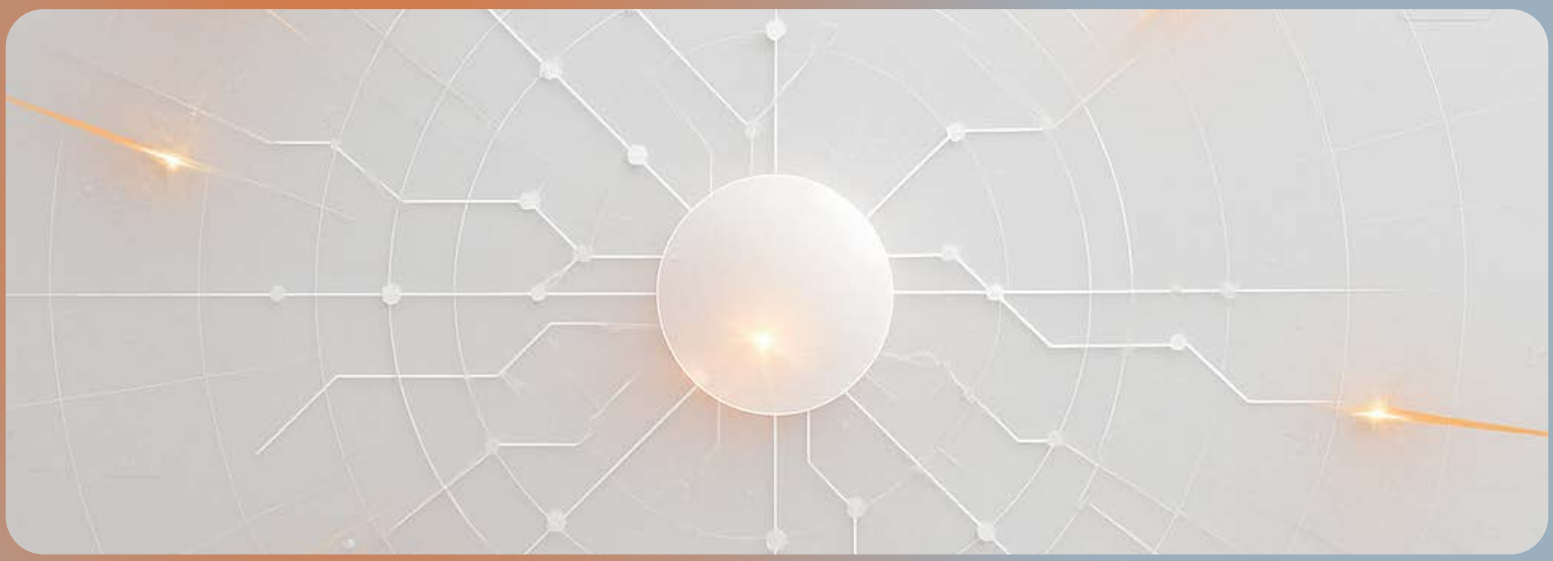
После получения доступа злоумышленники готовятся к развертыванию программы-вымогателя:

- Исследуют скомпрометированную инфраструктуру – сканируют сеть, ищут ценные данные и точки для дальнейшего продвижения.
- Повышают свои привилегии – используют уязвимости или украденные учетные данные для получения прав администратора.
- Продвигаются по сети горизонтально с целью дотянуться до всех критичных систем.
- Создают резервные каналы доступа – добавляют скрытые учетные записи, бэкдоры или туннели для сохранения контроля.
- Отключают средства защиты – останавливают антивирусы, удаляют резервные копии и блокируют системы мониторинга.
- Подготавливают данные к эксфильтрации и воруют ценную информацию.

Затем запускается вирус-вымогатель:

- Блокировщик – делает систему недоступной, показывая баннер с требованием выкупа.
- Шифровальщик – шифрует файлы, добавляя к ним специфичные расширения (например, .locked, .crypt, .abc).

