Community PlayBooks: Атаки через третьих лиц

Это кибератака, при которой злоумышленник компрометирует данные целевой организации **через уязвимого поставщика, партнёра или стороннего подрядчика**, имеющего доступ к её системам.

Компания MITRE разделяет угрозы через третьих лиц на **два типа**:

- T1199 (Trusted Relationship) - атаки через доверительные отношения. Злоумышленник пользуется уже имеющимися доверенными доступами. Например, компрометация поставщика услуг (MSP), подрядчика или партнера, имеющего VPN-доступ к цели. Обычно затрагивает конкретную целевую организацию (и другие организации, использующие то же доверенный доступ);
- T1195 (Supply Chain Compromise) - атаки через цепочку поставок. Злоумышленник встраивает вредоносную составляющую в продукт / сервис / репозиторий / ПО предоставляемый производителем до его получения потребителем. Атака может затронуть всех последующих потребителей скомпрометированного продукта / услуги. T1195 содержит три подтехники:
    - T1195.001 - Compromise Software Dependencies and Development Tools
    - T1195.002 - Compromise Software Supply Chain
    - T1195.003 - Compromise Hardware Supply Chain

Статистика: В 2023 году в США было зафиксировано 242 атаки через третьих лиц, что на 115% больше, чем в 2022 году. А в 2025 году атаки достигли ~30% от всех инцидентов безопасности согласно *Verizon 2025 Data Breach Investigations Report (DBIR).* Примеры атак можно посмотреть в соответствующей технике на сайте MITRE ATT&CK.

Процесс реагирования

1. Подготовка

- **Меры безопасности**
  - Внедрите строгий контроль доступа для всех сторонних поставщиков и партнеров;
  - Регулярно проводите аудит безопасности сторонних систем, подключенных к вашей сети;
  - Сегментируйте сеть для минимизации горизонтальных перемещений от скомпрометированных сторонних систем;
  - Используйте многофакторную аутентификацию (MFA) для всех внешних подключений;
  - Отслеживайте риски, связанные с цепочкой поставок и третьими сторонами, с помощью потоков данных об угрозах (Threat Intelligence).
- **Учет активов**
  - Ведите подробный учет всех сторонних подключений, систем и уровней доступа;
  - Документируйте критически важные активы и их зависимости от сторонних систем.
- **Контроль доступов**
  - Обеспечьте минимальные привилегии для всех сторонних учётных записей и регулярно проверяйте
  - права доступа;
  - Отключайте учётные записи сразу после расторжения договора или бездействия.
- **Инструменты мониторинга**
  - Настройте SIEM систему для автоматического обнаружения событий, таких как:
    - Необычные подключения с IP – адресов подрядчика;
    - Передача больших объемов данных и других шаблонов утечки данных;
    - Аутентификация с нетипичных устройств, местоположений или не рабочее время;
  - Разверните EDR устройства для выявления подозрительной активности на устройствах, получающих доступ к сети.
- **Тренировки по инцидентам**
  - Моделируйте сценарии, в которых сторонний поставщик или партнёр подвергается атаке, для проверки обнаружения и реагирования;
  - Обучайте сотрудников распознавать индикаторы атак через третьи лица.

2. Обнаружение

- **Определение индикаторов угроз**
  - **Алерты**
    - SIEM: Аномальное поведение из систем подрядчиков;
    - IDP/IPS: Обнаружение необычных передач файлов или попыток повышения привилегий;
    - EDR: Признаки горизонтального перемещения, исходящие от доверенного стороннего соединения.
  - **Логи**
    - VPN: Нетипичные входы от сторонних пользователей;
    - Логи облачных внезапные изменения политик доступа или необычные вызовы API.
- **Определение факторов риска**
  - **Общие риски**
    - Распространение вредоносных программ в уязвимые системы;
    - Эксфильтрация критически важных или конфиденциальных данных;
    - Внедрение программ-вымогателей или вредоносного ПО.
  - **Специфичные для компании риски**
    - Утечка данных клиентов через поставщиков;
    - Сбой в работе из-за нарушения работы систем цепочки поставок.
- **Сбор информации**
  - Анализируйте сетевой трафик на предмет аномальных закономерностей между внутренними системами и сторонними конечными точками;
  - Проверяйте журналы аутентификации на предмет подозрительной активности сторонних учётных записей.
- **Категорирование**
  - Эксплойты в цепочке поставок: Компрометация поставщика с целью проникновения в организацию;

- Переключение партнёров: Получение доступа через скомпрометированные сторонние учётные записи;
- Неправильные конфигурации облака: Эксплуатация интеграций сторонних облачных сервисов.

- **Это целевая атака (APT)?**
  - Использование легитимных учётных данных, украденных у третьих лиц;
  - Сложное вредоносное ПО или инструменты для горизонтального перемещения;
  - Скоординированные атаки, направленные на несколько организаций через одного поставщика.

3. Анализ

- **Подтверждение**
  - Воспроизведите подозрительную активность в песочнице, для подтверждения вредоносного поведения;
  - Проверьте логи и коммуникации с третьей стороной на предмет наличия признаков компрометации.
- **Определение индикаторов компрометации (IOC)**
  - Необычное время входа в систему или IP-адреса, связанные со сторонними учётными записями;
  - Подозрительные вызовы API или системные команды.
- **Извлечение индикаторов компрометации (IOC)**
  - Документирование вредоносных IP-адресов, URL-адресов, хэшей файлов и скомпрометированных учётных записей.
- **Отправка информации партнёрам**
  - Обмен индикаторами компрометации (IOC) с пострадавшими третьими сторонами и соответствующими отраслевыми группами.
- **Сканирование предприятия**
  - Проведение комплексного сканирования на предмет горизонтального перемещения или вредоносного ПО в сети;
  - Аудит разрешений (прав) для всех сторонних учётных записей и подключений.

