УДК 004.056

ПОДХОД К ФОРМИРОВАНИЮ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ НА ОСНОВЕ ИНФОРМАЦИИ ОБ АТАКАХ НА ЛОЖНЫЕ ЦЕЛИ

Шабала Е.Е (Университет ИТМО)
Научный руководитель – к.т.н, Менщиков А.А.
(Университет ИТМО)

Введение. Обнаружение индикаторов компрометации (IoC) в защищаемой системе с наибольшей вероятностью указывает на фактическое осуществление несанкционированного доступа к ней, ее компрометацию. В виде индикаторов компрометации обычно выступают заранее определенные паттерны вредоносной или нежелательной активности (запросы, ответы, действия) [1], вредоносного программного обеспечения (хэши, ip, домены). Сбор и формирование индикаторов компрометации требуют глубокого и неавтоматизированного ретроспективного анализа осуществленной атаки, или по крайней мере – попытки ее осуществления, которая была обнаружена и предотвращена. Однако, системы ложных целей (Deception) также могут быть поставщиками экспертизы по актуальным индикаторам компрометации [2], при этом данные индикаторы могут обнаруживаться автоматически и могут быть сразу использованы для защиты целевой системы. Это достоинство делает актуальным работы по анализу и разработке потенциальных методов и подходов формирования индикаторов компрометации на основе экспертизы, поставляемой системами ложных целей. Основной проблемой, которая требует решения – является неустойчивость автоматизированного подхода к формированию индикаторов компрометации на основе данных об атаках на ложные цели, склонность алгоритмов к ошибкам первого и второго рода.

Основная часть. На основе многосервисной архитектуры системы ложных целей предлагается подход к сбору, систематизации, накоплению, обработке поступающих данных об осуществляемых атаках для автоматизированного формирования индикаторов компрометации. Автоматизация данного процесса позволяет достичь решения трех основных задач: 1. Использовать систему ложных целей как дополнительный источник поставки индикаторов компрометации для иных средств защиты информации. 2. Уменьшить необходимость ретроспективного анализа атак на ложные цели. 3. Повысить скорость реагирования и распространения выявленных индикаторов, тем самым увеличить общую защищенность системы и обеспечить возможность более раннего выявления атак в будущем. Кроме того, предлагаемый подход позволяет исключить нецелевые данные из анализируемой выборки поступающих данных, снизить возможные ошибки первого и второго рода, повысить потенциальную достоверность определяемых индикаторов, там самым повысить общую защищенность системы.

Выводы. Предложен подход к формированию индикаторов компрометации на основе информации об атаках на ложные цели, позволяющий осуществлять их автоматизированное определение без необходимости ретроспективного анализа хода атаки, позволяющий уменьшить время реагирования и распространения индикаторов компрометации, тем самым повышающий общую защищенность системы.

Список использованных источников:

1. Masoumeh. A., Jafarian, J. A game-theoretically optimal defense paradigm against traffic analysis attacks using multipath routing and deception. // Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies. – 2022.
2. Li Zhang, Vrizlynn L. L. Thing. Three decades of deception techniques in active cyber defense - Retrospect and outlook // Computers & Security. – 2021 – № 106. – 102288.