**ИНЦИДЕНТ: ШИФРОВАЛЬЩИК**

ПОДГОТОВКА

**Проверка коммуникаций:**

* Проверить четкое определение ролей и обязанностей технического персонала и других отделов во время реагирования на кибер-инциденты. Убедиться, что каждый участник понимает свои задачи и действия в случае возникновения инцидента.
* Определить критерии эскалации инцидента на уровень руководства. Установить четкий процесс передачи информации и ответственности при эскалации.
* Создать готовые формы сообщений об инциденте для пользователей, CERT и иных заинтересованных лиц

**Должен существовать и быть доступным список активов и их владельцев для следующих категорий:**

* Активы клиентов:
  + Владельцы
  + Контактные лица
* Активы компании (включая все филиалы и подразделения):
  + Владельцы
  + Контактные лица
  + Администраторы
* Инвентаризация инфраструктуры:
  + Конечные точки (компьютеры, ноутбуки, мобильные устройства)
  + Серверы
  + Сетевое оборудование
  + Системы безопасности, СЗИ
  + Диапазоны сети:
    - Публичная
    - Частная
    - VPN / Внеполосные данные
  + Сотрудники
  + Партнеры
  + Клиенты

**Обзор последних кибер-инцидентов и их результатов:**

* Проанализировать произошедшие инциденты безопасности для выявления слабых мест и улучшения реагирования.
* Извлечь уроки из прошлых инцидентов для более эффективного реагирования в будущем.

**Обзор угроз, новых рисков и уязвимостей:**

* Изучить актуальные угрозы в киберпространстве, нацеленные на вашу организацию, поставщиков и отрасль.
* Анализировать общие тенденции и новые типы атак, чтобы быть готовым к ним.
* Внедрить процессы threat intelligence

**Менеджмент рисков:**

* Определить возможность организации платить выкуп за расшифрование данных. Оценить максимально допустимую сумму выкупа и возможность реализовывать переводы через криптовалюту.
* Обрести ключи расшифрования для разных видов программ-вымогателей.
* Убедиться в страховом покрытии в сфере компьютерных инцидентов

**Обеспечение доступа к необходимой документации и информации, в том числе вне рабочего времени, к:**

* Плану реагирования на кибер-инциденты
* Схеме сетевой архитектуры
* Схеме потоков данных
* Ключевым документам, необходимым для реагирования на инциденты.

**Проведение регулярных кампаний для информирования сотрудников о рисках информационной безопасности, включая:**

* Фишинговые атаки / вредоносные электронные письма:
  + Обучить сотрудников распознавать признаки фишинговых писем и избегать нажатия на подозрительные ссылки или вложения.
  + Предоставить инструкции о том, как безопасно обрабатывать электронную почту.
  + Провести симуляцию фишинговой атаки.
* Программы-вымогатели:
  + Объяснить сотрудникам, что такое программы-вымогатели и как они могут нанести ущерб организации.
  + Предоставить рекомендации по предотвращению заражения вредоносным ПО и действий в случае атаки.
  + Провести симуляцию атаки вымогателя.
* Возможность сообщения о подозрении на киберинцидент:
  + Установить четкий процесс и каналы связи для сообщения о подозрительной активности, связанной с безопасностью.
  + Поощрять сотрудников сообщать о любых инцидентах, не опасаясь негативных последствий.

**Обеспечение регулярного обучения по безопасности для сотрудников, управляющих персональными, конфиденциальными или критическими данными и системами:**

* Обязательное прохождение специализированных тренингов по безопасности для сотрудников, которые работают с чувствительной информацией.
* Регулярное обновление знаний и навыков сотрудников в области защиты данных и реагирования на угрозы.
* Проводить тренировку отдела безопасности в части реагирования (например, киберучения)

**Подготовка инфраструктуры:**

* Пропатчить уязвимости информационных активов
* Провести плановые проверки средств управления и СЗИ
* Провести плановые проверки наличия и состояния резервных копий (+ что резервные копии не заражены ВПО).
* Проверить расшаренные директории на наличие открытых привилегий
* Обеспечить поддержку обновлений EDR/AV приложений
* Сегментировать сеть и логировать траффик между сегментами. Убедиться в возможности изоляции сегментов, регионов, партнеров или Интернета.
* Внедрить deception-систему.
* Уделить внимание анти-фишинговым решениям и мониторингу появления процессов PS, CMD, WMI, MSHTA и тд.
* Настроить SIEM-систему для выявления подозрительной активности и автоматического оповещения о потенциальных угрозах. Определить четкие критерии, по которым система будет генерировать оповещения.
* Автоматизировать процессы реагирования в SOAR/IRP
* Включить функцию «Показывать расширения файлов» в настройках на пользовательских хостах.

