Инцидент с шифрованием данных

Как минимизировать последствия?

КОНСТАНТИН ТИТКОВ

28.02.2025

О чем пойдет речь?

ИТ-инфраструктуру взломали/зашифровали/удалили

- экстренные действия
- кто может помочь
- чем помочь
- что эффективно
- что делать после
- подозрение на взлом
- реагирование на инцидент
- как подготовиться

NB: Настоящие рекомендации предназначены для команд ИТ и ИБ СМБ (SMB) и разработаны в целях быстрого и эффективного реагирования на инцидент с привлечением внешней экспертной организации, и не адресованы экспертам DFIR (Digital Forensic and Incident Response) или SOC (Security Operations Center) крупных и крупнейших компаний, т.к. предполагается, что такие эксперты профессионалы в своем деле и руководствуются в своей работе промышленными тематическими рекомендациями и стандартами, малая часть из которых упоминается в настоящем докладе.

Краткий доклад на базе рекомендаций версии 0.4.7

Какие такие рекомендации?

Рекомендации составлены после пары обращений к автору в пятницу вечером знакомых сисадминов и позволили сэкономить много вечеров пятниц в дальнейшем

- Самое главное из знаний и опыта экспертов (10 стр)
- Можно:

  - запросить сами рекомендации (контакт на последнем слайде)

  - внести свой вклад: предложить их дополнить

  - фотографировать

Платить ли выкуп?

- Нет гарантий
- Второй выкуп «за удаление похищенных данных»
- «Мухи и мед»

- Придётся самостоятельно принять решение с учетом всех рисков и последствий…

Как это вообще могло произойти?

- VPN, RDP, SSH, OWA, Jira, Confluence, Gitlab, Sharepoint и т.д. - неисправленная уязвимость или подбор пароля
- Фишинг
- WEB-приложение - уязвимость
- Цепочка поставок
- Внутренний нарушитель
- И так далее…

Пятница и праздники

- Инцидент – это финал в цепочке событий, последний шаг
- Немедленно, быстро и эффективно (даже ночью)
- Готовность к инциденту
- Рассчитывайте на свои наработки и на дежурных сотрудников
- Возможность привлечь помощь – бесценна!

(и заметно затратна)

Экстренно …

- Заблокировать доступ к ДБО в банке
- Не выключать и не перезагружать зараженные узлы
- Отключить (физически вынуть Ethernet кабель) от ЛВС серверы с резервными копиями и важными данными
- «Снапшоты» текущего состояния, если виртуальные
- Проверить исходящий в сторону сети интернет сетевой трафик
- Провести DFIR (Digital Forensic and Incident Response / цифровая криминалистика и реагирование на инциденты)
- Обратиться в правоохранительные органы
- Кто главный? (лицо, обличенное полномочиями, и ответственный за коммуникации)
- Коммуникации только ВНЕ пораженной инфраструктуры
- Необходимость привлечения подрядчиков на реагирование и на восстановление ИТ-инфраструктуры
- Информировать клиентов и партнеров об инциденте (или нет)?
- Заглушка о «техническом сбое» на сайт
- Поддержать сотрудников, которые задействованы в ликвидации инцидента

Что такое DFIR, куда и как за ним обращаться?

Организация	Контактные данные
НКЦКИ (Национальный координационный центр по компьютерным инцидентам) под эгидой 8-го Центра ФСБ РФ	https://www.cert.gov.ru/abuse/
~~**Здесь могла быть Ваша реклама!**~~	

Первая коммуникация

- Выбор компании
- Оффлайн (с выездом) и онлайн (удаленно)?
- Дата и время выезда, адрес, ФИО и контакты (телефон) ответственного за встречу на месте
- Пропуска, парковка
- «Можно с коллегой?»
- «Можно с другом?»
- Гарантийные письма

И как это все будет?