Вирус может удалять резервные копии, чтобы препятствовать восстановлению данных

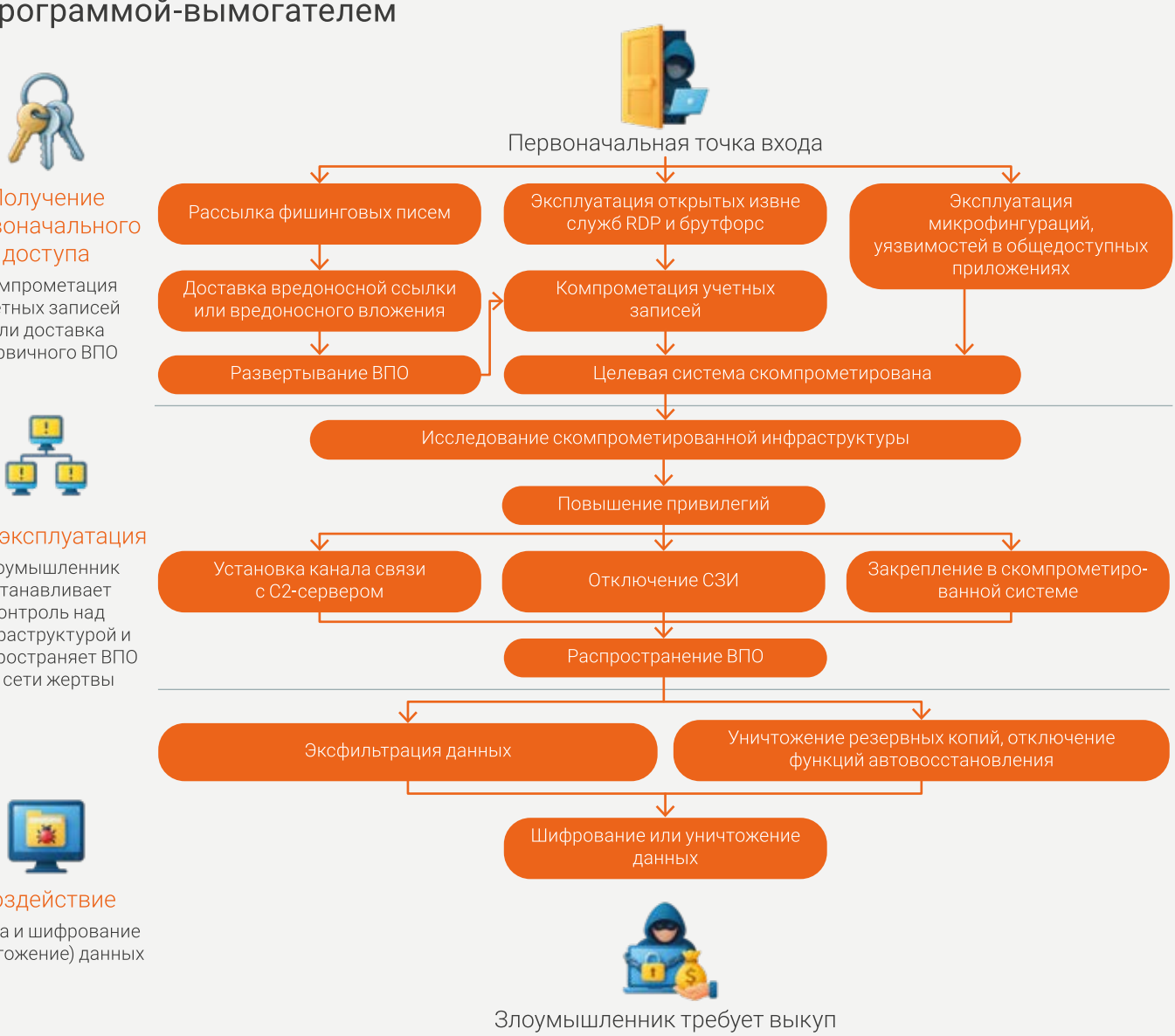


КОГДА ЖЕРТВА УЗНАЕТ ОБ АТАКЕ?

Обычно пользователи замечают проблему слишком поздно – когда файлы уже зашифрованы или система заблокирована.

На схеме ниже показан упрощенный процесс заражения. Для более детального изучения атак можно обратиться к Unified Ransomware Kill Chain и ознакомиться с отдельными TTP's из MITRE ATT&CK.

