?????????? ?? ????????????? ??????????

Windows события

eventvwr.msc

Категории системных журналов:

- Приложения (Application) – как и гласит название, содержит события и ошибки приложений.
- Безопасность (Security) – если в операционной системе включена и настроена функция аудита, журнал будет содержать записи, связанные с отслеживанием соответствующих событий (например, авторизация пользователя или попытки неудачного входа в операционную систему, события создания процессов и завершении их работы).
- Система (System) – здесь регистрируются события операционной системы и системных сервисов, их критичные завершения работы.
- Установка (Setup) – события, связанные с инсталляцией обновлений Windows, дополнительных приложений.

В разделе Журналы приложений и служб (Applications and Services Logs) детальная информация о событиях отдельных служб и приложений, зарегистрированных в операционной системе.

Типы событий:

- Сведения (Information) — информируют о штатной работе приложений;
- Предупреждение (Warning) — событие, свидетельствующее о возможных проблемах в будущем (например, заканчивается свободное место на диске – приложения могут продолжать работу в штатном режиме, но когда место закончится совсем, работа будет невозможна);
- Ошибка (Error) — проблема, ведущая к деградации приложения или службы, потерям данных;
- Критическое (Critical) — значительная проблема, ведущая к неработоспособности приложения или службы;
- Аудит успеха (Success audit) — событие журнала Безопасность (Security), обозначающее успешно осуществленное действие, для которого включено отслеживание (например, успешный вход в систему);
- Аудит отказа (Failure audit) — событие журнала Безопасность (Security) обозначающее безуспешную попытку осуществить действие, для которого

включено отслеживание (например, ошибка входа в систему).

Фильтр журнала:

Правый клик по журналу – Фильтр текущего журнала… (>Filter Current Log…), Можно задать временной период, уровни события, выбрать журналы и конкретные источники событий, коды событий.

По умолчанию файлы журналов событий Windows используют расширение EVTX и находятся в папке %SystemRoot%\System32\winevt\Logs.

Приложение Просмотр событий (Event Viewer) позволяет также настроить дополнительные свойства журналов. Доступ к настройкам можно получить через панель быстрых действий, либо через контекстное меню журнала – правый клик по журналу – Свойства (Properties):

Настраивается путь файла журнала, текущий размер, максимальный размер файла. Для журнала "Система" желательно увеличить 100Мб, журнал security до 500Мб (при наличии достаточного запаса объема дискового пространства то увеличить до 1Гб)

Вариант действия при достижении журналом максимального значения:

- Переписывать события при необходимости (Overwrite events as needed) – новое событие будет записываться поверх самого старого события в журнале, таким образом будут доступны события только за определенный диапазон времени.
- Архивировать журнал при заполнении (Overwrite the log when full) – заполненный журнал будет сохранен, последующие события будут записываться в новый файл журнала. При необходимости доступа к старым событиям, архивный файл можно будет открыть в приложении Просмотр событий (Event Viewer).
- Не переписывать события (Do not overwrite events) – при заполнении журнала выдается системное сообщение о необходимости очистить журнал, старые события не перезаписываются.

Настройка размера журналов с помощью групповой политики (GPO):

Запустите консоль Group Policy Management (gpmc.msc), создайте новую GPO и назначьте на OU с компьютерами или серверами, для которых вы хотите изменить настройки Event Viewer (или назначьте GPO на корень домена);
Перейдите в раздел GPO Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Event Log Service. Как вы видите, в этом ветке есть подразделы для управления базовыми журналами Windows: Application, Security, Setup, System;
Чтобы увеличить максимальный размер любого из журналов, откройте параметр Specify the maximum log file size (KB), включите его и задайте нужный вам размер (минимум для Security, Sysmon — 500Мб, для остальных журналов минимум — 200Мб;
Обновите настройки политики на клиентах и проверьте, что в свойствах журнала теперь указан новый размер.

Первоочередный анализ

Журнал Security (безопасность).

Будем перечислять события по идентификаторам (EventID):

- 4688 — событие создания процесса. Данное событие полезно для выявления создания нелегитимных процессов, для отслеживания запуска хакерских утилит, выявления нетипичных командных строк, выявления аномалий между родительским и дочерним процессом. По умолчанию аудит данного события в системе не настроен.
- 4624 — событие успешной аутентификации. Событие полезно для анализа нелегитимных входов пользователей, которые не должны аутентифицироваться на конкретном хосте, либо для выявления откуда исходило заражение.
- 4625 — событие неуспешной попытки аутентификации. Событие полезно для выявления попыток подбора пароля.
- 1102 — событие об очистке журнала событий Security.
- 4697 — событие установки службы. Событие полезно для выявления закрепления злоумышленника в системе через службы Windows.
- 4648 — событие попытки входа под заданной учетной записью. Активность может быть сгенерирована, когда процесс выполняется в режиме “Запуск от имени” (run as). В нормальном режиме работы систем данное событие встречается достаточно редко.

