УДК 004.056.53

МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ПРИМЕРЕ ТЕХНИК МОДЕЛИ MITRE ATT&CK TA0002-TA0009

Попович А.А.

гр. 367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации

Аннотация. В материалах доклада рассматриваются основные принципы и концепции модели MITRE ATT&CK, ее структуру, основные категории тактик и техник, а также примеры использования модели в практических задачах, что позволит углубить знания о принципах кибербезопасности и методах защиты от кибератак на примере техник модели TA0002-TA0009.

Ключевые слова: модели MITRE ATT&CK, техники модели TA0002-TA0009, кибербезопасность.

Введение. В современном цифровом мире информационные системы играют ключевую роль в повседневной деятельности организаций и частных лиц. От электронной почты до онлайн-банкинга, мы все используем различные информационные системы для обмена информацией, проведения операций и ведения бизнеса. Однако вместе со всеми преимуществами, которые приносят нам информационные технологии, возникают и серьезные угрозы для информационной безопасности.

Информационная безопасность информационных систем становится все более актуальной темой в современном мире. Утечки конфиденциальных данных, кибератаки, вредоносное программное обеспечение - все это потенциальные угрозы, с которыми сталкиваются организации и частные лица. Поэтому обеспечение безопасности информационных систем становится приоритетной задачей для многих компаний и организаций.

В данном докладе рассмотрим модель нарушителя MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), которая представляет собой базу знаний, которая классифицирует различные тактики, техники и процессы, используемые злоумышленниками при проведении кибератак. Данная модель разработана командой MITRE для организации информационной безопасности и служит для лучшего понимания и анализа поведения нарушителей.

Модель MITRE ATT&CK включает более 250 тактик и техник, которые могут быть использованы при целенаправленных атаках на информационные системы и сети. Эти тактики и техники разделены на матрицы ATT&CK, каждая из которых описывает определенную цель и способы ее достижения.

Модель нарушителя MITRE ATT&CK помогает организациям и специалистам в области кибербезопасности лучше понять, какие методы и инструменты могут быть использованы злоумышленниками, и принять необходимые меры по защите от таких атак. Она также помогает при анализе угроз и разработке стратегии защиты для предотвращения инцидентов информационной безопасности.

Основная часть. MITRE ATT&CK - это модель тактик, техник и процедур (TTP), которая описывает широкий спектр методов, которые злоумышленники могут использовать при проведении атак на компьютерные системы. Вот некоторые из основных тактик, техник и процедур, входящих в модель MITRE ATT&CK:

1. Использование программной реализации: злоумышленники используют программное обеспечение для достижения своих целей, например, установка вредоносного ПО, эксплойты и обратные двери.

2. Ложные флаги: злоумышленники могут использовать ложные сигналы или информацию, чтобы запутать защитные системы и направить внимание на другую область.

3. Кража и использование учетных данных: злоумышленники могут получить доступ к учетным данным и использовать их для несанкционированного входа в системы и сети.

4. Блокировка обнаружения: злоумышленники могут применять различные методы для предотвращения обнаружения своих операций, такие как шифрование коммуникаций, маскировка вредоносного ПО и удаление следов.

5. Управление доступом: злоумышленники могут получить несанкционированный доступ к системам и сетям, используя уязвимости в процессах аутентификации и авторизации.

6. Подкармливание и обнаружение информации: злоумышленники могут

манипулировать, фальсифицировать или удалять информацию, чтобы затруднить обнаружение своей активности и следов.

7. Установка задержки и персистентности: злоумышленники могут устанавливать механизмы задержки и персистентности, чтобы продолжать свою активность после инициации атаки.

Это только некоторые из тактик, техник и процедур, рассматриваемых в модели MITRE ATT&CK. Понимание этих методов может помочь в защите компьютерных систем и сетей от атак и повысить уровень безопасности.

В рамках MITRE ATT&CK различаются различные техники, обозначенные уникальными идентификаторами. В рамках данного доклада рассмотрим техники модели TA0002-TA0009, способы их обнаружения и противодействия.

1. TA0002 - Сканирование сети:

- Обнаружение: Мониторинг сетевого трафика для обнаружения повышенной активности сканирования, особенно если замечены необычные или неподдерживаемые порты или протоколы.

2. TA0003 - Оскорбительная подготовка:

- Обнаружение: Следить за необычными или подозрительными операциями создания и попытками запуска исполняемых файлов на компьютерах в сети.