Схема цепочки действий злоумышленника во время атаки с программой-вымогателем



КТО АТАКУЕТ

Большинство атак с использованием программ-вымогателей проводят финансово мотивированные преступные группировки. Их главная цель — деньги.

Кого выбирают злоумышленники?

Идеальная жертва — организация, которая может заплатить крупный выкуп. Например, в 2024 году для бизнеса разных размеров требования о выкупе составляли:

- Малый бизнес: выкуп от 100 тыс. до 5 млн рублей.
- Средний и крупный бизнес: выкуп от 5 млн до 321 млн рублей.

Но размер компании и ее бюджеты — не главный критерий. Для злоумышленников очень важны существующие возможности получить доступ к инфраструктуре организации.

Политически мотивированные атаки. В последние годы таких атак становится больше. Их цель — не деньги, а шпионаж или диверсии.

Кибершпионаж

Проводят группировки, связанные с государствами. Их мишени:

- Правительственные учреждения.
- Критическая инфраструктура.
- Военные и оборонные объекты.
- Наукоемкие компании.

Подобные атаки совершаются APT-группировками (Advanced Persistent Threat). Такие атаки:

- Включают в себя несколько этапов и совершаются с применением продвинутого технического инструментария, также называемого «APT».
- Продолжительные (злоумышленники остаются незамеченными в сети месяцами).
- Хорошо финансируются.
- Являются постоянной угрозой, которой сложно противостоять и которую сложно полностью устранить.

2 Диверсии и хактивизм

Хактивисты атакуют, чтобы:

- Украсть данные.
- Нарушить работу важных и критичных организаций и подорвать их авторитет.
- Дестабилизировать ситуацию в стране.

Их отличие от обычных киберпреступников — желание создать резонанс, а не заработать, но тем не менее их мотивация может быть смешанной. Хактивисты зачастую не являются «профессиональными хакерами», используют публично доступные вредоносные инструменты, в отличие от кибершпионов, но, тем не менее, их атаки могут быть разрушительными.

В настоящее время в регионе стран СНГ и в России наиболее активно действуют хактивисткие группировки, среди них примерно 7% шифруют данные жертв (по данным Positive Technologies).

Почему хактивисты опасны?

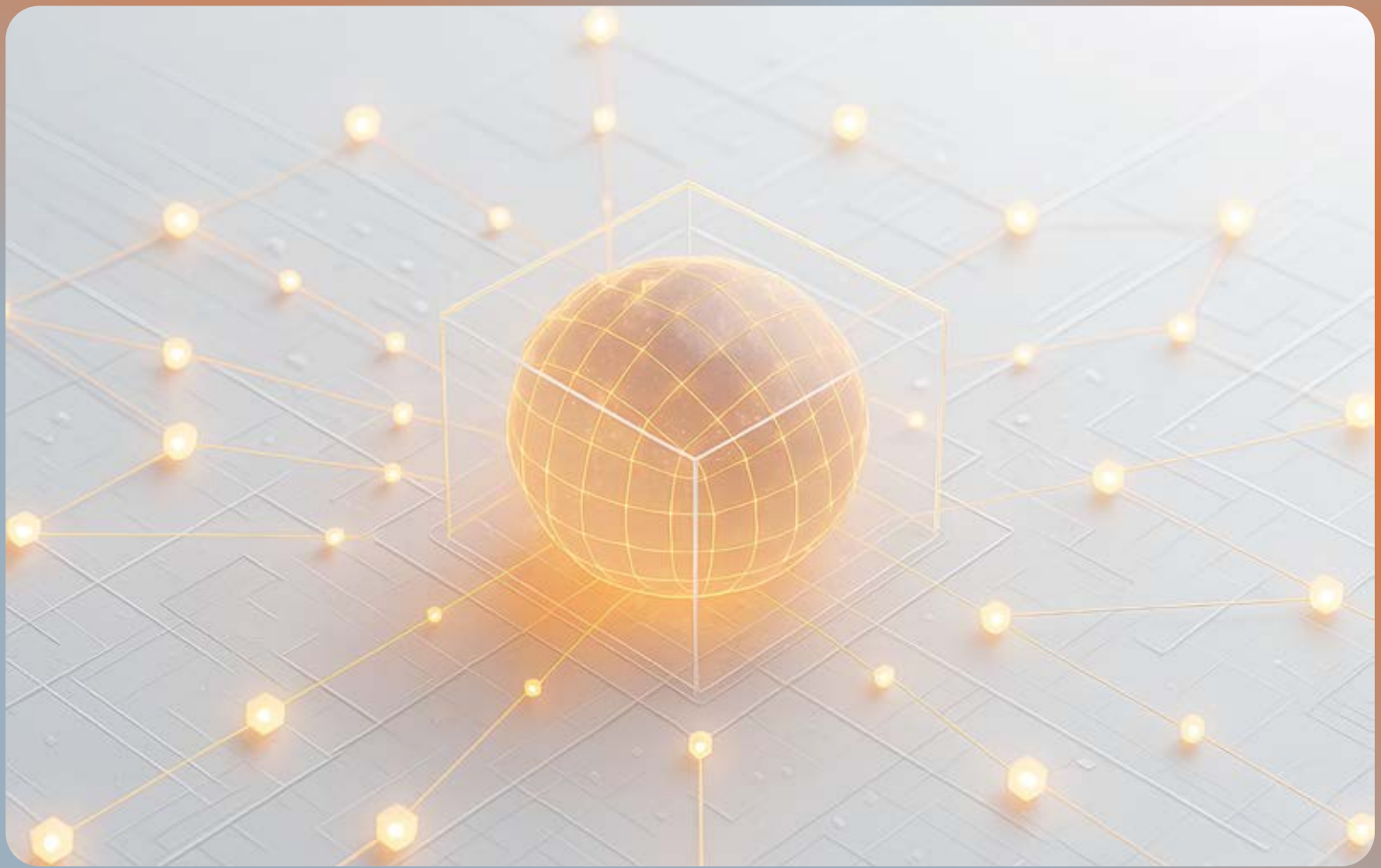
- Часто полностью уничтожают данные (без возможности восстановления даже за выкуп).
- Объединяются в альянсы, тем самым масштабируют свои атаки.