ВЫЯВЛЕНИЕ

**Анализ каналов выявления** **(автоматических и мануальных)**:

* Оповещения с AV/EDR, SIEM
* Обнаружения с почтовых фильтров (сообщения с подозрительными вложениями)
* Необычная активность на ПК, серверах или телефонах
* Сообщения от конечных пользователей (как правило, об искаженных или недоступных файлах)
* Появление необычных/потенциально вредоносных файловых расширений
* Необычный DNS-трафик
* Высокая скорость переименования/изменения файлов
* Скачки CPU в системах обмена файлами
* Необычные исполняемые бинарные файлы в пользовательской среде
* Аномальные сетевые соединения на хостах, сетевые подключения к известным CnC адресам
* Фаервол запрещает доступ к проверенным точкам обмена файлами
* Информация от deception-систем
* Использование TOR или I2P, истории поиска

**Срочное информирование о киберинциденте:**

* Проверить сообщения от СЗИ на факт ложного срабатывания (false positive)
* При подтверждении вредоносной активности шифровальщика, сообщить о ней через службу поддержки (Service Desk).
  + Если заявки еще не существует, создать новую с минимальной информацией.
* Подумать о том, чтобы уведомить и привлечь CERT к расследованию
* В установленные сроки уведомить ГосСОПКА/НКЦКИ/ФСБ при необходимости

**Определить, произошла ли утечка данных, и если да, то:**

* Обратиться к плейбуку по реагированию на утечки данных.
* Рассмотреть, целесообразно ли на данном этапе сообщать в РКН о подозреваемом или подтвержденном несанкционированном доступе к любым персональным данным.

**Классификация инцидента:**

* Оценить следующие данные о шифровальщике:
  + Всплывающие окна при открытии шифрованного файла, текстовые или html-файлы (как правило, всплывают сами после зашифрования)
  + Email для связи с атакующим
  + Язык всплывшего сообщения
  + Метод оплаты и реквизиты, валюта
  + Страница «поддержки»
  + Расширение/тип шифрованных файлов (.crypt, .cry, .locked, .abc., .xyz и т.д.)
  + Размещение зашифрованных файлов
  + Иконка зашифрованных файлов
* Загрузить зашифрованный файл в сервисы, *например*, Crypto Sheriff, ID Ransomware, ProvenData, noransom.kaspersky.com, nomoreransom.org. Там возможно определить тип (семейство) шифровальщика и даже получить приватные ключи.
* На основе имеющейся информации о потере данных и типах инцидентов классифицировать киберинцидент.

Если декриптор (ключ) не был получен:

**Подготовка к этапу анализа:**

* Мобилизовать группу реагирования на инциденты кибербезопасности (CIRT) для первоначального расследования кибер-инцидента. Определить вероятность широкомасштабного заражения программой-вымогателем.
* Собрать первоначальные данные об инциденте, включая как минимум следующее:
  + Тип кибер-инцидента;
  + Куда сообщили о кибер-инциденте;
  + Места появления сообщений о вымогательстве (физические и логические);
  + Количество пострадавших активов в организации (на начальном этапе) и увеличивается ли оно;
  + Идентификация вредоносного электронного письма, если оно есть;
  + Дополнительные отчеты, связанные с пострадавшими активами, включая журналы антивируса, системные журналы событий и журналы сетевого мониторинга;
  + Предварительная оценка воздействия на бизнес, критичность;
  + Любые текущие действия, предпринимаемые для устранения инцидента.
* Обеспечить сохранность артефактов, включая копии подозреваемого вредоносного ПО и криминалистические копии пострадавших систем для дальнейшего анализа.
* Оценить приоритет инцидента на основе первоначального расследования
* Оповестить руководство в соответствии с планом эскалации