- установочная встреча
- анализ скомпрометированных узлов
- поиск способа входа в инфраструктуру, всех пораженных узлов, закладок (RAT)
- анализ HDD и/или снятие с них копий с использованием блокираторов записи и так далее
- У 2-х экспертов DFIR режим работы 24/7: 8 часов эксперт работает в одиночку, 8 вдвоем с напарником, 8 на отдых
- Принимающая сторона обеспечивает аналогичный режим работы сотрудников ИТ и ИБ для эффективного взаимодействия
- Нужно быстрее – нужно больше экспертов DFIR (лучше обсудить желаемые сроки работ до выезда экспертов, а также их ставки)

Что приготовить к прибытию экспертов

- Рабочие места для экспертов (стол/стул/свет/электропитание)
- Чат ВНЕ корпоративного мессенджера с участием необходимых лиц (руководители ИТ и ИБ, представитель менеджмента, юрист, специалист службы маркетинга/PR)

Критически важна конфиденциальность чата

- «Режим тишины» во внутренней сети, включая: почту и приглашения на собрания, ТКС/ВКС, корпоративные мессенджеры, личные мессенджеры, если в них был осуществлен вход в корпоративной сети
- Предусмотреть синхронный режим работы сотрудников ИТ и ИБ с режимом работы экспертов DFIR
- Отмена отпусков, командировок, увольнений
- Компенсации за переработки

Шаги IR (1/6) Этап 1: Подготовка к будущему инциденту

Реализация политики хранения логов:

- *Настройка ведения журналов (логов) с достаточной детализацией*
- *Обеспечение безопасного хранения журналов (логов)*
- *Настройка длительности хранения журналов (логов)*

Физический доступ к содержимому каждого диска (HDD) с данными в компании с обеспечением возможности:

- *Взять диск в руки*
- *Расшифровать диск (если он зашифрован самой компанией в целях безопасности)*

Возможность доставать артефакты:

- *Сетевой доступ ко всем узлам*
- *Административные права для доступа ко всем узлам*
- *Хранение реквизитов доступа (паролей) для административного доступа ко всем узлам безопасным с точки зрения уничтожения образом (например на бумаге в противопожарном сейфе)*

Резерв оборудования, вычислительных мощностей и дискового пространства для временного или постоянного развертывания ИТ-инфраструктуры или ее части без отключения зараженных (взломанных) узлов, потребляющих ресурсы

Обеспечение удаленного хранения резервных копий и данных (согласно правилу резервного копирования «3-2-1»)

Шаги IR (2/6)
Этап 2: Идентификация того, что инцидент произошел

Вам необходимо знание того, куда смотреть, чтобы понять, что инцидент начался
Например:

- Источники Threat Intelligence фидов с данными о возможной подготовке атаки на вашу компанию (регистрация фишинговых доменов, объявления о покупке или продаже доступа в вашу сеть и т.д.)
- SIEM/SOC
- MDR
- Централизованный (!) EDR/XDR
- Централизованный (!) AV
- …
- Система ИТ-мониторинга для контроля работоспособности и выявления отключения средств защиты
- …
- Экран зашифрованного компьютера (если вы не озаботились пунктами выше)
- Телеграмм-каналы с данными о взломах и утечках (вы одним из первых прочтете про свою компанию по пути на работу, пока в офисе еще никого нет, но все уже зашифровано или удалено…)

Шаг 3/6 IR Этап 3: Изоляция выявленного пораженного злоумышленниками ИТ-парка оборудования

- НЕ отключать электропитание!
- НЕ перезагружать!
- Отключать от ЛВС:
  - Виртуальные машины - на уровне системы управления виртуализацией отправить в “down” сетевой интерфейс (все сетевые интерфейсы ВМ)
  - Физические машины - вынуть сетевой провод из сетевой карты (RJ45 или оптику) Или вынуть провод на свиче. Или погасить порт на свиче
  - Wi-Fi - погасить сетевой интерфейс в ОС
  - Или погасить Wi-Fi точку доступа
  - Или на точке доступа заблокировать узел по MAC (в случае уверенности что злоумышленник не имеет доступа к узлу по другим интерфейсам + сменить пароль Wi-Fi на случай автоматической смены MAC зловредной программой)