Журнал System (Система):

- 104 — событие очистки журнала событий.
- 7045 — событие установки службы. Событие полезно для выявления закрепления злоумышленника в системе через службы Windows.

Журнал TerminalServices-RemoteConnectionManager:

1149 — событие аутентификации по протоколу RDP (Remote Desktop Protocol). Полезен для выявления нелегитимных аутентификаций по RDP.

Журнал PowerShell:

4103 — событие фиксирует информацию о каждой выполненной команде и параметрах, с которыми она вызывалась. Полезен для выявления запуска командлетов powershell для выполнения разведки на рабочей станции или иных вредоносных действий. По умолчанию аудит данного события в системе не настроен.

4104 — событие фиксирует содержимое скрипта powershell на исполнение. Журналирование блокировки скриптов показывает каждый выполненный блок кода powershell. Даже если злоумышленник попытается скрыть команду, этот тип события покажет фактически выполненную команду powershell. Ещё в этом типе события могут фиксироваться некоторые выполняемые низкоуровневые вызовы API, эти события обычно записывается как Verbose, но, если подозрительная команда или сценарий используются в блоке кода, он будет зарегистрирован как с критичностью Warning. По умолчанию аудит данного события в

системе не настроен.

Расширение журналируемых событий

Пример конфигурационного файла Sysmon от Флориана Рофа - конфигурация.

Sysmon

Sysmon (сокращение от System Monitor) — инструмент Microsoft в наборе Sysinternals для мониторинга и регистрации деятельности в операционной системе Windows. Он предоставляет дополнительную информацию о событиях в системе.

Задачей Sysmon является обнаружение и защита от вредоносного поведения, а также расследование инцидентов безопасности в сети. Он позволяет анализировать системные события, предоставляя информацию о процессах, сетевых подключениях, файловой активности, загрузке драйверов, реестре и т. д.

Функциональность Sysmon позволяет:

- фиксировать событие запуска и завершения процессов, при этом событие создания процесса в sysmon содержит в себе хэш-сумму запущенного процесса и командную строку родительского процесса, которых нет в событи 4688 расширенного аудита Windows;
- мониторировать сетевую активность, включая открытие и закрытие сетевых соединений и DNS-запросы;
- отслеживать загрузку драйверов и загрузку DLL-библиотек;
- регистрировать создание и удаление файлов, доступ к файлам и изменение файловой системы;
- анализировать действия с реестром, включая создание, изменение и удаление ключей и значений;
- фиксировать создания потоков, именованных каналов между процессами;
- мониторить изменения содержимого буфера обмена, способы сокрытия;
- выполнять активную функцию по блокировке запуска исполняемых файлов указанных в конфигурационном файле.

EventLogExplorer: — эффективное средство для просмотра и анализа событий, хранящихся в журналах операционных систем семейства Microsoft Windows. Позволяет существенно ускорить и упростить решение задач анализа журналов событий. Возможности Event Log Explorer существенно шире, чем у стандартного приложения Просмотр событий. Остальной функционал и преимущества приведены ниже:

- Высокая производительность.
- Мощная система фильтрации. Предоставляет пять способов фильтровать события по любому критерию. Сложные фильтры можно использовать повторно — сохранять и позже использовать снова. Быстрые фильтры по подобию существенно ускоряют работу.