АНАЛИЗ

**Анализ инцидента:**

* Убедиться, что привлечены все технические специалисты из групп реагирования.
* Определить область поражения:
  + Где появляются сообщения о вымогательстве? Проверить смежные системы на предмет заражения (в том же домене/сегменте/группе и тд). В системах проверить файлы/хэши, процессы, сетевые подключения, логи и т.д.
  + Выполнить поиск по:
    - SHA-1 имени процесса, который был запущен файлом;
    - Имени исполняемого файла;
    - URL-адресу или IP-адресу аналогичных подключений в сети.
  + Проанализировать исходное вредоносное электронное письмо или иную точку входа и масштабы его распространения.
  + Определить метод горизонтального распространения[[1]](#footnote-1):
    - WMI
    - PSExec
    - RDP, SMB
    - logon-скрипт на контроллере домена
    - Pass-the-ticket (Kerberos)
    - Другое
  + Определить, какие системы являются целью поражения:
    - Серверы (версия ОС, ядро)
    - Рабочие станции (версия ОС)
    - Базы данных
    - Сетевые диски
    - Сеть хранения данных (SAN)
    - Резервные копии
    - Иные системы
* Провести реверс-инжиниринг вредоносного ПО в безопасной среде для понимания его механизмов и реализуемых функций (статический анализ)
* Запустить вредоносное ПО в безопасной среде или песочнице, изолированной от корпоративной сети, чтобы определить его поведение на тестовой системе, включая созданные файлы, запущенные службы, измененные ключи реестра и сетевые коммуникации (динамический анализ)
* Проверить пораженную инфраструктуру на наличие индикаторов компрометации, полученных в ходе анализа вредоносного ПО, для выявления любых дополнительных скомпрометированных систем.
* Оценить угрозу при перезагрузке зараженного хоста
* Сохранить все доказательства для поддержки установления виновных или возможных судебных действий.

**Анализ вектора атаки:**

* Drive-by компрометация (вредоносный код на ненадежном веб-сайте. Когда пользователь посещает этот сайт, код автоматически загружается на его устройство. +Расширения в браузере, уязвимости в CMS, веб-серверах, открытых интерфейсах, JavaScript-снифферы)
* Пограничное сетевое оборудование
* Эксплуатация общедоступного приложения (уязвимость в общедоступном приложении, чтобы получить доступ к устройству пользователя)
* УЗ (доменные, локальные): брутфорс, слабый пароль, RCE
* Внешние удаленные службы (RDP, VNC, SSH…) а также VPN-точки подключения (непропатченные сетевые устройства, к которым подключаются)
* Подключаемое оборудование (подключение вредоносного устройства по физ. портам)
* Фишинг (почта, голосовой фишинг)
* Компрометация цепочки поставок (внедрение ВПО в легитимное программное обеспечение или аппаратное обеспечение до того, как оно попадет к пользователям)
* Доверительные отношения (кто-то из доверенных сотрудников передал чувствительную информацию злоумышленнику)

**Выявление и отчетность о потенциально скомпрометированных данных:**

* Определить любые данные, пострадавшие от атаки с использованием программы-вымогателя, включая данные в процессе передачи.
* Связаться с владельцами данных и руководством для понимания влияния скомпрометированных данных на бизнес.
* Определить могли ли конфиденциальность, целостность или доступность идентифицированных данных быть скомпрометированы.
* При рассмотрении юридических аспектов инцидента, следует задуматься о проведении полного судебно-криминалистического расследования. Все действия с доказательствами должны осуществляться в соответствии с руководством по надлежащей практике обращения с цифровыми доказательствами. Рассмотреть необходимость сообщения об инциденте в полицию.
* Рассмотреть требования к отчетности перед соответствующим регулирующим органом или компетентным органом, если таковые имеются.
* Информировать старших должностных лиц о любом подозреваемом или подтвержденном нарушении данных, включая несанкционированный доступ к личным или конфиденциальным данным организации.
* Группа реагирования на инциденты кибербезопасности (ГРИИБ) должна немедленно сообщить о любом подозреваемом или подтвержденном нарушении данных, включая утечку личных данных, соответствующим сторонам

**Разработка плана восстановления:**

* Готова ли наша компания платить выкуп?
  + Возможно ли страховое покрытие?
  + Многие злоумышленники готовы к переговорам и иногда понижают цену выкупа
* Совместно с техническими специалистами и руководством разработать приоритетный план восстановления. Нужно ли вмешательство сторонних организаций (вендоров, подрядчиков) в процесс реагирования?
* План должен учитывать:
  + Анализ технического аспекта инцидента.
  + Оценку влияния на бизнес.
* Реализовать коммуникационную стратегию в соответствии с планом восстановления.

