

# Оценка покрытия матрицы MITRE ATT&CK

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

Статья онлайн-справки «Покрытие матрицы MITRE ATT&CK»:

<https://support.kaspersky.ru/kuma/4.0/272743>

Если вы хотите оценить покрытие матрицы MITRE ATT&CK (<https://attack.mitre.org/>) корреляционными правилами, используемыми в KUMA («коробочными» и/или пользовательскими), выполните следующие шаги:

- Загрузите справочник техник MITRE из официального репозитория MITRE ATT&CK и импортируйте справочник техник MITRE в KUMA.
- Привяжите техники MITRE к правилам корреляции.
- Экспортируйте правила корреляции в MITRE ATT&CK Navigator.
- В результате вы сможете визуально оценить покрытие матрицы MITRE ATT&CK.

Загрузить справочник техник MITRE можно из официального репозитория MITRE ATT&CK: <https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json>

KUMA поддерживает работу только со справочником техник MITRE ATT&CK версии 14.1.

## Импорт справочника техника MITRE

Чтобы импортировать список техник MITRE ATT&CK:

- В веб-интерфейсе KUMA перейдите в раздел **Параметры** → **Другое** → **Общие**.
- В разделе **Настройки списка техник MITRE** нажмите на кнопку Импортировать из файла.

Кaspersky Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панели мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры 1

Доступ

Интеграции

Другое 2

Состояние источников

Метрики

Общее 3

Алерты

Лицензия

Инциденты

Обновление репозитория

Активы

Мониторинг сервисов

Теги

Поля расширенной схемы событий

Пусто

### Настройка GeoIP

+ Импортировать из файла Экспортировать

### Настройки списка техник MITRE

Список техник MITRE. Для получения подробной информации смотрите [онлайн-справку](#).

+ Импортировать из файла Просмотреть список

4

### Параметры подключения к SMTP-серверу

Очистка очереди уведомлений

Состояние ☒

Адрес сервера\*

Порт\*

Секрет\*

Псевдоним сервера Ядра KUMA ⓘ

От кого\*

Выключить уведомления мониторинга ☐

Регулярность уведомлений мониторинга\*

Сохранить

- В окне выбора файлов выберите скачанный справочник техник MITRE ATT&CK и нажмите на кнопку **Открыть**.

Список техник MITRE ATT&CK будет импортирован в KUMA. Вы можете увидеть список импортированных техник и версию справочника техник MITRE ATT&CK, нажав на кнопку **Просмотреть список**.

## Техники MITRE

Версия : 14.1



| ID тактики | Название тактики     | ID техники | Название техники                     |
|------------|----------------------|------------|--------------------------------------|
| TA0005     | defense-evasion      | T1055.011  | Extra Window Memory Injection        |
| TA0004     | privilege-escalation | T1055.011  | Extra Window Memory Injection        |
| TA0002     | execution            | T1053.005  | Scheduled Task                       |
| TA0003     | persistence          | T1053.005  | Scheduled Task                       |
| TA0004     | privilege-escalation | T1053.005  | Scheduled Task                       |
| TA0005     | defense-evasion      | T1205.002  | Socket Filters                       |
| TA0003     | persistence          | T1205.002  | Socket Filters                       |
| TA0011     | command-and-control  | T1205.002  | Socket Filters                       |
| TA0009     | collection           | T1560.001  | Archive via Utility                  |
| TA0008     | lateral-movement     | T1021.005  | VNC                                  |
| TA0002     | execution            | T1047      | Windows Management Instrumentation   |
| TA0009     | collection           | T1113      | Screen Capture                       |
| TA0005     | defense-evasion      | T1027.011  | Fileless Storage                     |
| TA0003     | persistence          | T1037      | Boot or Logon Initialization Scripts |
| TA0004     | privilege-escalation | T1037      | Boot or Logon Initialization Scripts |

Отмена

Чтобы проверить отображение списка техник MITRE ATT&CK для «коробочных» правил корреляции [OOTB] SOC Content - RU for KUMA 3.2:

- Перейдите в **Ресурсы** → **Правила корреляции** и выберите слева папку **Main**.
- Убедитесь, что в столбце **Техники MITRE** отображается **ID Техники**.