4. Сдерживание и устранение

- **Сдерживание угрозы**
  - Отключите скомпрометированные сторонние учётные записи или подключения;
  - Заблокируйте вредоносные IP-адреса и домены на межсетевых экранах или системах веб-фильтрации.
- **Устранение первопричины**
  - Взаимодействуйте с пострадавшей стороной для устранения уязвимостей в её системах;
  - Устраните все уязвимости, эксплуатируемые в вашей среде;
  - Пересмотрите и усильте политики сегментации сети и доступы.
- **Проверка**
  - Проверьте подключения и журналы активности, чтобы убедиться в отсутствии дальнейшей вредоносной активности;
  - Проведите учения Red Teaming / пентесты для подтверждения эффективности мер по снижению риска.

5. Восстановление

- **Восстановление процессов**
  - Возобновите доступ третьих лиц только после проверки безопасности их систем;
  - Восстановите затронутые системы или данные из резервных копий.
- **Информирование**
  - При необходимости уведомляйте заинтересованные стороны, включая клиентов, партнеров и регулирующие органы;
  - Предоставьте подробный отчет после инцидента.

6. Извлеченные уроки

- Проведите тщательный анализ после инцидента, чтобы понять, каким образом была скомпрометирована третья сторона;
- Обновите контракты и политики для обеспечения более строгих требований к кибербезопасности для поставщиков и партнеров;
- Расширьте возможности мониторинга действий третьих лиц;
- Обучите сотрудников и пользователей третьих лиц передовым практикам кибербезопасности.

Примеры логики для обнаружения атаки

Полезные запросы можно найти на странице KB KUMA Community: ссылка

1. Использование доверенного аккаунта для админ-команд

```
EVENTS = SELECT FROM audit_logs WHERE user IN [доверенные_аккаунты] AND action IN [CREATE USER, ALTER ROLE, DROP DATABASE]
IF EXISTS(EVENTS) THEN ALERT "Доверенный аккаунт выполняет административные действия"
```

2. Массовые подключения от доверенного аккаунта

```
EVENTS = SELECT FROM connection_logs WHERE user = trusted_service GROUP BY time_window(5 минут)
IF COUNT(EVENTS) > 50 THEN ALERT "Аномальное количество подключений доверенного аккаунта"
```

3. Подключение доверенного аккаунта с нового хоста

```
KNOWN_HOSTS = SELECT DISTINCT hostname FROM connection_logs WHERE user = trusted_service
EVENTS = SELECT FROM connection_logs WHERE user = trusted_service AND hostname NOT IN KNOWN_HOSTS
IF EXISTS(EVENTS) THEN ALERT "Доверенный аккаунт используется с нового хоста"
```

4. Изменение кода приложения в CI/CD pipeline

```
EVENTS = SELECT FROM cicd_logs WHERE action IN [modify, replace, inject] AND file_type IN [source_code, build_scripts]
AND user NOT IN [список CI/CD сервисных аккаунтов]
IF EXISTS(EVENTS) THEN ALERT "Неавторизованное изменение кода в процессе сборки"
```

5. Установка неподписанных бинарников

```
EVENTS = SELECT FROM software_install_logs WHERE signature_status = "unsigned"  AND source_url NOT IN [trusted_repos]
IF EXISTS(EVENTS) THEN ALERT "Установлено неподписанное ПО"
```

6. Внезапное изменение зависимостей

```
EVENTS = SELECT FROM package_manager_logs WHERE dependency_name IN [critical_libs] AND version != expected_version
AND source_url NOT IN [trusted_sources]
IF EXISTS(EVENTS) THEN ALERT "Подмена зависимостей в цепочке поставки"
```

7. Использование доверенного аккаунта для доступа к чувствительным таблицам

```
EVENTS = SELECT FROM query_logs WHERE user IN [доверенные_аккаунты] AND table_name IN [финансовые, персональные данные]
IF EXISTS(EVENTS) THEN ALERT "Доверенный аккаунт обращается к критическим данным"
```

8. Изменение хэшей исполняемых файлов

```
EVENTS = SELECT FROM file_integrity_logs WHERE file_path IN [bin/, lib/] AND current_hash != baseline_hash
IF EXISTS(EVENTS) THEN ALERT "Подмена бинарников в среде исполнения"
```

9. Попытка внедрения стороннего плагина разработчиком

```
EVENTS = SELECT FROM developer_activity_logs WHERE action = "install plugin"  AND plugin_source NOT IN [официальный_маркетплейс]
IF EXISTS(EVENTS) THEN ALERT "Разработчик установил плагин из неизвестного источника"
```

10. Вход с доверенной учетной записи в нерабочее время

```
EVENTS = SELECT FROM connection_logs WHERE user IN [доверенные_аккаунты]
IF event_time NOT IN [рабочие часы: 08:00-20:00, Пн-Пт] THEN ALERT "Вход с доверенной учетной записи в нерабочее время"
```