- Непосредственный доступ. Позволяет организовать в виде дерева компьютеры и их Windows-логи (журналы), а также лог-файлы. При этом доступ к журналам и управление компьютерами, журналами становится очень простым, наглядным и быстрым.
- Объединение журналов событий. Позволяет анализировать события Windows из разных источников (журналов и файлов) одновременно. Event Log Explorer позволяет объединять разные журналы с разных машин в одно представление (общий лог). Это очень помогает при анализе хронологии событий из множества источников.
- Пользовательские колонки. Показывают данные из описаний событий (имя пользователя, имя файла и т.д.) в отдельных колонках в списке событий. Это позволяет анализировать отдельные самые важные данные из описаний событий без необходимости просматривать описания событий целиком. Эта возможность сильно ускоряет анализ данных журналов событий Windows.
- Менеджер учетных данных. Позволяет хранить учетные данные к компьютерам. Когда вы открываете журнал компьютера по сети, Event Log Explorer использует те учетные данные, которые использовались в прошлый раз при работе с этим удаленным компьютером и его логами.
- Распечатка и экспорт. Позволяет вам распечатывать события, отфильтрованные выборки событий из журналов, журналы целиком — все что пожелаете. Также можете экспортировать данные в разные форматы (Excel - xls, xlsx, csv-текст, html и evt). Вы можете выбрать колонки, которые нужно экспортировать или печатать, выбрать из различных макетов размещения данных при печати и просмотреть как будут выглядеть распечатки.
- Планировщик и автоматизация. Позволяет легко автоматизировать многие задачи. Например, вы можете запланировать регулярный экспорт определенных выборок определенных событий из определенных журналов в Excel-файл в определенной папке.
- Активный мониторинг. Можете настроить Event Log Explorer на регулярное обнаружение новых событий, удовлетворяющих заданному фильтру в определенных Windows-журналах в вашей сети. Также можно настроить получение оповещений на e-mail, когда заданные события появятся. Это позволит более оперативно реагировать на проблемы.
- Резервное копирование. Предоставляет три способа резервного копирования журналов Windows: бэкап вручную, автоматическое резервное копирование при заполнении лога или планируемое расширенное резервное копирование с помощью нашей утилиты, интегрированной с Event Log Explorer.
- Аналитические отчеты. В Event Log Explorer очень просто сделать аналитические отчеты и диаграммы для журналов Windows и выборок событий Windows.
- Прямой доступ к файлам. Event Log Explorer может получать данные из EVT and EVTX файлов напрямую (без Windows API). Это позволяет извлекать данные даже из поврежденных файлов или работать с EVTX файлами в Windows XP.
  Закладки и цветовое кодирование. В Event Log Explorer процесс исследования сложных ситуаций становится немного приятнее благодаря множеству маленьких удобств, таких как цветовое кодирование (подсветка определенных событий заданными Вами цветами) и закладки (запоминание позиций в журнале или

выборке и быстрый возврат к этим позициям).
- Подмена источника описаний. При следственных действиях часто приходится работать с лог-файлами, взятыми с машин другой сетевой инфраструктуры. Вы можете задать другой компьютер, с которого будут браться описания событий, так как на компьютере исследователя могут отсутствовать необходимые описания. Например, при анализе логов, взятых с Windows-сервера, к которому нет доступа, можно указать другой сервер и получить необходимые описания.
- Коррекция времени. При проведении исследования Вы можете столкнуться с журналами, взятыми с компьютеров, находившихся в другой временной зоне. По умолчанию события будут показываться в вашей временной зоне. Вы можете задать коррекцию времени и увидеть события так, как они происходили в том месте, в той временной зоне, где находится компьютер, с которого взяты данные.

EvtxECmd: Инструмент EvtxECmd — парсер событий EVTX из набора утилит Эрика Зиммермана. Утилита позволяет конвертировать EVTX файлы с событиями в формат CSV, XML, JSON для более удобной дальнейшей работы с событиями.

EvtxECmd не имеет графического интерфейса. Сконвертировать журнал событий Sysmon в формат CSV из формата EVTX с помощью команды:

```
EvtxECmd.exe -f "Microsoft-Windows-Sysmon%4Operational.evtx" --csv "C:\tools\EvtxECmd" --csvf sysmon.csv
```

Где ключ -f означает какой журнал событий принимается для конвертации, ключ --csv означает в какую папку сохраняем полученные данные, ключ --csvf задает имя сохраняемого файла в формате csv.

PowerShell — командлеты PowerShell для работы с событиями позволяют гибко выполнять поиск нужных событий. Основные команды PowerShell для работы с логами:

Get-EventLog — для работы с классическими журналами (Application, System, Security);
Get-WinEvent — для работы с любыми журналами.
Список доступных журналов можно получить командой:

Get-WinEvent -ListLog

Вывести 10 последних записей журнала System позволяет команда:

Get-WinEvent –LogName ‘System’ –MaxEvents 10

Для более удобной фильтрации можно использовать хеш-таблицы, например, следующая команда выводит информацию о событиях журнала Security с кодом 4688, генерация которых связана с созданием процесса в операционной системе Windows:

Get-WinEvent –FilterHashTable @{LogName=’Security’;ID=4688}

Анализ активности при дампе памяти процесса lsass.exe

Сервис проверки подлинности локальной системы безопасности (Local Security Authority Subsystem Service, LSASS) — часть операционной системы Windows, отвечающая за авторизацию локальных пользователей отдельного компьютера.