## Правила корреляции



+

Добавить папку

► Main

1

+

Добавить

Дублировать

Удалить

Привязать к коррелятору

Поиск...

| Последнее обновление | Создал        | Название пакета                    | Описание                                                                                          | Техники MITRE                           |           |           |           |
|----------------------|---------------|------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------|-----------|-----------|-----------|
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Рабочие станции являются персональными рабочими местами пользователей                             | TA0002: T1059.003 Windows Command Shell |           |           |           |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Злоумышленник может выполнить удаленный вредоносный код с помощью процесса rundll32.exe.          | T1059.003                               | T1218.011 | T1071.001 | T1071.002 |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Обнаруживает действия по копированию/созданию исполняемых файлов на сетевых...                    | T1080                                   |           |           |           |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Обнаруживает выполнение скрипта Install-PTASpy.ps1, внедрение PTASpy.dll через...                 | T1556                                   | T1556.007 | T1556     | T1556.007 |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Злоумышленники могут часто использовать технику внедрения в легитимные процессы с целью...        | T1055                                   | T1055     |           |           |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Правило направлено на обнаружение подозрительной активности с использованием C...                 | T1059.008                               |           |           |           |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Обратный shell представляет собой командную оболочку, запущенную на одном хосте,...               |                                         |           |           |           |
| 28.02.2025 17:25:10  | Administrator | [OOTB] SOC Content - RU for KUM... | Злоумышленники могут создавать артефакты (объекты, ВПО и т.д.), которые могут быть использован... | T1055                                   | T1055     | T1587     |           |

- Если столбец **Техники MITRE** остается пустым, выполните повторный импорт пакета **[OOTB] SOC Content - RU for KUMA 3.2** из репозитория (см. Раздел [Импорт ресурсов из репозитория](#)).

## Привязка техник MITRE к правилам корреляции

Чтобы привязать техники MITRE ATT&CK к правилам корреляции (на примере созданного правила корреляции из Раздела [Создание правила корреляции типа Standard](#)):

- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Правила корреляции**.
- В панели слева выберите ранее созданную папку для пользовательских правил корреляции и откройте окно редактирования правила корреляции, нажав на имя правила корреляции.

## Правила корреляции



+ Добавить папку

▼ Main

- ▶ KUMA Packages
- LAB
- PoC 1
- TEST

+ Добавить

Дублировать

Удалить

Привязать к коррелятору

Поиск...

| <input type="checkbox"/> | Название                                                          | ▼ Тип    | ▼ Последнее обновление | ▼ Создал      |
|--------------------------|-------------------------------------------------------------------|----------|------------------------|---------------|
| <input type="checkbox"/> | Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA 2 | standard | 26.02.2025 14:07:07    | Administrator |
| <input type="checkbox"/> | Неудачная попытка входа в веб-интерфейс KUMA                      | simple   | 26.02.2025 12:36:52    | Administrator |

- В окне редактирования правила корреляции во вкладке **Общие** нажмите на поле **Техники MITRE** откроется список доступных техник.
- Для удобства поиска доступен фильтр: в поле можно ввести название техники, ID техники или тактики. Для привязки к правилу корреляции доступна одна или несколько техник MITRE ATT&CK. Так как созданное правило относится к технике Brute Force и производится многократная попытка подобрать пароль введите в поле саб-технику **Password Guessing** (<https://attack.mitre.org/techniques/T1110/001/>).

# Редактирование правила корреляции

1

ОбщиеСелекторыДействияКорреляторы

Название\*

Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUM/

Тенант\*

Main

Тип\*

standard

Группирующие поля\* ⓘ

DeviceAction ×SourceAddress ×SourceUserName ×EventOutcome ×

Время жизни контейнера, сек.\*

60

Уникальные поля ⓘ

Частота срабатываний ⓘ

0

Политика хранения базовых событий

all

Уровень важности

Сортировать по

Описание

Техники MITRE

password 2

Сохранить

Отмена

- Нажмите на кнопку **Сохранить**.

Техника MITRE ATT&CK будет привязана к правилу корреляции. Убедитесь, что в столбце **Техники MITRE** отображается **ID Техники**.

|                  |                   |                                                                 |               |                 |          |          |
|------------------|-------------------|-----------------------------------------------------------------|---------------|-----------------|----------|----------|
| + Добавить папку |                   | + Добавить    Дублировать    Удалить    Привязать к коррелятору |               |                 |          | Поиск... |
| ▼ Main           | ...               | Последнее обновление                                            | Создал        | Название пакета | Описание |          |
|                  | ... KUMA Packages | 28.02.2025 17:45:15                                             | Administrator |                 |          |          |
|                  | ... LAB           | 26.02.2025 12:36:52                                             | Administrator |                 |          |          |
| ...              | PoC               |                                                                 |               |                 |          |          |
| ...              | TEST              |                                                                 |               |                 |          |          |

# Экспорт правил корреляции в MITRE ATT&CK Navigator

Чтобы оценить покрытие матрицы MITRE ATT&CK корреляционными правилами, используемыми в KUMA («коробочными» и/или пользовательскими), выполните следующие шаги:

Предварительно выполните привязку техник MITRE к правилам корреляции, созданным самостоятельно.