Шаги IR (4/6) Этап 4. Зачистка

- Удалить троянов/закладок/web-шелов/RAT и т.д.
- Установить **обновления безопасности** для устранения уязвимостей, включая новейшие обновления (*могут закрывать еще не опубликованные, но уже известные злоумышленникам уязвимости*)
- Установить и настроить **средства защиты** (*которые, как правило, отключаются или “портятся” злоумышленниками*)
- **Сменить пароли.** Включая все системные УЗ. Включая в домене. И локальные. И в СУБД. И в VPN. И в прикладе. И ключи SSH/SSL тоже. И сертификаты web-сервисов. И пароли и ключи в ДБО вашего банка. И в интернет – сервисах и кабинетах. **Вообще ВСЕ пароли сменить.**
- **Kerberos** - необходимо **сменить пароль дважды**.

Шаги IR (5 и 6)

Этап 5. Восстановление

- Восстановление из резервных копий
- Включение ранее отключенных сетевых интерфейсов

Этап 6. Уроки

- Отчет об инциденте и реагировании
- Рекомендации для исключения повторения инцидента -> план работ
- Все работает!

А это все долго?

- Анализ 2-х HDD – 1 день
- Небольшая организация в 100 - 200 узлов - 1 неделя работы 1-го эксперта
- Крупная организация в 1000 - 2000 узлов - 2 недели работы 2-х экспертов
- Огромная организация в 50 000 - 150 000 узлов - 2 месяца работы сводных команд

Можно онлайн?

- Сотрудники ИТ и ИБ заказчика собирают улики, логи и т.д., и направляют результаты для анализа экспертам, после изучения материалов экспертами процесс повторяется
- Онлайн IR по ставкам экспертов DFIR может быть на 20-30% дешевле, чем оффлайн + не требуется учитывать в оплате время на дорогу и командировочные расходы
- Однако, если на стороне заказчика работ НЕ будет слаженной, быстрой и экспертной работы, то суммарное время DFIR может оказаться больше, чем в случае оффлайн работы - DFIR может продлиться дольше и может в итоге оказаться даже дороже, чем оффлайн вариант

И это все? Нет, к сожалению…

- В ходе или после проведения DFIR и после согласования с юристами Вашей компании может быть принято решение осуществить обращение в правоохранительные органы. Для этого юрист пострадавшей компании уже в процессе DFIR готовит заявительные материалы. Можно обращаться в правоохранительные органы после получения отчета о DFIR, можно еще в процессе DFIR или даже до его начала - компания решает самостоятельно, отчет о DFIR может быть предоставлен в правоохранительные органы впоследствии, но крайне желательно до вынесения решения о возбуждении уголовного дела или об отказе от его возбуждения. Правоохранительные органы самостоятельно примут решение, возбуждать уголовное дело или нет, на основании представленной информации и собственных выводов. Поэтому, если компания хочет получить и представить в правоохранительные органы отчет экспертов DFIR для возбуждения уголовного дела, может быть целесообразно отложить подачу заявления в правоохранительные органы до получения отчета. С указанными материалами и доверенностью на представление интересов компании в правоохранительных органах юрист компании обращается, обычно, в РОВД/ОВД по месту регистрации компании (в случае компании федерального значения иногда может быть целесообразно обращение выше, например в ГУВД, или СК, или УБКП).
- При первом обращении юрист получит первую справку - талон-уведомление о том, что заявление принято. У талона будет уникальный в рамках даты номер (КУСП). Рекомендуем всегда обращаться в правоохранительные органы, в том числе потому, что без КУСП активный поиск злоумышленников с помощью отдельных мер может быть незаконен.
- В течение 30 дней после подачи заявления компания получит вторую справку о том, что следователь согласен с тем, что имело место преступление и возбуждено уголовное дело. Либо компания получит отказ (что довольно плохо для компании; причиной отказа может быть, например, не предоставление отчета об инциденте или иных необходимых доказательств, на основании которых можно возбудить уголовное дело и признать пострадавшую компанию потерпевшей стороной). Рассмотрим процесс взаимодействия со следствием немного подробнее.