МНОГОФАКТОРНЫЙ ШАНТАЖ: КАК ПРЕСТУПНИКИ ВЫМОГАЮТ ДЕНЬГИ

Киберпреступники-вымогатели следуют одной и той же схеме: шифруют файлы взломанных организаций и требуют выкуп в обмен на восстановление доступа.

Однако многие компании отказываются платить, особенно если у них есть резервные копии данных.

Чтобы усилить давление, преступники стали применять многофакторный шантаж (в зарубежных источниках — multi-extortion). Теперь они угрожают не только потерей данных, но и утечкой конфиденциальной информации, DDoS-атаками на сервисы компании, шантажом клиентов и партнеров.



ОСНОВНЫЕ ЦЕЛИ ДЛЯ ЭКСФИЛЬТРАЦИИ

Защищенная медицинская информация (Protected Health Information)

Любые сведения, связанные со здоровьем того или иного пациента, проводимым лечением или оплатой медицинских услуг и позволяющие однозначно идентифицировать пациента. К PHI относятся: медицинские карты и истории болезни, поставленные диагнозы и результаты обследований, номера страховых полисов, данные о платежах за медицинские услуги, иная персональная информация, относящаяся к оказанию медпомощи.

Персональные данные (Personally Identifiable Information)

Любая информация, прямо или косвенно относящаяся к определенному лицу, позволяющая однозначно идентифицировать его, например, ФИО человека, адрес регистрации, сведения о семейном, социальном и имущественном положении, номера социального страхования (Social Security number) и др.

Учетные данные (Account Credentials)

Уникальные идентификаторы, такие как имя пользователя и пароль, которые позволяют пользователю подтвердить свою личность и авторизоваться в той или иной системе. Учетные данные представляют особую ценность для киберпреступников, так как позволяют получить несанкционированный доступ к корпоративным системам, осуществлять горизонтальное перемещение по сети, повысить привилегии в системе. Особую опасность представляет компрометация учетных данных администраторов и привилегированных пользователей.

Интеллектуальная собственность (Intellectual property)

Уникальные активы, представляющие коммерческую ценность для организации.