Память процесса lsass.exe в нем хранятся хеши паролей учетных записей, прошедших аутентификацию. Если еще включить функцию WDigest, то в таком случае злоумышленник получит уже пароли в открытом виде. Сделать это злоумышленник может одним из способов с помощью изменения реестра:

reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1

Способов дампа различными утилитами памяти процесса lsass.exe огромное множество, мы проанализируем один из вариантов.

Один из способов дампа памяти процесса lsass.exe

Событие 1 Sysmon зафиксировало подозрительную командную строку:

"C:\Windows\system32\rundll32.exe" C:\windows\system32\comsvcs.dll MiniDump 728 dump.bin full

Где rundll32.exe запускает библиотеку comsvcs.dll и вызывает функцию MiniDump, цифра 728 — это идентификатор процесса lsass.exe. Далее сохраняет в файл дамп памяти процесса lsass.exe, full - означает полный дамп памяти процесса.
Команда, запущенная с высокими правами - High.

Процесс-инициатор — C:\Windows\system32\rundll32.exe
Процесс, к области памяти которого было обращение. Напомним, что lsass.exe содержит в памяти как минимум хеши аутентифицированных пользователей — C:\Windows\system32\lsass.exe
Права доступа запрошены, в том числе и на чтение, которое достаточно для дампа - 0x1410
Стек вызовов (CallTrace) содержит библиотеку comsvcs.dll, у которой есть функция MiniDump для дампа памяти процессов.

Таким образом злоумышленнику даже не нужно на рабочую станцию с собой приносить инструмент для дампа памяти процесса lsass.exe, т.к. операционная система имеет достаточный функционал для этого. Подобный функционал, который используется злоумышленниками в своих атаках называется LOLBins.

LOLBins (Living Off the Land Binaries and Scripts) – это термин, используемый в кибербезопасности для обозначения легитимных исполняемых файлов, скриптов или утилит, уже доступных на компьютере пользователя, с помощью которых хакеры выполняют различные вредоносные действия.

Поведенческий анализ

Поведенческий анализ помогает выявлять отклонения от нормального поведения пользователя, что может указывать на компрометацию аккаунта или вредоносную активность. Анализируя поведение, системы безопасности могут классифицировать типы угроз и атак, определяя потенциальные цели злоумышленников. Техника направлена на быстрое обнаружение подозрительных действий, что позволяет оперативно реагировать на угрозы.

Поведенческий анализ в приложениях

В контексте безопасности под поведенческим анализом понимается мониторинг и анализ поведения пользователей в приложениях с целью выявления аномальных и подозрительных активностей.

Месседжеры

- Обнаружение необычных входов — проверка местоположения входа в аккаунт.
- Сравнение с предыдущими местами входа.
- Мониторинг частоты сообщений — анализ необычно высокой или низкой активности в отправке сообщений.
- Фильтрация контента — обнаружение отправки или получения подозрительных файлов.
- Анализ необычного поведения в чатах.

Почтовые приложения

- Обнаружение подозрительных вложений — мониторинг вложенных файлов с подозрительными расширениями.
- Отслеживание необычных попыток входа — защита от несанкционированных попыток доступа к электронной почте.
- Анализ паттернов активности — определение необычных времен отправки и получения писем.

1С

- Аномальные попытки входа в систему.
- Необычные запросы и операции: изменение уровня доступа или ролей пользователя, необычные или редкие запросы к базе данных или изменения данных.
- Попытки доступа к защищенным или чувствительным данным после нескольких неудачных попыток.
- Необычные объемы передачи данных.
- Попытки изменения или удаления журналов регистрации.

Системы анализа поведения пользователей

Системы анализа поведения пользователей (User and Entity Behavior Analytics, UEBA) позволяют проводить анализ поведения пользователей и сущностей (Entity). Основная цель UEBA заключается в выявлении аномальных и потенциально угрожающих действий, которые могут указывать на наличие киберугроз или несанкционированной активности в сети.

Основные задачи систем UEBA:

- Определение типичного поведения пользователей в приложениях.
- Выявление аномалий на фоне определенного типичного поведения пользователей.
- Выявление потенциальных угроз безопасности.
- Анализ данных в контексте, с учетом особенностей среды и типичное поведение пользователей в различных ситуациях.

С открытым исходным кодом можно использовать системы ниже:

- Wazuh — платформа для обеспечения безопасности, предоставляющая агентов для сбора данных, включая логи, и систему анализа поведения.
- MozDef — это бесплатная открытая платформа для обработки и анализа событий безопасности, которая включает в себя модули для обнаружения аномалий.
- ELK Stack (Elasticsearch, Logstash, Kibana) — ELK Stack часто используется для централизованного сбора и анализа логов, и его можно настроить для обнаружения аномалий.

