

?????????? ?????????????? DLL hijacking

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.ru/kuma/4.2/304384>

Для работы этой функции KUMA требуется:

- Лицензия с модулем AI
- Доступ по KSN

Перехват библиотеки DLL работает во время обогащения событий, поэтому его можно настроить либо на стороне сборщика (базовые события), либо на стороне коррелятора (коррелированные события). Рекомендуется использовать последний метод, поскольку потому что это позволяет эффективно управлять производительностью и нагрузкой на стороны KUMA и KSN

Как это работает с коррелятором:

1. На конечной точке настроен Sysmon + KUMA Agent или EDR Expert Agent , который отправляет телеметрию в KUMA
2. Сборщик успешно нормализует данные (включая хэши, пути к файлам, имена процессов) и пересылает их дальше для хранения и коррелятора
3. Коррелятор запускает правило корреляции, которое запускает событие корреляции с соответствующими данными, которые могут быть дополнительно обогащены с помощью KSN
4. KSC проверяет индикаторы и отправляет обратно вердикт, который хранится в поле

KL_AI_DLLHijackingCheckResult:

- 0- Не классифицирован. Чтобы получить статус, вам необходимо повторно отправить запрос.
- 1 - Неизвестно. На момент получения статуса библиотека не считается вредоносной
- 2 - Подозрительно. При получении такого результата выдается предупреждение, если у вас настроено соответствующее правило корреляции.
- 3 - Ошибка. Статус "Неисправен" указывает на более высокую вероятность обнаружения перехвата библиотеки DLL, чем статус "Подозрительно"

????????? ? ???????? Agent EDR

1. Убедитесь, что в SIEM поступает телеметрия KEDR

Результаты запроса

TSV

| TenantID | Timestamp | Name | DeviceVendor | DeviceAddress | DeviceProduct |
|----------|-------------------------|-------------------|--------------|---------------|---------------|
| Main | 02.07.2026 14:40:00.463 | File change | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | Process | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | Process terminate | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | File change | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | Process | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | Process | Kaspersky | 10.68.85.129 | EDR |
| Main | 02.07.2026 14:40:00.463 | Process | Kaspersky | 10.68.85.129 | EDR |

2. Лицензия KUMA поддерживает модуль AI

Лицензия

Kaspersky Unified Monitoring and Analysis Platform with Netflow supp... 351 д

Доступный EPS 500 Текущий EPS в день 9 Дата истечения срока действия Срок

Модули

- AI
- GosSOPKA
- NetFlow

3. Перейдите в **Ресурсы** -> **Правила Обогащения** -> **Создать**

Заполните поля:

- Название - DLL Hijacking
- Тенант
- Тип источника данных - проверка DLL Hijacking

4. В разделе **Сопоставление** в редактировании правила обогащения установите поля событий

Сопоставление

| + Добавить | | Удалить | |
|----------------------------|-------------|-------------------------|--------------------------|
| Поле KUMA | | Поле DLL Hijacking | |
| <input type="checkbox"/> | OldFileHash | хеш файла DLL (md5) | <input type="checkbox"/> |
| <input type="checkbox"/> | OldFilePath | путь до файла DLL | <input type="checkbox"/> |
| <input type="checkbox"/> | FileHash | хеш процесса (md5) | <input type="checkbox"/> |
| <input type="checkbox"/> | FilePath | путь до процесса | <input type="checkbox"/> |
| <input type="checkbox"/> | OldFileName | имя файла DLL | <input type="checkbox"/> |
| <input type="checkbox"/> | FileName | имя процесса | <input type="checkbox"/> |

5. В разделе **Параметры фильтра** в редактировании правила обогащения выберите корбочный фильтр - **[OOTB] Events for DLLHijacking enrichment. Filter for correlator**

Параметры фильтра

Фильтр* [OOTB] Events for DLLHijacking enrichment. Filter for correlator

[Конструктор](#) [</> Код](#)

[ИЛИ](#) [+ Добавить условие](#) [+ Добавить группу](#)

[И](#) [+ Добавить условие](#) [+ Добавить группу](#)

- Если e: **Type** = 3
- Если e: **DeviceEventCategory** = module
- Если не e: **EventOutcome** = true
- Если не e: **FilePath** = <Пустая строка>

6. Добавьте созданное правило обогащения на коррелятор для этого перейдите в **Ресурсы - > Корреляторы**, откройте нужный и в параметрах редактирования:

Общие

Глобальные переменные

Корреляция

Обогащение 1

Реагирование

Маршрутизация

Проверка параметров

Обогащение

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Общие
✕

| | |
|--|--|
| Правило обогащения | DLL Hijacking (correlator) 2 |
| Тип источника данных* | проверка DLL Hijacking |
| Максимальный размер кэша* ⓘ | 128 |
| Обработчики | 0 |
| Максимальное количество событий в очереди обогащения ⓘ | 1000000 |
| Выполнять повторный запрос ⓘ | <input checked="" type="checkbox"/> |
| Создавать дубликаты событий ⓘ | <input checked="" type="checkbox"/> |
| Количество запросов* ⓘ | 10 |
| Интервал запросов* ⓘ | 1 |
| Размер буфера* ⓘ | 10240 |
| Прокси-сервер | Создать |