И еще...

- Для возбуждения уголовного дела инцидент должен иметь признаки состава преступления, например:
  - Троян/шифровальщик/RAT - статья 273 УК РФ
  - Кража ПДн/логинов и паролей/фото - статья 272 УК.
  - DDOS - статья 274 УК.
  - Действия, направленные на неправомерное воздействие на критическую информационную инфраструктуру – статья 274.1 УК.
- Вы можете самостоятельно подготовить отчет о расследовании и реагировании для его направления в правоохранительные органы, но вам необходимо будет изложить в отчете все факты объективной стороны преступления, контрольные суммы файлов вредоносных программ, перечислить функциональные возможности выявленных вредоносных программ с указанием признаков, которые по вашему мнению можно отнести к вредоносному программному обеспечению (например такие как уничтожение или блокирование информации - см. ст. 273 УК РФ), необходимо быть готовым предоставить следствию сами вредоносные программы на флешке и так далее.
- Все, что указано в отчете, должно быть воспроизводимо, например должны быть указаны контрольные суммы, указание использованных программ с их версиями и так далее.
- Детальные требования к отчету (что должно в нем быть) можно найти в соответствующей методичке МВД, изданной МосУ МВД России имени В.Я. Кикотя.

И затем...

- В процессе рассмотрения заявления компании будет определен следователь, который будет вести дело. Следователь с постановлением на выемку обратится в компанию и предложит предоставить свидетельства инцидента в виде выемки, очно, под протокол и видеосъемку, после чего предоставленные свидетельства станут вещественными доказательствами в деле. Крайне важно, чтобы следователь после выемки признал пострадавшую компанию потерпевшей стороной и возбудил дело (пусть и против неустановленного пока круга лиц). В дальнейшем целесообразно чтобы данный вывод подтвердил суд. Для возмещения убытков целесообразно стремиться к тому, чтобы совершившие атаку лица были найдены и признаны виновными на основании вступившего в законную силу решения суда, а компания была признана потерпевшим в уголовном деле. Это позволит предъявить иск о возмещении причиненного преступлением вреда (ст. 42 Уголовно-процессуального кодекса РФ). При этом установление виновных в атаке лиц не снимает с компании и ее уполномоченных работников ответственность в случае нарушения ими правил защиты информации (например, правил эксплуатации критической информационной инфраструктуры).
- Пострадавшая компания может периодически обращаться к следователю с просьбой о доступе к уголовному делу (в отношении информации только своего юридического лица) для отслеживания прогресса.
- Дальнейшей задачей следствия является, если упростить, установить 3-е лицо (злоумышленника), подать его в розыск, задержать, направить дело в суд.
- Когда злоумышленник будет признан виновным потерпевшие смогут предъявить к нему претензии в суде.

А потом

В числе прочего **справка о признании компании потерпевшей** и о возбуждении уголовного дела **необходима для ряда государственных органов**, например для ФНС, если была утрачена или зашифрована бухгалтерия компании, так ФНС вполне может подать на компанию в суд за несвоевременное или неполное предоставление очередной бухгалтерской отчетности и соответствующая справка может помочь компании получить отсрочку в предоставлении отчетности.

Справка подтвердит в суде, что компания не сама удалила (скрывает) свою бухгалтерию

Это ещё не все проблемы… Утечка данных

- Возможно, еще до шифрования данных украли изрядную долю информации. Определить это часто можно по журналам сетевых средств защиты или статистике исходящего трафика в сторону сети интернет.
- У вас могут попросить выкуп за ее удаление злоумышленниками, но нет гарантий, что они это сделают, а если вы не платили выкуп за расшифрованные данных - то нет гарантий вдвойне.
- Поэтому ваши данные скорее всего будут проданы всем, готовым за них заплатить
- В украденных у вас данных могут быть:
  - Ключи и пароли от личных кабинетов во внешних сервисах, включая госучреждения, сервисы партнеров и т.д.
  - Персональные данные сотрудников и клиентов
  - Информация о вашей экономической деятельности, договорах и т.д.
  - Интеллектуальная собственность: разработанный программный код и т.д.
- Сменить ключи и пароли от личных кабинетов во внешних сервисах сразу после завершения DFIR
- В сервисах проверить состав операций и пользователей - т.к. злоумышленники могут создать дополнительные аккаунты для доступа к вашим личным кабинетам

А потом еще...

