Исследование электронных носителей информации

при недоступности средств защиты информации

Павенский Юрий Алексеевич
независимый эксперт

СЗИ развернуты, но штатный доступ ограничен

КОНТУР ИБ

СЗИ развернуты

SIEM, EDR, DLP, WAF, NGFW, SOAR и другие решения

Пентесты и практические учения

Совершенствование процессов реагирования

Регулярное прохождение проверок

СЕТЬ ПЕРЕДАЧИ ДАННЫХ

Отсутствует связность

Корпоративная сеть должным образом не функционирует

ДОСТУП К СЗИ

Ограничен

Штатный доступ через корпоративную сеть отсутствует. Доступ к отдельным СЗИ может сохраняться

ЦИФРОВЫЕ СЛЕДЫ

Остаются локально

И продолжают изменяться с каждой секундой

Наличие СЗИ не гарантирует доступность их данных во время инцидента

Пароль из утечки открыл доступ к личным ресурсам

01 / ИСТОЧНИК

База данных интернет-магазина

В открытом доступе оказались персональные данные клиентов, включая адреса электронной почты и пароли для доступа к личным кабинетам

02 / ПОЛЬЗОВАТЕЛЬ

Работник компании-разработчика IdM-системы

Для регистрации в интернет-магазине использовался личный почтовый ящик

03 / ПАРОЛЬ

Повторное использование

Один и тот же пароль использовался для нескольких личных учетных записей работника

04 / ДОСТУП

Компрометация личных ресурсов

Личный почтовый ящик

Публичное облачное хранилище

На этом этапе скомпрометированы только личные ресурсы работника

Электронная переписка раскрыла сведения о заказчиках

01 / OSINT

Профиль работника

Дополнительные личные почтовые ящики

Корпоративный адрес электронной почты

Контактные данные

Организация и занимаемая должность

02 / ЛИЧНЫЕ РЕСУРСЫ

Личный почтовый ящик и облачное хранилище

Обнаружена служебная переписка

03 / ЗАКАЗЧИКИ

Организации и ИТ-инфраструктура

Перечень организаций

Джамп-хосты

Способы удаленного подключения

04 / ACTIVE DIRECTORY

Учетные записи

Сервисные

Привилегированные

Полученные сведения позволили подготовить атаку на одного из заказчиков

Под видом подрядчика получен доступ к джамп-хосту

01 ПЕРЕПИСКА — Диалог с одним из заказчиков продолжен через личную почту работника подрядной организации

02 ПРЕДЛОГ — Дополнительные работы представлены как продолжение легитимного взаимодействия

03 ДОСТУП — Получено удаленное подключение к джамп-хосту заказчика

04 РАЗВЕДКА — Изучались способы удаленного подключения, доменная среда, учетные записи и права, критические серверы, базы данных и сетевая архитектура

Доступ к джамп-хосту использовался для разведки в течение следующей недели

Компрометация AD обеспечила устойчивое присутствие

AD

ДОМЕННАЯ СРЕДА

Точка перехода от джамп-хоста к ИТ-инфраструктуре

01 УЧЕТНЫЕ ЗАПИСИ

Скомпрометированы учетные записи Active Directory

02 ПРИВИЛЕГИИ

Получены данные для использования привилегированных и сервисных учетных записей

03 ЗАКРЕПЛЕНИЕ

Обеспечено устойчивое присутствие в ИТ-инфраструктуре

После компрометации AD атака перестала ограничиваться одним джамп-хостом

Выгружены базы данных и резервная копия личного мобильного устройства работника ИТ-подразделения

01 / ОБНАРУЖЕНИЕ И ВЫГРУЗКА

БАЗЫ ДАННЫХ

СОДЕРЖАЛИ СВЕДЕНИЯ О

Финансах
Работниках
Клиентах
Логистических процессах

02 / ОБНАРУЖЕНИЕ И ВЫГРУЗКА

НЕЗАШИФРОВАННАЯ РЕЗЕРВНАЯ КОПИЯ МОБИЛЬНОГО УСТРОЙСТВА

Личное мобильное устройство производства «Apple»
Обнаружена на корпоративном АРМ работника ИТ-подразделения

СОДЕРЖИМОЕ КОПИИ

Электронная переписка в мессенджерах
Различные учетные данные
Схемы организации связи
Фотографии документов с конфиденциальной информацией

Незашифрованная резервная копия личного мобильного устройства стала отдельным источником конфиденциальной информации