СДЕРЖИВАНИЕ

**Локализация технических механизмов атаки с использованием программы-вымогателя (закрытие вектора атаки):**

* Минимизировать дальнейшую вредоносную активность:
  + Карантин зараженных систем и их отключение от сети, по возможности (отключение с помощью фаервола, отключение сетевого интерфейса, отключение свитч-порта на маршрутизаторе).
  + Применение контроля доступа устройств для изоляции от производственных сетей
  + Приостановка учетных записей пользователей/групп, подозреваемых во взломе, удаление нелегитимно созданных УЗ
  + Отключение от питания НЕ зараженных систем, по возможности. Зараженные системы НЕ выключать.
  + Отключение *всех* сетевых дисков
    - NET USE x:\\unc\path\/DELETE
  + Карантин резервных копий
  + Блокировать трафик к CnC
* Разработать меры защиты на основе анализа вредоносного кода:
  + Защитить инфраструктуру от конкретного вредоносного кода и других программ-вымогателей, которые могут использовать тот же механизм заражения.
* В случае атаки по электронной почте:
  + Блокировать отправителя и сообщение, пометив его как спам;
  + Блокировать IP-адрес, найдя его в заголовке электронного письма.
  + Напомнить пользователям перемещать подозрительные электронные письма в папку «Спам»
* В случае взлома веб-сайта:
  + Блокировать веб-сайт на сетевом периметре;
  + Использовать sinkhole[[2]](#footnote-2) для домена на внутренних DNS-серверах;
  + Блокировать IP-адрес сайта на межсетевом экране;
  + Убедиться, что все браузеры имеют последние обновления;
  + Оценить необходимость перехода пользователей на более новые/защищенные браузеры.
* Блокировать доступ к любым идентифицированным инструментам удаленного доступа (RAT), чтобы предотвратить связь с серверами CnC, веб-сайтами и эксплуатируемыми приложениями.
* Подключить EDR- или иных агентов на хостах, которые могут прекратить процесс заражения
* Обеспечить безопасное хранение копий вредоносного кода, зараженных систем и любых идентифицированных артефактов для дальнейшего расследования (при необходимости привлечь экспертов по компьютерной криминалистике).
* Информировать владельцев данных и заинтересованных лиц о ходе действий по локализации.
* Приостановить резервное копирование

УСТРАНЕНИЕ

**Устранение вредоносного воздействия с систем:**

* Определить методы удаления вредоносного ПО на основе результатов анализа вредоносного кода и информации от надежных источников.
* Выполнить автоматический или ручной процесс удаления для устранения вредоносного ПО или скомпрометированных исполняемых файлов с использованием соответствующих инструментов.
* Проверить резервные копии на наличие индикаторов компрометации (IOC), соответствующих профилю атаки, ДО восстановления систем.
* Переустановить отдельные системы с чистого резервного образа ОС, прежде чем обновлять их с помощью проверенных резервных копий данных.
* Восстановить пораженные сетевые системы из надежной резервной копии.

**Защита учетных записей:**

* Изменить данные всех скомпрометированных учетных записей.
* Очистка Active Directory
  + Дважды[[3]](#footnote-3) поменять пароль KBRTGT
  + Сбросить все привилегированные УЗ
  + В случае, если мы предполагаем компрометацию доменного администратора:
    - Восстановить AD из копии, предшествующей заражению
    - Если копии нет, построить AD с нуля (по согласованию)
    - Изменить метод защиты важных УЗ.

**Мониторинг:**

* Продолжить мониторинг на предмет обнаружения сигнатур, горизонтального перемещения, повышения привилегий и других индикаторов компрометации, чтобы предотвратить повторную атаку с использованием программы-вымогателя.

ВОССТАНОВЛЕНИЕ

* Полное сканирование всех затронутых систем на наличие вредоносного ПО и IoC, соответствующих профилю атаки.
* Восстановить системы до RPO в рамках RTO
* Выборочно проверить незатронутые или критичные системы.
* Реинтегрировать ранее скомпрометированные системы.
* Восстановить любые поврежденные или уничтоженные данные.
* Восстановить мониторинг для обнаружения дальнейшей подозрительной активности.
* Внедрить необходимые патчи и устранить выявленные уязвимости на затронутых и незатронутых объектах.

