УДК 004.056

АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ПО ОБНАРУЖЕНИЮ ТЕХНИК БОКОВОГО ПЕРЕМЕЩЕНИЯ

Агарков А.В. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Заколдаев Д.А.
(Университет ИТМО)

Введение. Боковое перемещение – это совокупность техник, используемых для получения удаленного доступа к системе или к нескольким системам в корпоративной сети. Для этого злоумышленники могут использовать легитимные учетные данные пользователей или собственные инструменты. Зачастую при боковом перемещении атакующие используют сложные механизмы атак, что усложняет их обнаружение классическими системами мониторинга. Чтобы решить данную проблему рекомендуется использовать методы машинного обучения, позволяющие выявлять аномальное поведение, связанное с боковым перемещением. Данная работа сосредоточена на подробном анализе способов обнаружения бокового перемещения с помощью методов контролируемого и неконтролируемого машинного обучения.

Основная часть. Согласно отчету [1] за 2023 год, техники бокового перемещения применялись в 25% случаев при всех зафиксированных атаках на организации. В данной работе исследуются работы по обнаружению бокового перемещения, в которые входят:

1. В работе [2] предлагается метод, основанный на построении графа связей сущностей в корпоративной сети с помощью графической нейронной сети и неконтролируемого алгоритма машинного обучения для обнаружения аномальных аутентификаций между сущностями графа.
2. В работе [3] исследуются алгоритмы машинного обучения для обнаружения бокового перемещения на основе вредоносного RDP трафика.
3. В работе [4] предлагается метод обнаружения бокового перемещения, основанный на организации систем функциональным по ролям. Данный метод использует неконтролируемые алгоритмы машинного обучения для анализа последовательностей процессов и используемых портов.
4. В работе [5] сравниваются алгоритмы глубокой и поверхностной классификации обнаружения бокового перемещения, основанные на анализе системных журналов Sysmon.

Выводы. Проведен обзор исследований по обнаружению техник бокового перемещения с помощью методов машинного обучения. На основе обзора выявлены основные преимущества и недостатки используемых в работах подходах, которые могут быть полезны для будущих исследователей.

Список используемых источников:

1. Global Incident Response Threat Report – VMware. URL: https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1553238_Global_Incident_Response_Threat_Report_Weathering_The_Storm.pdf (Дата обращения 01.12.23).
2. Benjamin Bowman, Craig Laprade, Yuede Ji H. and Howie Huang. Detection lateral movement in Enterprise Computer Networks with Unsupervised Graph AI // USENIX 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2020.
3. Tim Bai, Haibo Bian, Mohammad A. Salahuddin, Abbas Abou Daya, Noura Limam and Raouf Boutaba. RDP-based Lateral Movement detection using Machine Learning // Computer Communications. 2021. Vol. 165, P. 9-19.

4. Brian A. Powell. Role-based lateral movement detection with unsupervised learning. // Intelligent Systems with Applications. 2022. Vol 16.

5. Christos Smiliotopoulos, Georgios Kambourakis and Konstantia Barbatsalou. On the detection of lateral movement through supervised machine learning and an open-source tool to create turnkey datasets from Sysmon logs // International Journal of Information Security. 2023. Vol. 22, 1893-1919.