- В веб-интерфейсе KUMA перейдите в раздел **Ресурсы → Правила корреляции**.
- В правом верхнем углу нажмите на кнопку .
- В раскрывающемся списке нажмите на кнопку **Экспортировать в MITRE ATT&CK Navigator**.

## Правила корреляции

+ Добавить папку

+ Добавить
Дублировать
Удалить
Привязать к коррелятору

Импортировать ресурсы  
Экспортировать ресурсы  
Экспортировать в MITRE ATT&CK Navigator

Main

:: KUMA Packages

:: LAB

:: PoC

:: TEST

| Название                                                                                   | Тип      | Последнее обновление | Создал        |
|--------------------------------------------------------------------------------------------|----------|----------------------|---------------|
| <input type="checkbox"/> Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA   | standard | 28.02.2025 17:41:51  | Administrator |
| <input type="checkbox"/> R032_Вход на рабочую станцию под разными учетными записями        | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R291_03_Вызов внешних ресурсов для системных приложений Window... | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R285_03_Создание исполняемых файлов на сетевое шаре               | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R083_11_Подозрительная активность, связанная с PTASpy.dll (ps)    | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R087_01_Внедрение в процесс (KATA)                                | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R435_01_Выполнение подозрительных команд на сетевых устройствах   | simple   | 28.02.2025 17:25:10  | Administrator |
| <input type="checkbox"/> R286_Подозрение на запуск обратного shell                         | simple   | 28.02.2025 17:25:10  | Administrator |

- В открывшемся окне выберите правила корреляции, которые вы хотите экспортировать (выберите все для оценки покрытия всеми правилами корреляции).

## Выбор правил корреляции



- ☒ Main
- ☒ KUMA Packages

1
- ☒ PoC

Нажмите на кнопку **ОК**.

- Файл с экспортированными правилами будет загружен на ваш компьютер в формате json.
- Загрузите файл с вашего компьютера в MITRE ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/>) для оценки покрытия матрицы MITRE ATT&CK.



## MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme](#)

Create New Layer

Create a new empty layer

⌵

Open Existing Layer

Load a layer from your computer or a URL

⌵

Upload from local

OR

Load from URL

>

Create Layer from Other Layers

Select layers to inherit properties from

⌵

Create Customized Navigator

Create a hyperlink to a customized ATT&CK Navigator

⌵

### KUMA Coverage of MITRE TECHNIQUES

| Reconnaissance                                                                                                                                                                                                                                                                                                                            | Resource Development                                                                                                                                                                                                                                                                                                                                                 | Initial Access                                                                                                                                                                                                                                                                                                                                      | Execution                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Persistence                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Privilege Escalation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Defense Evasion                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Credential Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Discovery                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Lateral Movement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Collection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Command and Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Exfiltration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> <div>Active Directory (10)</div> | <div>Acquire Accounts (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> <div>Acquire Information (10)</div> | <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> <div>Content Injection (10)</div> | <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> <div>Cloud Administration Command (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> | <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> <div>Cloud Configuration Modification (10)</div> |

В результате будет отображено покрытие MITRE ATT&CK. При наведении курсора на конкретную технику или суб-технику будет отображено, покрывающее ее правило.

| Reconnaissance<br>10 techniques          |    | Resource<br>Development<br>8 techniques                                                                 | Initial Access<br>10 techniques   |
|------------------------------------------|----|---------------------------------------------------------------------------------------------------------|-----------------------------------|
| Active Scanning (1/3)                    | II | Acquire Access                                                                                          | Content Injection                 |
| Gather Victim Host Information (0/4)     |    | Acquire Infrastructure (0/8)                                                                            | Drive-by Compromise               |
| Gather Victim Identity Information (0/3) |    | Compromise Accounts (0/3)                                                                               | Exploit Public-Facing Application |
| Gather Victim Network Information (0/6)  |    | Compromise Infrastructure (7/7)                                                                         | External Remote Services          |
| Gather Victim Org Information (0/4)      |    | Develop Capabilities (3/4)                                                                              | Hardware Additions                |
|                                          |    | Spearphishing Attachment A (T1598.002) (4/3)                                                            | Phishing (2/4)                    |
| Phishing for Information (2/4)           | II | Score:1<br>Rule: R402_05 Попытка отправки письма с вредоносным файлом нескольким внутренним получателям | Reputation Through Remote Med     |
|                                          | 1  | Stage Capabilities (1/6)                                                                                | Supply Chain Compromise           |
| Search Closed Sources (0/2)              | II |                                                                                                         | Trusted Relationship              |
| Search Open Technical Databases (0/5)    | II |                                                                                                         | Valid Accounts (3/4)              |
| Search Open Websites/Domains (0/3)       | II |                                                                                                         |                                   |
| Search Victim-Owned Websites             |    |                                                                                                         |                                   |