Резервные копии серверов уничтожены, связность корпоративной сети нарушена

01 УНИЧТОЖЕНЫ РЕЗЕРВНЫЕ КОПИИ ИТ-СЕРВЕРОВ

02 УДАЛЕНЫ КОНФИГУРАЦИОННЫЕ ФАЙЛЫ СЕТЕВОГО ОБОРУДОВАНИЯ

03 ВНЕСЕНЫ ИЗМЕНЕНИЯ В КОНФИГУРАЦИЮ КОММУТАТОРОВ УРОВНЯ ЯДРА

РЕЗУЛЬТАТ

НАРУШЕНА СВЯЗНОСТЬ КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

01 ДЕГРАДАЦИЯ ДОМЕННОЙ СРЕДЫ
02 УТРАТА ШТАТНОГО ДОСТУПА К БОЛЬШИНСТВУ СЗИ
03 ОГРАНИЧЕНИЕ ЦЕНТРАЛИЗОВАННОГО ДОСТУПА К ТЕЛЕМЕТРИИ

Шифрование баз данных переросло в вымогательство

01 ПАРОЛИ

Сменены пароли доступа
к корпоративным базам данных

02 ШИФРОВАНИЕ

Зашифрованы базы данных
в ИТ-инфраструктуре организации

03 ВЫКУП

Через Telegram работнику ИТ-подразделения
выдвинуто требование выкупа за восстановление доступа к данным

04 ПУБЛИКАЦИЯ ДАННЫХ

Злоумышленники угрожали опубликовать
в полном объеме информацию из резервной копии
личного мобильного устройства «Apple», способную опорочить
честь, достоинство и деловую репутацию работника. В подтверждение
реальности угрозы часть этой информации они разместили в Telegram-канале

Вымогательство сочетало блокирование данных и давление через угрозу публикации чувствительной информации

Три фактора риска и роль криминалистики

01 / ЛИЧНЫЙ АККАУНТ

НАЧАЛО ЦЕПОЧКИ

Компрометация одного личного аккаунта может привести к масштабному инциденту

02 / ПОДРЯДЧИК

ДОВЕРЕННЫЙ ДОСТУП

Доверенный доступ подрядным организациям без достаточного контроля создает существенный риск

03 / ХРАНЕНИЕ ДАННЫХ

ДАННЫЕ ВНЕ КОНТРОЛЯ

Несанкционированное хранение служебной информации ограниченного доступа на личных мобильных устройствах и в их резервных копиях может причинить ущерб организации и работнику

При отсутствии штатного доступа к СЗИ компьютерная криминалистика помогает восстановить картину инцидента

10 этапов реагирования без штатного доступа к СЗИ

01–05 / ПЕРВИЧНЫЕ ДЕЙСТВИЯ И ПРИНЯТИЕ РЕШЕНИЙ

01 Фиксация, регистрация и первичная эскалация

02 Организация реагирования

03 Предварительное установление масштаба инцидента

04 Обязательные уведомления и внешнее взаимодействие

05 Определение дальнейших действий в отношении проверяемых систем и устройств

06–10 / СБОР ДАННЫХ, РЕКОНСТРУКЦИЯ И ЗАВЕРШЕНИЕ

06 Сохранение volatile-артефактов и данных с высоким риском утраты

07 Получение проверяемых копий накопителей, виртуальных машин и постоянных цифровых данных для последующего исследования

08 Реконструкция последовательности атаки и проверка версий

09 Устранение последствий и восстановление ИТ-инфраструктуры

10 Закрытие инцидента ИБ и проведение корректирующих мероприятий

Сохранить volatile-артефакты или изолировать узел?

01 / СОХРАНЕНИЕ VOLATILE-АРТЕФАКТОВ ДО ИЗОЛЯЦИИ УЗЛА

Условия:

- связь с инцидентом установлена;
- ущерб не продолжается;
- подозрительных сетевых соединений и доступного злоумышленнику пути к другим системам и ресурсам не имеется.

ДО ОКОНЧАНИЯ 6 ЭТАПА УЗЕЛ ОСТАВЛЯЕТСЯ ВКЛЮЧЕННЫМ

Дальнейшие действия выполняются по зафиксированному решению.

02 / ПРИОРИТЕТ СДЕРЖИВАНИЯ

Условия:

- продолжается шифрование, удаление или изменение данных;
- имеется подозрительное сетевое соединение;
- сохраняется доступный злоумышленнику путь к другим системам и ресурсам.