Интеграция систем поведенческого анализа с мессенджерами

При интеграции мессенджеров с UEBA-системами осуществляется:

- Логирование и сбор данных. Необходим доступ к логам мессенджеров. Логи как правило включают в себя события входа и выхода, обмен сообщениями, создание и редактирование групп и другие активности пользователей. Логи должны быть стандартизованы и нормализованы в зависимости от используемой системы.
- Анализ поведения. Системы поведенческого анализа используют алгоритмы и методы машинного обучения для анализа поведения пользователей. Они используются для выявления стандартных паттернов активности и обнаружения аномальных действий.
- Учет контекста. Стандартные паттерны активности пользователей включают в себя контекст — время активности, местоположение пользователя, устройства и другие параметры, таким образом можно выявить аномалии в поведении пользователя.
- Обнаружение аномалий. После выявления стандартных паттернов с учетом окружающего контекста, становится возможным выявлять аномалии в поведении пользователей.
- Использование баз известных угроз. Помимо вышеперечисленного, подозрительные действия также выявляются на основе предыдущих инцидентов безопасности.

Метрики, которые могут использоваться при выявлении аномалий:

- Время активности пользователя;

- Геолокация пользователя;
- События успешных/неуспешных логинов;
- Объем передаваемых и получаемых данных;
- При наличии доступа к соответствующим логам: изменения в структуре групповых чатов, содержание сообщений и содержание вложенных файлов.

В системах поведенческого анализа без интеграции с SIEM и IRP можно настроить отправку оповещений Blue Team, в которых будет содержаться информация о событиях ИБ. Далее Blue Team может принимать меры по расследованию и реагированию.

Логирование в мессенджерах на примере Telegram

По умолчанию логирование в Telegram крайне ограничено. Путь к файлу логов можно найти, открыв окно с настройками и введя viewlogs, - после этого откроется папка с файлом log.txt

Это могут быть пути:

- На MacOS: /Users/USERNAME/Library/Application Support/log.txt.
- На Windows: C:\Users\USERNAME\AppData\Roaming\Telegram Desktop\log.txt.
- На Linux Ubuntu: /home/user/.local/share/TelegramDesktop/log.txt.

Файл log.txt постоянно обновляется, при этом вес его не должен превышать 250 Кб. Файл содержит логи об ошибках приложения, визуальной составляющей (например, загрузка шрифтов), о работе аудиоустройств и т.д. Эти логи, прежде всего, необходимы разработчикам для устранения ошибок в работе приложения, и представляют мало интереса с точки зрения безопасности.

Расширенные логи можно получить путем включения режима отладки (debug mode). Для этого при открытом окне настроек Telegram необходимо ввести debug mode, Telegram запросит подтверждение для включения этого режима. По умолчанию debug mode отключен. Если организации необходимо отслеживать расширенные логи приложения Telegram у сотрудников, нужно учесть следующие важные моменты:

- На рабочем устройстве в Telegram должен быть включен debug mode. Например, сотрудники получают устройства с предустановленным ПО, и администраторы заранее включили режим отладки. Учитывая, что любой пользователь может самостоятельно отключить debug mode, организации небходимо отслеживать события включения-выключения этого режима, что можно делать с помощью записи событий из обычных логов log.txt.
- Логи с включенным debug mode могут содержать чувствительную для пользователя и для организации информацию: названия чатов, в которых состоит пользователь, контакты пользователя, текст сообщений, время просмотра чатов, время звонков, формат звонков (аудио/видео) и т.д. Это требует, во-первых, предупреждения сотрудников о том какую информацию собирает компания, во-вторых, необходимо обеспечить безопасную передачу данных из файлов логов до, например, SIEM.

Пути до файлов логов будут аналогичными тем, где находится log.txt, сами логи хранятся в папке DebugLogs.