**Определить, какие из следующих действий необходимо выполнить:**

* Снять ограничения, ранее наложенные для сдерживания кибератаки:
  + Подключить ранее отключенные от сети хосты
  + Восстановление работы сервисов
  + Переподключить сетевые диски, которые были отключены во время атаки.
  + Включить резервное копирование, которое могло быть отключено во время атаки.
  + Включить сетевые интерфейсы, которые были отключены во время атаки.
  + И т.д.
* Необходимо обновить или изменить правила межсетевого экрана восстановления нормального трафика.
* Обновить систему обнаружения и реагирования на конечных точках (EDR) / Антивирус (AV) - Обновление программного обеспечения безопасности является критическим шагом. Необходимо обновить:
  + Ядро EDR/AV– программное ядро системы безопасности, отвечающее за обнаружение угроз.
  + Политики - правила, определяющие поведение системы безопасности.
  + База данных вредоносных программ и уязвимостей, используемая системой безопасности для их обнаружения.
* Связаться со страховой компанией, если это возможно и необходимо

ПОСТ-ИНЦИДЕНТ

* Подготовить отчет об инциденте, включая все детали и действия, предпринятые для его устранения.
* Завершить процессы *выявления* уроков и управления проблемами с предыдущих этапов.
* Обеспечить соответствующие внутренние и внешние коммуникации об инциденте
* Внедрить в СЗИ полученные сигнатуры данной атаки; обновить правила детектирования в SIEM, Анти-спам (фильтры), EDR (готовые TTP или ручные настройки) и иных решениях
* Пересмотреть процесс харденинга инфраструктуры
* Если инцидент был вызван человеческой ошибкой:
  + Устроить соответствующее обучение сотрудников
* Провести анализ первопричины для выявления и устранения уязвимостей.
* Провести оценку работы сотрудников: продолжительность рабочего времени, сверхурочные, отгулы за переработку и расходы.

**Составление отчета о последействиях инцидента, который должен включать как минимум следующую информацию:**

* Детали причин и воздействия инцидента, а также действий, предпринятых для смягчения киберинцидента, включая даты, тип и местоположение инцидента, а также его влияние на пользователей; время, затраченное на реагирование. Оценить выплаченный выкуп или иной ущерб, штрафы от государственных органов.
* Действия, предпринятые соответствующими группами реагирования, поставщиками услуг и заинтересованными сторонами бизнеса, которые позволили возобновить нормальную работу.
* Анализ ошибок реагирования и рекомендации по улучшению действий, процессов или технологий в организации, чтобы предотвратить повторное возникновение подобного киберинцидента.
* Мониторинг каких прекурсоров и индикаторов должен осуществляться для предотвращения подобного рода инцидентов?
* Сделать вывод о проанализированных артефактах форензики.

**Подтверждение соответствия политик:**

* Подтвердить соответствие политик безопасности по всей организации.
* Перенастроить процессы и процедуры, требующие улучшения
* Обновить плейбуки, если что-то в ходе реагирования шло не так

**Также возможно:**

* Публикация внутренних коммуникаций для информирования и обучения сотрудников о атаках с использованием программ-вымогателей и повышении осведомленности о безопасности.
* Публикация внешних коммуникаций, в соответствии с коммуникационной стратегией, для предоставления консультаций клиентам, взаимодействия с рынком и информирования прессы о киберинциденте, если это *необходимо*
  + Эти сообщения должны содержать ключевую информацию о киберинциденте, не ставя организацию в уязвимое положение и не провоцируя дальнейшие атаки с использованием программ-вымогателей.
* Поделиться TI-фидами

1. https://habr.com/ru/articles/439026/ [↑](#footnote-ref-1)
2. DNS Sinkholing – это механизм, направленный на защиту пользователей путем перехвата DNS-запросов, пытающихся подключиться к известным вредоносным или нежелательным доменам, и возврата ложного, а точнее контролируемого IP-адреса. Исп. для предотвращения подключения узлов к известным вредоносным направлениям, таким как C&C-сервер, и сбора журнала событий [↑](#footnote-ref-2)
3. Менять пароль нужно дважды (с задержкой достаточной для выполнения репликации во всем домене), т.к. в домене хранится текущий и предыдущий пароль. [↑](#footnote-ref-3)