- Через какое-то время после продажи ваших данных (или если на них не найдется покупатель) данные вполне могут быть опубликованы в открытом доступе частично или целиком
- Вы можете столкнуться с обращениями клиентов и партнеров, а также правоохранительных органов. Если вы ранее не уведомили все необходимые правоохранительные органы, например, Роскомнадзор об утечке персональных данных, вам необходимо будет выполнить соответствующие мероприятия в установленные законом срок.
- В будущем могут быть опубликованы новые части ранее украденных у вас данных и выданы за новую утечку - необходимо быть готовыми проанализировать такие данные, чтобы либо подтвердить, что это старая утечка, либо снова проводить DFIR либо Compromise Assessment (CA).

Я все понял. А можно пройти профилактический осмотр?

Что делать, если у вас есть подозрение, что вашу ИТ-инфраструктуру взломали и могут зашифровать и уничтожить, но этого еще не произошло.

Что может быть таким основанием?

- Ощущение некорректной работы ИТ-инфраструктуры, например, ввиду происходящих в ней с административными правами изменений, не санкционированных вами
- Наличие уязвимого ПО или сервисов на внешнем (интернет) периметре, которые вы не устраняете оперативно.
- Отчет о тесте на проникновение с успешной компрометацией вашей компании.
- И многое другое…

В данной ситуации целесообразно:

- провести CA (Comromise Assessment) – поиск следов взлома
- проверить безопасность, целостность и доступность ваших бэкапов (резервных копий данных)
- рассмотреть рекомендации со следующего слайда

Прививка …. от вирусов

- Контакты сервисных компаний по реагированию на киберинциденты. Согласованный порядок взаимодействия, лимит согласованных расходов, полномочия у потенциальных подписанотов NDA и гарантийных писем для начала проведения DFIR. Шаблоны гарантийных писем и NDA, готовность крайне быстро внести в них изменения без длительного согласования.
- Проверку возможности выполнить все, указанное в Приложении № 1 выше, особенно указанное в составе Этапа 1.
- Правило резервного копирования «3-2-1» (три резервные копии на двух разных носителях, один из которых находится вне предприятия).
- Безопасность системы резервного копирования и бэкапов не должна зависеть от компрометации AD. Можно рассмотреть отдельные не доменные учетные записи для СРК или многофакторную аутентификацию.
- Запись паролей на бумажный носитель и размещение его в сейфе (либо размещение в сейфе носителя с зашифрованным файлом с паролями, который при необходимости может быть подключен в режиме read-only).
- Составление карты сети с указанием точек подключения к Интернет и узлов (сетей), взаимодействующих с интернет.
- Внедрение SIEM и построение на его базе SOC, либо подключение вашей ИТ-инфраструктуры к внешнему SOC.
- Внедрение MDR (как временное решение в отсутствие SOC или дополняющее SOC).
- Настройку правил аудита (журналирования, логирования) событий безопасности и глубины (длительность) хранения журналов.
- Безопасное хранение журналов аудита (недоступно для злоумышленников при взломе вашего AD или вне вашей инфраструктуры) – например внешний SOC или DataLake.
- Исключить подключение носителя с ключами ДБО (интернет-банка) к компьютеру кроме выполнения действия по подписанию документов. Да, это не так удобно, зато, когда бухгалтер отходит от компьютера злоумышленник не подпишет и не отправит несанкционированный платеж.
- Средства коммуникации между сотрудниками и с сервисной (DFIR) компанией при инциденте, исключающие чтение переписки злоумышленниками, то есть вне пораженной инфраструктуры.
- Ответственные за коммуникации при инциденте и шаблоны-заготовки (кому и о чем сообщить):
  - коммуникации с руководством, СД, акционерами;
  - коммуникации с техническим персоналом и сервисными компаниями;
  - коммуникации с работниками;
  - коммуникации с клиентами;
  - коммуникации с гос.органами.