Пример log.txt:

```
[2024.01.22 13:22:02] Launched version: 4014009, install beta: [FALSE], alpha: 0, debug mode: [FALSE]
[2024.01.22 13:22:02] Executable dir: /Applications/, name: Telegram.app
[2024.01.22 13:22:02] Initial working dir: //
[2024.01.22 13:22:02] Working dir: /Users/USERNAME/Library/Application Support/Telegram Desktop/
[2024.01.22 13:22:02] Command line: /Applications/Telegram.app/Contents/MacOS/Telegram -noupdate -tosettings
[2024.01.22 13:22:02] Executable path before check: /Applications/Telegram.app
[2024.01.22 13:22:02] Logs started
[2024.01.22 13:22:02] Connecting local socket to /tmp/7cf2fc74b790e21d12eb2abd54c62016-{87A94AB0-E370-4cde-98D3-ACC110C5967D}...
[2024.01.22 13:22:02] This is the only instance of Telegram, starting server and app...
[2024.01.22 13:22:02] Moved logging from '/Users/USERNAME/Library/Application Support/Telegram Desktop/log_start0.txt' to '/Users/USERNAME/Library/Application Support/Telegram Desktop/log.txt'!
[2024.01.22 13:22:02] Global devicePixelRatio: 2
[2024.01.22 13:22:02] Primary screen DPI: 72, Base: 72.
[2024.01.22 13:22:02] Computed screen scale: 100
[2024.01.22 13:22:02] DevicePixelRatio: 2
[2024.01.22 13:22:02] ScreenScale: 110
[2024.01.22 13:22:02] Font: from ':/gui/fonts/DAOpenSansRegular.ttf' loaded 'DAOpenSansRegular'
[2024.01.22 13:22:02] Font: from ':/gui/fonts/DAVazirRegular.ttf' loaded 'DAVazirRegular'
[2024.01.22 13:22:02] Font: from ':/gui/fonts/DAOpenSansRegularItalic.ttf' loaded 'DAOpenSansRegularItalic'
...

[2024.01.22 14:18:25] Could not send ping for some seconds, restarting...
[2024.01.22 14:23:36] Audio Info: -receiveWakeNote: received, scheduling detach from audio device
[2024.01.22 14:33:00] Audio Info: recreating audio device and reattaching the tracks
[2024.01.22 14:33:02] Audio Info: Closing audio playback device.
[2024.01.22 14:36:19] API Warning: not loaded minimal channel applied.
[2024.01.22 14:36:47] Audio Info: recreating audio device and reattaching the tracks
```

```
[2024.01.22 14:36:49] Audio Info: Closing audio playback device.
[2024.01.22 14:53:01] Message Info: bad message notification received (error_code 16) for
msg_id = 7326916857930079324, seq_no = 1378
[2024.01.22 14:53:01] Message Info: bad message notification received (error_code 16) for
msg_id = 7326916858150819740, seq_no = 1378
```

С точки зрения безопасности в этих логах могут быть полезными следующие сообщения:

Версия приложения:
Launched version: 4014009, install beta: [FALSE], alpha: 0, debug mode: [FALSE].
Является ли включенным/выключенным debug mode:
Launched version: 4014009, install beta: [FALSE], alpha: 0, debug mode: [FALSE].
Рабочая директория:
Working dir: /Users/USERNAME/Library/Application Support/Telegram Desktop/.
Также могут быть полезны сообщения Message Info — в рамках рассмотрения логов по умолчанию, эти сообщения содержат коды ошибок (error_code), которые связаны с определенным msg_id, где msg_id — это уникальный идентификатор сообщения или контейнера (контейнеры представляют собой сообщения, содержащие несколько других сообщений и используются для возможности передачи нескольких запросов RPC и/или служебных сообщений одновременно).

Варианты error_code:

16: msg_id слишком низкий (скорее всего ошибка связана с неверным временем клиента, нужно синхронизировать его с использованием уведомлений msg_id и переслать сообщение с "правильным" msg_id или упаковать его в контейнер с новым msg_id, если исходное сообщение слишком долго ожидалось на клиенте для передачи);
17: msg_id слишком высокий (аналогично предыдущему случаю необходима синхронизация времени клиента, и сообщение должно быть перенаправлено с правильным msg_id);
18: неверные два последних бита msg_id (сервер ожидает, чтобы msg_id клиентского сообщения делился на 4);
19: msg_id контейнера совпадает с msg_id ранее полученного сообщения (это никогда не должно происходить);
20: сообщение слишком старое, и нельзя проверить было ли сервером получено сообщение с этим msg_id или нет;
32: msg_seqno слишком низкий (сервер уже получил сообщение с более низким msg_id, но с более высоким или равным и нечетным seqno);
33: msg_seqno слишком высокий (аналогично, есть сообщение с более высоким msg_id, но с более низким или равным и нечетным seqno);
34: ожидается четный msg_seqno (несущественное сообщение), но получено нечетное;
35: ожидается нечетный msg_seqno (существенное сообщение), но получено четное.

Журнал MTP

Так же, как и расширенные логи, логи MTP записываются в файлы каждые 15 минут, названия файлов логов имеют структуру mtp_HH_MM.txt, где:

HH - час в 24-часовом формате;
MM - минуты в интервалах 15 минут.
Например: mtp_14_15.txt, mtp_14_30.txt.