РАЗБЕРЕМ СХЕМЫ ВЫМОГАТЕЛЬСТВА

1 Простое вымогательство

Классическая схема: криптовирус шифрует файлы, а злоумышленники требуют деньги за дешифратор.

2 Двойное вымогательство

Преступники не только шифруют данные, но и угрожают их утечкой в открытый доступ. Перед этапом развертывания вируса-вымогателя атакующие собирают и перемещают конфиденциальные данные в собственные хранилища. Жертва шантажируется угрозами публикации информации на открытых теневых ресурсах злоумышленников – их сайтах утечек (Data Leak Site, DLS).

Первыми такой метод использовали хакерские группировки Maze и DoppelPaymer.

Какие данные чаще всего крадут?

- Учетные данные.
- Персональные данные клиентов и сотрудников.
- Коммерческая тайна.
- Защищенная медицинская информация (PHI, Protected Health Information).

3 Тройное вымогательство

Если компания не заплатит выкуп, злоумышленники могут атаковать ее сервисы с целью нарушить их доступность, то есть организовать DDoS-атаки. Такое воздействие влечет финансовые потери и удар по репутации компании-жертвы. Подобный подход применяли операторы AvosLocker.

Четырехфакторное вымогательство

Чтобы увеличить давление на жертву, в ход идет шантаж партнеров и клиентов компании-жертвы. Преступники:

- Рассылают информацию об утечке;
- Требуют выкуп уже не только от компании, но и от ее контрагентов.

Так действовали группы REvil и AvosLocker.

Многофакторное вымогательство

Многофакторное вымогательство делает атаки более опасными, поскольку злоумышленники используют комбинацию различных методов давления на жертву, чтобы увеличить вероятность выплаты выкупа. Компаниям необходимо совершенствовать защитные меры, регулярно делать бэкапы и готовить план реагирования на случай атаки.

СТОИТ ЛИ ПЛАТИТЬ ВЫКУП?

Если вашу организацию атаковали программы-вымогатели, перед вами встает сложный выбор: платить или не платить выкуп. Мы не рекомендуем платить преступникам, и вот почему.

Нет гарантии восстановления данных

Даже если вы заплатите, злоумышленники могут:

- Не расшифровать файлы (например, если на самом деле использовался вредонос-вайпер).
- Прислать нерабочий дешифратор.

По данным Veeam 2024 Ransomware Trends Report, каждая третья организация не смогла восстановить данные после выплаты требуемой суммы.

Риск повторных атак

Даже если файлы удастся восстановить, преступники могут:

- Потребовать новый выкуп за «предоставление гарантии» неразглашения украденной информации.
- Атаковать снова.

Компания, согласившаяся платить выкуп, должна осознавать, что с выплатой денег злоумышленникам состояние безопасности не улучшится.

Платя выкуп, вы финансируете преступников

Каждая выплата поддерживает киберпреступность:

- Разрабатывается новое вредоносное ПО, развивается инфраструктура злоумышленников.
- Совершенствуются старые методы атак.
- Преступники становятся сильнее.

Лучше вложиться в защиту данных, чем финансировать киберпреступность.

ПОЧЕМУ ВЫПЛАТА ВЫКУПА — НЕ РЕШЕНИЕ

Отсутствие гарантий

Нельзя гарантировать корректную работу дешифратора и верить в добропорядочность злоумышленников.

Финансирование преступности

Большая часть группировок кибервымогателей живет за счет средств, полученных от успешных атак.

Бреши в безопасности останутся

Злоумышленники смогут вернуться и атаковать организацию снова, если не будут приняты меры по улучшению состояния ИБ.

Мультифакторное вымогательство

Злоумышленники могут потребовать дополнительный выкуп по схеме мультифакторного вымогательства.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ВСЕ ЖЕ РЕШИЛИ ПЛАТИТЬ?

01 Привлеките экспертов для переговоров с злоумышленниками.

02 Потребуйте доказательства работоспособности дешифратора перед оплатой.

03 Расследуйте атаку, чтобы определить причинно-следственные связи и понять слабые места в инфраструктуре.

Помните: выплата выкупа не устраняет угрозу, а только поощряет злоумышленников. Надежная защита основана на совершенствовании превентивных мер, а не на финансировании киберпреступников.