СДЕРЖИВАНИЕ В ПРИОРИТЕТЕ

Осуществляется автоматизированный сбор данных, если это допустимо.
Затем узел изолируется, по возможности без выключения.
При недопустимой задержке — изоляция хоста осуществляется немедленно, после чего сохраняются доступные данные.

ОСОБЫЕ СЛУЧАИ (ПОЛНЫЙ ПОРЯДОК ДЕЙСТВИЙ ДОСТУПЕН ПО QR-КОДУ):

- связь с инцидентом не установлена → сбор данных не выполняется (при наличии новой информации решение может быть пересмотрено);
- узел выключен → его включение и загрузка его ОС не осуществляется;
- работающая VM → создается snapshot с ОЗУ (если платформа позволяет и это не задерживает сдерживание).

Универсального правила «сначала собрать все данные» или «сразу все изолировать» здесь не имеется.
Решение принимается отдельно по каждому узлу

Сначала — данные с наибольшим риском утраты

01 БАЗОВЫЕ СВЕДЕНИЯ ОБ УЗЛЕ

имя узла, версия операционной системы или загруженного ядра, время работы после последней загрузки (uptime), текущая учетная запись, системные дата, время и часовой пояс, одновременно зафиксированное время независимого источника и расхождение с системным временем узла

02 СЕАНСЫ И АКТИВНОСТЬ

активные пользователи и сеансы, процессы и службы с параметрами запуска, кешированные данные аутентификации текущих сеансов и открытые файлы

03 ЖУРНАЛЫ И МОДУЛИ

Локальные журналы с риском перезаписи, загруженные драйверы и модули, расширения ядра и активные средства межпроцессного взаимодействия.

04 СЕТЕВОЕ СОСТОЯНИЕ

Сетевые интерфейсы, активные соединения и слушающие порты, сетевые маршруты и сведения о соседних узлах (ARP/NDP).

Дамп оперативной памяти формируется после сбора вышеуказанных данных*

*** - если имеется совместимое проверенное средство и операция не создает неприемлемого риска.**

Состояние фиксируется до восстановления сети

CLI

ЛОКАЛЬНЫЙ ДОСТУП

Подключение выполняется через локальный консольный порт с автономного недоменного АРМ

01 ДО ПЕРВОЙ КОМАНДЫ

Включается протоколирование терминального сеанса и фиксируется время независимого источника

02 ПЕРВАЯ КОМАНДА

Фиксируется доступная история команд: новые команды могут вытеснить ранние записи из ограниченного буфера

03 ЗАТЕМ — СОСТОЯНИЕ

Фиксируются: системное время, версия и время работы устройства (uptime), административные сеансы, журналы, сведения о текущей и загрузочной конфигурации, состояние интерфейсов, сетевые маршруты и основные оперативные таблицы

Используются только заранее проверенные команды просмотра с минимальным и прогнозируемым воздействием

Проверяемая копия: происхождение и целостность

ПРОВЕРЯЕМОСТЬ → источник данных, способ их получения, использованное средство и его версия, время операции, место сохранения результата
и рассчитанные контрольные суммы.

01 / ФИЗИЧЕСКИЙ НАКОПИТЕЛЬ

ЗАЩИТА ОТ ЗАПИСИ

ОС с исследуемого накопителя не загружается

Аппаратный блокиратор записи является приоритетным

Если аппаратного блокиратора не имеется, используется заранее проверенная программная защита

Посекторная (побитовая) копия — когда технически возможна и оправданна

02 / RAID-МАССИВ

БЕЗ ЛИШНЕЙ РАЗБОРКИ

Фиксируют: модель контроллера, уровень и состояние массива, количество дисков, номера физических отсеков (слотов), серийные номера и состояние каждого диска

Если логический том доступен через штатный контроллер, данные получают без разборки массива, исключив запись и автоматическое перестроение

Иначе — реконструкция выполняется по копиям физических носителей

03 / ВИРТУАЛЬНАЯ МАШИНА

НЕЗАВИСИМЫЙ КОМПЛЕКТ

Выгружаются: конфигурация, журналы платформы, основной виртуальный диск и вся цепочка связанных разностных дисков

При наличии, выгружается файл состояния оперативной памяти

Если посекторная (побитовая) копия технически невозможна → документированный целевой сбор