3. TA0004 - Доставка вредоносного ПО:

- Обнаружение: Использование антивирусных программ и инструментов для обнаружения вредоносных программ при доставке на конечные устройства или точки входа в сеть.

4. TA0005 - Установка вредоносного ПО:

- Обнаружение: Мониторинг активности установки программного обеспечения, особенно при обнаружении необычного или запрещенного программного обеспечения.

5. TA0006 - Запуск вредоносного ПО:

- Обнаружение: Обнаружение необычных процессов, активированных в системе, а также использование инструментов мониторинга активности процессов для обнаружения потенциально вредоносного ПО.

6. TA0007 - Получение данных:

- Обнаружение: Слежение за необычными запросами к файловым системам, базам данных или другим источникам данных, а также мониторингом активности сетевого трафика.

7. TA0008 - Коммуникации через сеть:

- Обнаружение: Использование инструментов для контроля и анализа сетевого трафика с целью обнаружения аномальной коммуникации или несанкционированной передачи данных.

8. TA0009 - Выход из системы:

- Обнаружение: Мониторинг активности пользователя, включая необычные попытки выхода из системы или переключения учетных записей, а также отслеживание активности удаленного доступа к системе [1].

Обнаружение этих техник часто осуществляется при помощи интеллектуальных систем обнаружения вторжений (IDS/IPS), анализа журналов событий, мониторинга сетевого трафика и использования специализированных инструментов для обнаружения вредоносных действий и поведения.

Противодействие техникам модели TA0002-TA0009 можно осуществлять путем следующих действий:

Обучение сотрудников: обеспечить сотрудников компании знаниями и навыками по распознаванию и предотвращению использования техник из указанных моделей.

Внедрение систем защиты: реализовать системы мониторинга и защиты, которые могут обнаружить попытки использования этих техник и предотвратить их дальнейшее применение.

Создание процедур и политик безопасности: разработать и внедрить строгие процедуры и политики безопасности, которые могут помочь предотвратить атаки при помощи указанных техник.

Систематическое обновление знаний: следить за новыми техниками и методами, которые могут быть использованы злоумышленниками, и обеспечивать периодическое обновление знаний сотрудников компании.

Сотрудничество с экспертами по кибербезопасности: в случае возникновения сомнений или необходимости принятия решения по атаке с использованием подобных техник, обращаться за помощью к специалистам в области кибербезопасности [2].

Заключение. Модели MITRE ATT&CK TA0002-TA0009 представляют собой набор тактических приемов и техник, используемых злоумышленниками в рамках кибератак. Эти модели помогают аналитикам и специалистам по кибербезопасности лучше понимать и противодействовать различным угрозам и атакам. Используя модели TA0002-TA0009, компании и организации могут анализировать свои системы и сети на предмет возможных уязвимостей и улучшать свои меры защиты. Эти модели представляют собой ценный ресурс для обучения персонала по кибербезопасности, а также для разработки стратегий противодействия угрозам в сети.

В целом, модели MITRE ATT&CK TA0002-TA0009 могут значительно повысить уровень кибербезопасности организации и помочь защитить информацию и данные от потенциальных атак и угроз. Они являются важным инструментом в борьбе с киберпреступностью и поддержании безопасности в цифровой среде.

Список литературы

1. MITRE ATT&CK: A Guide to the Modern Threat Tactics [Электронный ресурс]. –Режим доступа: https://attack.mitre.org/. - Дата доступа : 15.02.2024.

2. Cybersecurity and Technology Controls [Электронный ресурс]. –Режим доступа: https://www.mitre.org/publications/technical-papers/cybersecurity-and-technology-controls Дата доступа : 15.02.2024.

UDC 004.056.53

METHODOLOGY FOR BUILDING A SYSTEM FOR MONITORING INFORMATION SECURITY EVENTS IN AN INFORMATION SYSTEM USING THE EXAMPLE OF MITRE ATT&CK MODEL TECHNIQUES TA0002-TA0009

Popovich A.A.

gr.367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Borbotko T.V. – Dr. of Sci. (Tech.), Head of the Department of Information Security

Annotation. The report contains the basic principles and conceptual models of MITER ATT&CK, its structure, categories of tactics and techniques, as well as examples of using models in practical tasks that allow you to use knowledge about the principles of cybersecurity and methods of protection against cyber attacks based on the main technical models TA0002-TA0009.

Keywords: MITRE ATT&CK models, TA0002-TA0009 models, cybersecurity.