Как происходит выплата выкупа

После успешной ransomware-атаки жертва остается с зашифрованными данными и запиской о выкупе. В ней указаны сумма выкупа, срок оплаты, контакты для связи.

ПОЧЕМУ ПРЕСТУПНИКИ ТРЕБУЮТ КРИПТОВАЛЮТУ?

Криптовалюта обеспечивает анонимность:

- Переводы проходят без участия банков — напрямую между криптокошельками.
- Транзакции записываются в блокчейн, но связаны только с адресами кошельков, а не с личными данными злоумышленников.

Все эти факторы усложняют отслеживание злоумышленников.

КАК УСТРОЕН ПРОЦЕСС ВЫПЛАТЫ ВЫКУПА?

01

ПЕРЕГОВОРЫ

Жертва или привлеченные эксперты связываются с преступниками и могут попытаться договориться о снижении требуемой суммы.

02

ПОКУПКА КРИПТОВАЛЮТЫ

Фиатную валюту (рубли, доллары и т.д.) обменивают на нужную криптовалюту через обменник или биржу.

03

ПЕРЕВОД ВЫКУПА

- Криптовалюта отправляется на указанный злоумышленниками адрес.

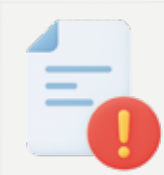
Это может быть:

- Анонимный кошелек (не требует идентификации).
- Счет на зарубежной криптовалютной платформе, которая не сотрудничает с правоохранительными органами страны жертвы.

Для каждой атаки преступники часто используют новый кошелек, чтобы скрыть следы.

Процесс выплаты выкупа

Вирус-вымогатель поразил компьютер жертву



В записке о выкупе приведены требования и инструкции по выплате выкупа

Компания-жертва совместно со специалистами по реагированию на инциденты может вступить в переговоры со злоумышленниками

Подготовка к выплате выкупа. Жертва осуществляет обмен фиатной валюты на криптовалюту

Жертва осуществляет перевод средств на указанный злоумышленниками адрес криптокошелька

Злоумышленники легализуют полученный доход, используя различные методы

Жертва получает ключ-дешифратор

КАК ЗЛОУМЫШЛЕННИКИ ЛЕГАЛИЗУЮТ СВОЙ ДОХОД?

Чтобы легализовать доходы и скрыть их преступное происхождение, злоумышленники применяют разные методы:

- Peeling Chain — переводы через множество кошельков, чтобы запутать цепочку.
- Криптомиксеры — сервисы, смешивающие транзакции разных пользователей.
- Chain Hopping — обмен одной криптовалюты на другую через разные блокчейны.
- «Денежные мулы» — перевод через подставные лица, которые выводят криптовалюту в фиат и передают сумму злоумышленникам.

Эти методы помогают преступникам оставаться в тени и затрудняют отслеживание и возврат украденных средств.

ЭТАПЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Сдерживание

Цель: остановить распространение угрозы и минимизировать ущерб.

- Документируйте все действия и применяемые меры.
- Выявите зараженные устройства и изолируйте их от сети.
- Настройте сеть так, чтобы предотвратить дальнейшее заражение, сохранив работоспособность систем.

Уведомление

Кого оповестить?

Провайдер MSS (если есть):

- Отправьте данные о вредоносном ПО (скриншоты, хэши файлов, логи).
- Укажите, как обнаружили заражение, количество и тип пораженных систем.

НКЦКИ (для организаций КИИ):

- Сообщите об инциденте в течение 3 часов (для значимых объектов) или 24 часов (для остальных).

Роскомнадзор (если затронуты персональные данные):

- Первое уведомление об обнаружении инцидента ИБ — в течение 24 часов.
- Результаты расследования — в течение 72 часов.

ФинЦЕРТ (для кредитно-финансовых учреждений):

- Первое уведомление об обнаружении инцидента ИБ — в течение 3 часов.
- Результаты расследования — в течение 30 дней.

Правоохранительные органы.

Изоляция

Как изолировать зараженные системы?