Журнал last_call_log

Файл содержит информацию о последнем совершенном аудио/видео звонке. Логи предоставляют информацию о запуске и конфигурации WebRTC (Web Real-Time Communication) в приложении. В контексте информационной безопасности эти логи могут быть полезными для следующих аспектов:

1. Криптография. В логах видно создание ключевых пар и сертификатов для шифрования данных с использованием OpenSSL.
2. Сетевая активность. Логи содержат информацию о портах и сетевых настройках, таких как IP-адреса и использование сетей. Это может быть полезно для отслеживания и анализа сетевой активности приложения.
3. Протоколы и передача данных. Протоколы и механизмы передачи данных, такие как DTLS (Datagram Transport Layer Security) и SRTP (Secure Real-time Transport Protocol), указываются в логах. Это важно для понимания, как происходит обеспечение безопасности данных в реальном времени.
4. Отладка и анализ ошибок. Логи содержат информацию о возможных ошибках, отладочные сообщения и стеки вызовов. Это может помочь в обнаружении и решении проблем, связанных с аудио- и видеокоммуникациями.
5. Информация о сети. Логи отображают сетевые параметры, такие как тип сети, стоимость соединения, а также IP-адреса и порты. Это полезная информация для оценки стабильности и производительности сети.

С точки зрения информационной безопасности важно следить за корректностью настроек шифрования, обеспечивать правильное управление ключами, а также мониторить сетевую активность для выявления потенциальных угроз или несанкционированной активности. Логи также могут быть использованы для анализа событий в случае инцидентов безопасности.

1. Установка параметров эксперимента WebRTC:

   ```
   Setting field trial string:WebRTC-DataChannel-Dcsctp/Enabled/WebRTC-Audio-MinimizeResamplingOnMobile/Enabled/WebRTC-Audio-iOS-Holding/Enabled/WebRTC-IceFieldTrials/skip_relay_to_non_relay_connections:true/
   ```

   Здесь указана строка параметров для WebRTC, включающая различные опции для аудио и ICE (Interactive Connectivity Establishment).

2. Настройка аудио-устройства:

```
AudioDeviceBuffer::ctor SetRecordingSampleRate(48000) SetRecordingChannels(1)
```

Происходит инициализация и настройка параметров аудио-устройства, включая частоту дискретизации и количество каналов.

3. Создание ключевых пар и сертификата с использованием OpenSSL:

```
Making key pair Returning key pair Making certificate for WebRTC Returning
certificate
```

Записи связаны с генерацией ключевых пар и сертификата с использованием OpenSSL для обеспечения безопасности.

4. Информация о подключенных модулях обработки аудио:

```
Injected APM submodules... Denormal disabler: supported
```

Указываются внедренные модули обработки аудио и их параметры, такие как поддержка Denormal disabler.

5. Настройка параметров сети и ICE:

```
Set continual_gathering_policy to 1 Set backup connection ping interval to 25000
milliseconds. Set ICE receiving timeout to 2500 milliseconds
```

Установка параметров сети и ICE (Interactive Connectivity Establishment) для обеспечения стабильности и надежности подключения.

6. Настройка параметров шифрования:

```
Setting RTCP Transport on null transport 0 Setting RTP Transport on null transport 0
```

Установка параметров транспорта для RTCP и RTP, связанных с безопасностью и шифрованием.

7. Информация о параметрах обработки звука и аудиопроцессинге:

```
WebRtcVoiceEngine::ApplyOptions: AudioOptions... AudioProcessing::ApplyConfig:
AudioProcessing::Config{...
```

Указываются параметры аудиопроцессинга, такие как управление эхом, уровень шума, фильтры высоких частот и др.

8. Информация о сетевой активности и портах:

```
Start getting ports with turn_port_prune_policy 0
Port[ac5d5800::1:0:local:Net[en0:192.168.1.x/24:Unknown:id=1]]: Port created with
network cost 50
```

Указываются действия по получению портов, инициализация порта сети и соответствующая сетевая информация.

Поведенческий анализ в почтовых приложениях

Заголовки почтовых сообщений

Почтовые сообщения содержат различные заголовки, которые предоставляют информацию о различных аспектах сообщения. Вот некоторые из основных заголовков электронных писем:

Заголовок	Описание
From (От)	Адрес электронной почты отправителя и его имя
To (Кому)	Содержит адрес(а) электронной почты получателя(ей)
Subject (Тема)	Тема письма
Date (Дата)	Дата и время отправки сообщения. Обычно, это значение генерируется почтовым сервером отправителя.
Message-ID (Идентификатор сообщения)	Уникальный идентификатор, присвоенный каждому сообщению. Используется для уникальной идентификации конкретного письма.
MIME-Version	Указывает версию стандарта MIME (Multipurpose Internet Mail Extensions), который определяет формат сообщения и поддерживает отправку не только текстовых данных, но и изображений, аудио, видео и других типов файлов.
Content-Type (Тип контента)	Определяет тип содержимого сообщения (текст, изображение, аудио и т.д.) и его подтип.
Content-Disposition (Расположение содержимого)	Определяет, каким образом содержимое должно быть отображено или обработано (например, встроено в сообщение или вложено как файл).