И второй компонент прививки:

- Инструменты и методы для сетевой изоляции пораженных хостов, включая физические и виртуальные, пользовательские и серверы - как вы будет их отключать от сети? Сколько это займет времени? Кого и как предупредить об отключении узла с тем, что какой-то процесс остановился и что нельзя включить узел в вычислительную сеть обратно и нельзя отключать электропитание?
- Инструменты для отключения сети организации от сети интернет: полностью, а также частично: по “белому” списку проверенных адресов контрагентов, включая ведение таких списков, и, аналогично по “черному” списку (включающему известные файлообменники, ресурсы в иных странах, не связанных с клиентской базой, облачных провайдеров типа Amazon и т.п.).
- Средства выявления эксфильтрации и скачивания данных, или хотя бы выявления нестандартного большого исходящего в сеть интернет трафика.
- Инструменты анализа перечня запущенного ПО и его избирательной блокировки.
- Инструменты массового распространения, запуска и удаления нужных вам файлов и каталогов.
- Инструменты, дистрибутивы и экспортированные настройки для возможности развертывания пораженного узла из образа или с помощью дистрибутива.
- Запуск внешних вэб-сервисов и поддерживающих их СУБД и иных компонентов с помощью ограниченных (не административных) учетных записей в операционных системах и отсутствие уязвимостей, позволяющих осуществить повышения привилегий на таких узлах.
- Принудительное отключение PowerShell и WMI там, где они не используются.
- Принудительное отключение макросов MS Office там, где они не используются.
- Запрет внутри-vlan-ного входящего сетевого взаимодействия однотипных узлов, например, терминальных серверов или рабочих станций, кроме случаев, когда это не связано с задачами управления и нет возможности вынести узел управления в отдельный сегмент.
- Запрет ICMP, для исключения передачи данных с помощью ICMP-тунеллей внутри вашей сет ии в сеть Интернет.
- Мониторинг исходящих рекурсивных DNS-запросов для выявления DNS-туннелей с помощью или отдельных сервисов защиты DNS.
- Мониторинг отключения VolumeShadow Copy Service под Windows и отключения СЗИ либо изменения их конфигурации (в т.ч. внесения ВПО в исключения) для раннего обнаружения злоумышленников.
- Мониторинг источника авторизации административных доменных УЗ и даты смены krbtgt.
- Инвентаризацию узлов сети, проверку наличия на них средств защиты и мониторинг отключения таких СЗИ.
- Периодическое использование BloodHound/PingCastle для анализа безопасности AD.
- Наличие инструментов для обработки TI-фидов (включая ручной ввод), в том числе в части блокировки как входящих, так и исходящих подключений (обращений) с/ко внешним IP-адресам и доменам, загружаемых и размещенных на файловой системе файлов (имена и хеши).
- Подключение источника или источников TI-фидов.
- Двухфакторную аутентификациию, в первую очередь – для доступных из сети интернет сервисов, где скорее всего уже сейчас ведется подбор ваших паролей.

Что может сделать владелец бизнеса?

- Довести рекомендации до ИТ и ИБ служб компании
- Убедиться, что никто не стесняется сказать, что он не может что-то выполнить или у него чего-то нет
- Убедиться, что все подготовительные шаги выполнены
- Привлечь при инциденте все возможные ресурсы и не терять время, по возможности – вернуть технический персонал из отпуска и т.д.
- Ни в коем случае не увольнять и не наказывать работников в ходе ликвидации последствий инцидента, наоборот – поддерживать!

Помните, что демотивированный сотрудник меньше всего будет заинтересован в реагировании на инцидент, а сотрудник, который допустил (по своей вине или нет), но исправил ситуацию, для вашей компании лучше и ценнее нового!

Константин Титков

tg: @ktitkov