Выявление индикаторов компрометации

Р.С. Ларичев

Поволжский Государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. В настоящее время информационные технологии играют важную роль во многих сферах деятельности человека. Однако вместе с преимуществами они несут и определенные риски, связанные с информационной безопасностью. Одним из таких рисков является компрометация информационных систем, которая может привести к потере важных данных, а именно конфиденциальной информации, финансовым потерям и другим негативным последствиям. Для предотвращения компрометации информационных систем необходимо использовать различные варианты защиты информации. Одним из методов защиты является выявление индикаторов компрометации (IoC).

Цель — рассмотреть способы выявления индикаторов компрометации (IoC).

Методы. Выявление индикаторов компрометации (IoC) — это процесс, включающий в себя анализ данных и поиск признаков, которые могут указывать на наличие компрометации в информационной среде. Существует несколько показателей компрометации, которые организациям следует отслеживать. Перечислим несколько ключевых показателей компрометации: необычный исходящий сетевой трафик, аномалии в активности учетной записи пользователя, вход в систему: красные флажки, увеличение объема чтения базы данных. Проводя мониторинг сетевой активности, можно обратить внимание на необычные или подозрительные запросы, аномальный объем данных или попытки несанкционированного доступа к ресурсам. Можно воспользоваться внешними источниками активного поиска Threat Intelligence, чтобы получить информацию о новых угрозах и индикаторах компрометации. Дополнительно можно изучить матрицу MITRE ATT&CK, чтобы понять классические тактики, методы и техники, которые свойственны злоумышленникам. Она может определить соответствующие индикаторы компрометации, так как имеет большую базу знаний о тактиках, методах и техниках, которые могут использовать злоумышленники в рамках кибератак. Матрица может быть использована для оценки качества эффективности существующих методов обнаружения атак. Аналитики могут сопоставлять обнаруженные атаки с тактиками и техниками, которые описаны в MITRE ATT&CK, чтобы определить, как хорошо их системы закрыты и где есть уязвимости.

Результаты. Результатом применения этих методов является оперативное срабатывание на угрозы и компрометации, что позволяет быстро реагировать на атаки и минимизировать потенциальный ущерб. Также регулярное выявление IoC помогает улучшить защиту организации, находя слабые места и уязвимости.

Выводы. Выявление индикаторов компрометации является важным компонентом стратегии кибербезопасности любой организации. Threat Intelligence и MITRE ATT&CK играют ключевую роль в этом процессе, предоставляя информацию о киберугрозах и тактиках, которые могут быть использованы злоумышленниками. Использование этих инструментов позволяет организациям оперативно реагировать на угрозы и обеспечивать безопасность своих информационных ресурсов.

Ключевые слова: индикаторы компрометации; компрометация информационных систем; уязвимости; Threat Intelligence; MITRE ATT&CK.

Сведения об авторе:

Роберт Сергеевич Ларичев — студент, группа ИБТС-21, факультет №1; Поволжский Государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: la-robin@yandex.ru

Сведения о научном руководителе:

Ирина Сергеевна Поздняк — доцент кафедры информационной безопасности; Поволжский Государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: i.pozdnyak@psuti.ru