- Изолируйте скомпрометированные системы от корпоративной сети (на всех интерфейсах: проводных, Wi-Fi или мобильных).
- Не выключайте компьютеры! Оставьте их включенными или переведите в спящий режим/режим гибернации.
- Пораженные виртуальные машины переведите в режим «Suspend».
- Отключите общие ресурсы (Admin$, C$, IPC$), сетевые диски, внешние накопители.
- Ограничьте доступ через ресурсы удаленного доступа, такие как VPN, RDP, SSO.
- Изолируйте серверы хранения резервных копий, сетевые хранилища от зараженной сети.
- При использовании облачных хранилищ отключите синхронизацию с локальными устройствами.

Важно: бесфайловые вредоносные программы размещаются в оперативной памяти — выключение пораженного хоста уничтожит следы атаки! Также из-за выключения или перезагрузки системы могут быть утеряны многие другие криминалистические артефакты.

Обнаружение, анализ, блокировка

- Заблокируйте скомпрометированные учетные записи.
- Сбросьте пароли административных и системных аккаунтов (включая KRBTGT).
- Приостановите автоматическую ротацию журналов.
- Удалите права на запись для процессов или учетных записей, связанных с вредоносным ПО.
- Проверьте работу двухфакторной аутентификации (2FA).
- Заблокируйте обмен данными с потенциально зараженными организациями-партнерами.
- Определите конкретный вариант программы-вымогателя и изучите рекомендации по нему (например, через ID Ransomware).
- Не используйте скомпрометированные средства связи (почта, мессенджеры).

Сбор криминалистических данных

Передайте провайдеру MSS индикаторы компрометации (подозрительные IP-адреса, домены, URL).

Сохраните ключевые артефакты:

- Файлы журналов ОС и встроенных средств защиты.
- Дампы оперативной памяти.
- Кусты реестра Windows: SAM, SECURITY, SOFTWARE, SYSTEM (в том числе раздел AppCompatCache), а также артефакты NTUSER.DAT, Amcache.hve.
- Ярлыки (LNK) и временные файлы (Prefetch).
- Данные браузеров (кэш, расширения).

Если нет своих специалистов — обратитесь к экспертам по цифровой криминалистике.

2 Ликвидация угрозы

Цель: привести скомпрометированную ИС в первоначальное состояние, в котором она функционировала до атаки. Когда начинать? Только после полного понимания масштабов атаки и сбора всех криминалистических артефактов!

Варианты ликвидации угрозы на конечных точках

01 Полная переустановка ОС – надежно, но данные будут потеряны.

02 Ручное удаление вредоносного ПО и его компонентов – сохраняет данные, но требует экспертизы и не гарантирует полного устранения угрозы.

Что делать:

- Удалите вредоносные файлы (проверьте директории %ALLUSERSPROFILE%, %APPDATA%, %SYSTEMDRIVE% и временные папки).
- Проведите аудит запланированных задач на хосте.
- Проверьте каталоги автозагрузки Windows.
- Удалите подозрительные службы, установленные на хосте.
- Проверьте ветки реестра, отвечающие за автозапуск ПО.
- Обновите антивирусные базы.
- Проведите аудит групповых политик и удалите подозрительные.
- Проведите аудит доменных и локальных УЗ.
- Проведите аудит доменных групп безопасности с административными правами.
- Проведите аудит доверительных отношений (трастов) в домене и удалите подозрительные.
- Устраните уязвимости, которые были проэксплуатированы.

Восстановление

Цель: обеспечить безопасное возвращение к нормальной работе без риска повторного заражения.

Что делать?

- На контроллерах домена корректно настройте входящую и исходящую репликацию, чтобы предотвратить повторное заражение системы.
- Восстановите системы из предварительно проверенных резервных копий.
- Не подключайте непроверенные на ВПО устройства к восстанавливаемой инфраструктуре!
- Мониторьте сеть и конечные точки на предмет подозрительной активности.

Если нет бэкапов:

- Попробуйте найти дешифратор (например, на No More Ransom).
- Не платите выкуп — это финансирует киберпреступность и не гарантирует восстановление данных!

4 Анализ и улучшение

После ликвидации инцидента

01 Оцените эффективность работы команды реагирования и сделайте выводы.

02 Улучшите процессы, касающиеся мониторинга и реагирования, резервного копирования и хранения резервных копий, обучения сотрудников.