3 Сохранить

Сохранить с комментарием

Отмена

7. Создайте правило корреляции **Ресурсы -> Корреляторы -> Корреляция -> в редактировании коррелятора -> Добавить**

Заполните параметры в разделе **Общие**:

- Название
- Тип - Simple
- наследуемые поля - FileName
- Уровень важности - высокий

в разделе **Селекторы**:

Параметры Локальные переменные

Параметры фильтра

Фильтр* Создать

Сохранить фильтр

Конструктор </> Код

И ▾ + Добавить условие + Добавить группу

Если e: N.KL_AI_DLLHijackingCheckResult > 1

В разделе **Действия**

Редактирование правила корреляции

Общие Селекторы **Действия** Сервисы Исключения

ⓘ В ресурсе типа simple может быть только один триггер: На каждом событии. Он активируется каждый раз, когда срабатывает селектор.

- В дальнейшую обработку
- В коррелятор
- Не создавать алерт

в разделе **Сервисы** привяжите правило корреляции к коррелятору

8. Обновите параметры коррелятора через **Ресурсы -> Активные сервисы**

9. В результате запуска вредоносной библиотеки в системе сформируется алерт, в базовом событии добавиться вердикт о вредоносности

Уровень важности: Высокий Назначить: Не назначено Закрыть алерт Создать инцидент Привязать

Информация об алерте

| | | |
|--------------------------------------|---------------------|--|
| Уровень важности правила корреляции | Первое появление | Тенант |
| Высокий | 24.06.2026 15:57:43 | Main |
| Наивысшая важность категории активое | Последнее появление | Правило корреляции |
| Средний | 25.06.2026 14:26:04 | Demo 3 - DLL Hijacking detection (correlator-based enrichment) |

Идентификатор алерта
3e1d282f-7c0f-48ea-b498-89a922872637

Связанные события

| Время ↓ | Информация о событии | Тенант |
|------------------------------------|---|--------|
| 25.06.2026 14:26:04 | FileName: notepad++.exe | Main |
| 25.06.2026 14:25:58 | EndTime: 25.06.2026 14:24:06, Message: Module NppExport.dll was loaded by C:\Program Files\Notepad++\notepad++.exe on winSrv-test-KUMA.truecompany.local, DeviceAddress: 10.68.85.140, DeviceAssetID: 7e2a9fb7-2220-4803-bcd0-1a01d551c949, DeviceDnsDomain: truecompany.local, DeviceEventCategory: module, DeviceExternalID: windows, DeviceHostName: winSrv-test-KUMA.truecompany.local, DevicePayloadID: module_loading_without_standard_metadata, DeviceProduct: EDR | Main |
| Найти в событиях 1 | | |
| 24.06.2026 15:57:43 | FileName: notepad++.exe | Main |

Информация о событии

```
ParentFilePath: C:\Windows
ParentIntegrityLevel: I2288
ParentLogonType: 1
ParentMdi: 05181a5ac4197d6c5c02ace6070af234
ParentOriginalFileName: EXPLORER.EXE
ParentSha256: 64798a2e4448a395956044ae925489715cd-c5f76
0e92a68b991350ba907750
ParentSignatureCheckResult: true
ParentSignatureSubjectName: Microsoft Windows
ParentStartupParameters: C:\Windows\Explorer.EXE
ParentSystemPid: 4536
ParentUserName: WINSRV-TEST-KUM\Администратор
ProcessCreationFlags: 1
ProductName: Notepad++
ProductVendor: Don HO don.ho@free.fr
Sw2Timestamp: 1782349560000000
Timestamp: 1782386646553000
Umlid: 6af0942-7a1b-c153-5667-0f271499fd5
UniqueParentId: 4937843353401698572
UniquePid: -675946656685035379
Version: 4
```

Поля расширенной схемы событий

N.KL_AI_DLLHijackingCheckR 2 (Подозрительная) **есть**

Исходное событие Форматировать

```
{
  "AccountProperties": "285873023222672",
  "AccountType": 1,
  "AgentVersion": "12.11.0.637",
  "CurrentDirectory": "C:\Program Files\Notepad++\",
  "DllCreationTime": "177564254724000",
  "DllFileAttributes": 32,
  "DllFileDescription": "",
  "DllFileType": 5,
  "DllFullName": "C:\Program Files\Notepad++\plugins\NppExport\NppExport.dll",
  "DllMd5": "12c42418c845411eba4a7a9b2e636c73",
  "DllModificationTime": "177564078047000",
  "DllName": "NppExport.dll",
  ...
}
```

Revision #8

Created 2026-07-02 11:33:08 UTC by lerat

Updated 2026-07-03 11:30:22 UTC by lerat