Received (Получено)	Этот заголовок создается каждым промежуточным почтовым сервером, через который проходит сообщение. Он содержит информацию о времени и месте обработки сообщения, а также идентификатор сервера.
References (Ссылки)	Используется для связи с другими сообщениями в цепочке.
In-Reply-To (В ответ на)	Указывает на сообщение, на которое отвечает текущее.
Return-Path (Обратный путь)	Содержит адрес, на который возвращаются недоставленные сообщения.

Помимо стандартных заголовков существуют кастомные заголовки, или x-headers.

X-headers (или расширенные заголовки) в почтовых письмах представляют собой дополнительные заголовки, начинающиеся с "X-" и используемые для включения дополнительной информации в сообщение. Эти заголовки могут быть добавлены почтовыми серверами, клиентами электронной почты или другими почтовыми агентами с целью предоставить дополнительные метаданные или сведения, которые не входят в стандартные заголовки электронных писем.

Примеры X-headers могут включать в себя:

Заголовок	Описание
X-Spam-Status	Этот заголовок может предоставить информацию о том, было ли сообщение отмечено как спам, и включать дополнительные детали о результатах анализа спам-фильтров.
X-Mailer	Указывает на почтовый клиент или программное обеспечение, использованное для отправки письма. Этот заголовок может быть полезен для анализа, какие клиенты чаще всего используются отправителями.
X-Priority	Устанавливает приоритет сообщения. Это может использоваться для определения, насколько важным отправитель считает своё сообщение.
X-MS-Exchange-Organization-AuthSource	Этот заголовок используется в Microsoft Exchange для указания источника аутентификации, когда отправитель представляется системе.
X-OriginalArrivalTime	В Microsoft Exchange этот заголовок содержит информацию о времени прибытия сообщения на сервер.
X-Forwarded-For	Используется в сетях, где сообщение проходит через промежуточные серверы, чтобы указать список IP-адресов, через которые оно прошло.

X-Originating-IP	Содержит IP-адрес отправителя. Этот заголовок может быть использован для идентификации возможного источника письма.
X-AntiAbuse	Может содержать информацию о действиях, предпринятых системой для предотвращения злоупотреблений.

X-headers не являются стандартными и могут различаться в зависимости от почтового сервера или клиента электронной почты. Некоторые из них могут быть полезными для анализа и фильтрации сообщений, в то время как другие могут использоваться для внутренних целей или же могут быть добавлены сторонними службами для слежения за потоком сообщений.

Администраторы систем электронной почты, разработчики и аналитики могут использовать X-headers для отслеживания и анализа трафика электронной почты, но их присутствие или отсутствие обычно не влияет на отображение письма в клиенте электронной почты для конечного пользователя.

Почтовые логи, которые можно проанализировать

Получение почты (SMTP-логи):

- Записи о входящих соединениях с другими почтовыми серверами.
- Информация о отправителях и получателях электронных писем.
- Данные о передаче электронных писем между серверами.

Отправка почты (SMTP-логи):

- Информация о исходящих соединениях с почтовыми серверами.
- Детали отправляемых писем, такие как отправитель, получатель, время отправки.
- Доставка почты (POP/IMAP-логи)

Фильтрация и обработка спама (спам-логи):

- Журналы обнаружения и блокировки потенциально нежелательной почты.
- Информация о действиях антиспам-фильтров.

Аутентификация и безопасность (логи безопасности):

- Записи об успешных и неудачных попытках входа в почтовый ящик.
- Информация о попытках аутентификации и блокировках при нарушении правил безопасности.

Журналы ошибок (error logs):

- Информация о любых ошибках, происходящих на сервере.
- Ошибки доставки писем или сбои в работе почтовой системы.

Журналы производительности (performance logs):

- Данные о загрузке сервера и производительности.
- Статистика использования ресурсов, таких как процессор, память и дисковое пространство.

Журналы обновлений и конфигурации:

- Записи об изменениях в конфигурации почтового сервера.
- Информация об обновлениях программного обеспечения.

Revision #2
Created 24 October 2025 18:08:04 by Admin
Updated 25 October 2025 07:23:45 by Admin