03 Внедрите современные средства защиты для мониторинга и анализа угроз, автоматизации реагирования, защиты конечных точек и сети, управления уязвимостями и доступом.

Главное:

- Не поддавайтесь панике — следуйте плану реагирования на инциденты ИБ.
- Документируйте каждый шаг — это поможет в расследовании и защите от будущих атак.

КАК НЕ ДОПУСТИТЬ ЗАРАЖЕНИЯ

Программы-вымогатели чаще всего проникают в систему следующими способами:

01 Через компрометацию доступа по RDP и другие внешние удаленные службы.

02 Через фишинговые письма.

03 Через эксплуатацию уязвимостей в публичных приложениях.

04 Через компрометацию третьей доверенной стороны (Trusted Relationship).

РАЗБЕРЕМ, КАК ЗАЩИТИТЬСЯ ОТ КАЖДОГО ИЗ ЭТИХ МЕТОДОВ

1 Защита от компрометации

Через уязвимости в публично доступных приложениях:

- Регулярно проверяйте сеть на уязвимости, особенно устройства, доступные из Интернета.
- Обновляйте ПО и ОС — устанавливайте все патчи безопасности.
- Отключите неиспользуемые сервисы и порты для доступа извне.
- Для защиты веб-приложений внедрите WAF (Web Application Firewall).

Через внешние удаленные службы:

- Настройте безопасность устройств – отключите неиспользуемые порты для внешнего доступа (например, RDP — порт 3389).
- Контролируйте установку и использование легитимных программ для организации удаленного доступа и администрирования (AnyDesk, TeamViewer, VNC, Ассистент и т.д.).
- Используйте многофакторную аутентификацию (MFA) для удаленного доступа.
- Настройте строгую парольную политику.
- Защититесь от брутфорс-атак на RDP — настройте блокировку учетных записей после нескольких неудачных попыток входа.

Защита от фишинга

- Обучайте сотрудников основам кибербезопасности. Многие компании предоставляют услуги по повышению осведомленности сотрудников.
- Отключите макросы в документах, скачанных из Интернета или почты.
- Открывайте подозрительные файлы в защищенном режиме.
- Не скачивайте почтовые вложения и не переходите по ссылкам в письмах от подозрительных отправителей, особенно если письмо содержит призывы к срочным действиям или запугивающее содержание.
- Используйте Secure Email Gateway — систему фильтрации писем, которая блокирует вредоносные вложения.

Общие рекомендации

- Резервное копирование. Используйте правило 3-2-1: 3 копии данных, на 2 разных носителях, 1 копия — вне корпоративной сети.
- Включите Volume Shadow Copy (VSS) для восстановления файлов после атаки и минимизации негативных последствий.
- Контроль доступа:
  1. Применяйте принцип минимальных привилегий — доступ только к необходимым ресурсам.
  2. Регулярно проверяйте группы безопасности в домене. При штатном функционировании инфраструктуры AD группы Enterprise Admins, Schema Admins должны быть пустыми.
  3. Меняйте пароли: сложные пароли для всех учетных записей; ежегодная смена пароля для сервисной учетной записи krbtgt.
  4. Реализуйте многоуровневую модель доступа в доменной инфраструктуре (контроллеры домена, серверы, рабочие станции).
- Мониторинг и дополнительные меры:
  - Включите расширенное ведение логов (Windows Event Logging).
  - Рассмотрите внедрение EDR/XDR или SIEM для мониторинга и анализа угроз в сети и на конечных точках.
  - Организуйте контроль утечек данных, рассмотрите возможность внедрения DLP-системы.
  - Внедрите Windows LAPS для управления паролями локальных администраторов.
  - Ограничьте доступ к сетевым дискам.
  - Используйте File Server Resource Manager (FSRM) для блокировки работы шифровальщиков.
  - Запрещайте запуск ненадежных программ с помощью AppLocker, WDAC, Software Restriction Policies (SRP).

Следуя этим рекомендациям, вы значительно снизите риск заражения программами-вымогателями. Регулярно пересматривайте свои меры защиты, проводите аудит уязвимостей, обучайте сотрудников и тестируйте инфраструктуру на устойчивость к атакам.

Информацию подготовил Отдел анализа, мониторинга и реагирования