МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ   
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»   
(МОСКОВСКИЙ ПОЛИТЕХ)**

Отчёт по практической работе

Выполнил:

студент учебной группы 241-351, Деген С.В.

Проверил:

Шорников Андрей Валерьевич

Москва, 2024 г.

**Матрица “MITRE ATT&CK”**

Матрица MITRE ATT&CK содержит в себе паттерны поведения киберпреступников. Матрицу можно использовать для подробного анализа кибер-атак, а также для разработки стратегии защиты информации.

**Основные аспекты MITRE ATT&CK:**

1. База знаний
   1. Тактики - ресурс предоставляет доступ к уже известным целям злоумышленников, которые они пытаются достич методом взлома
   2. Техники - каждая из тактик имеет различные методы взлома для получения информации необходимой для следующего этапа атаки. Так на этапе “Разведка” злоумышленники собирают информацию для этапа “Первоначальный доступ”
   3. Подтехники - в данном разделе указаны варианты и детали осуществления техники
2. Применение
   1. Оценка угрозы - матрицу можно использовать для исследования собственной системы и её уязвимостей
   2. Разработка защитных мер - знание тактик и методов злоумышленников поможет разработать более эффективную систему защиты, а также поспособствует в обучении молодых сотрудников
   3. Тестирование и имитация атак - используя матрицу, можно в точности разработать сценарий атаки для проверки эффективности защиты
3. Сообщество
   1. Матрица MITRE ATT&CK пополняется исходя из отчётов о кибератаках, тем самым матрица остаётся актуальной и обновляется за счёт сообщества кибербезопасности
4. Интеграция
   1. Матрица MITRE ATT&CK доступна для интеграции в любые утилиты и платформы, что помогает автоматизировать обнаружение и реагирования на угрозы
5. Разделы
   1. Enterprise - раздел содержащий информацию о тактиках и техниках взлома направленных на корпоративные системы
   2. Mobile - раздел содержащий информацию о тактиках техниках взлома направленных на мобильные устройства
   3. Cloud - раздел содержащий информацию о тактиках и техниках взлома направленных на облачные среды
   4. Pre-ATT&CK - раздел описывающий действие злоумышленников на этапе “Разведка”, до начала непосредственной атаки

**Портал OWASP Foundation**

OWASP (Open Web Application Security Project) — это международная некоммерческая организация, её цель - улучшить безопасность программного обеспечения. Портал предоставляет доступ к различным ресурсам, инструментам, а также информации, для того, чтобы разработчики могли создавать, тестировать и поддерживать безопасность своих приложений.

**Основные аспекты OWASP:**

1. Проекты
   1. OWASP Top Ten - это список самых распространённых и критических уязвимостей за последние несколько лет. Список регулярно обновляется, что даёт разработчикам понимание от чего нужно защищаться в первую очередь
   2. OWASP ZAP (Zed Attack Proxy) - бесплатная утилита для тестирования веб-приложений на наличие уязвимостей
   3. OWASP SAMM (Software Assurance Maturity Model) - модель, которая проверяет процессы обеспечения безопасности программного обеспечения и даёт им оценку
   4. OWASP ASVS (Application Security Verification Standard) - стандарт, который предоставляет набор требований для проверки безопасности веб-приложений.
2. Ресурсы и материалы
   1. Документация - подробные руководства и документы содержащие лучшие практики, методологии и советы по проектированию безопасных приложений
   2. Инструменты - полезные утилиты в общем доступе помогающие в тестировании, анализе кода и управлении уязвимостями
   3. Обучение - ресурсы для обучения и повышения навыков в формате курсов и вебинаров
3. Сообщество
   1. У OWASP активное сообщество из специалистов высокого класса в области информационной безопасности, разработки приложений и исследований. Организация часто проводит очные мероприятия: семинары, митапы, конференции, которы помогают участникам обмениваться опытом
4. Глобальная инициатива
   1. OWASP имеет глобальное присутствие с местными проектами и главами в различных странах. Это позволяет адаптировать рекомендации и ресурсы к конкретным регионам и их потребностям.
5. Принципы безопасности
   1. Безопасность по умолчанию - это означает, что приложение должно быть безопасным по умолчанию, без дополнительных настроек
   2. Прозрачность - процессы и принципы безопасности должны быть открытыми и доступными для изучения
   3. Обучение и осведомленность - требование по обучению и осведомлению разработчиков и пользователей в вопросе безопасности.

**Разбор кибератаки на компанию "SolarWinds"**

1. Введение

В феврале 2024 года компания "SolarWinds", известная своим программным обеспечением для управления IT-инфраструктурой, вновь оказалась в центре внимания из-за новой кибератаки. На этот раз злоумышленники использовали уязвимости в обновлениях ПО для распространения вредоносного кода, что привело к компрометации данных клиентов и нарушению работы их систем.

2. Хронология событий

- 5 февраля 2024 года: Специалисты SolarWinds обнаружили подозрительную активность в своих системах обновления ПО.

- 7 февраля 2024 года: Было подтверждено, что злоумышленники внедрили вредоносный код в один из модулей обновления, который автоматически распространялся среди клиентов.

- 10 февраля 2024 года: SolarWinds выпустила экстренное обновление для устранения уязвимости и уведомила клиентов о потенциальной угрозе.

- 12 февраля 2024 года: Появились первые сообщения о компрометации данных у нескольких крупных клиентов, включая государственные учреждения и частные компании.

3. Примененные тактики, техники и процедуры (TTPs)

- Разведка (Reconnaissance, T1595): Злоумышленники заранее изучили инфраструктуру SolarWinds, чтобы выявить уязвимости в системе обновлений.

- Первоначальный доступ (Initial Access, T1195): Использование цепочки поставок (supply chain attack) для внедрения вредоносного кода через легитимные обновления ПО.

- Закрепление (Persistence, T1078): Создание скрытых учетных записей для поддержания доступа к системам.

- Обход защиты (Defense Evasion, T1562): Отключение журналирования и использование шифрования для скрытия активности.

- Доступ к учетным данным (Credential Access, T1003): Кража учетных данных администраторов для расширения контроля.

- Развертывание вредоносного ПО (Execution, T1059): Запуск скриптов для удаленного управления системами.

- Эксфильтрация данных (Exfiltration, T1041): Передача украденных данных на внешние серверы.

4. Последствия инцидента

- Для SolarWinds:

- Повторный удар по репутации после инцидента 2020 года.

- Финансовые потери из-за судебных исков и затрат на восстановление.

- Для клиентов:

- Компрометация конфиденциальных данных.

- Нарушение работы IT-систем, требующее временного отключения сервисов.

5. Меры по восстановлению и предотвращению

- Восстановление:

- SolarWinds выпустила патчи для устранения уязвимостей.

- Клиентам рекомендовано провести аудит систем и сменить учетные данные.

- Предотвращение:

- Усиление контроля за цепочкой поставок.

- Внедрение более строгих процедур проверки обновлений.

- Регулярное обучение сотрудников по вопросам кибербезопасности.