УДК *004.056*

ИНСТРУМЕНТ ДЛЯ OSINT-РАЗВЕДКИ И РЕАЛИЗАЦИИ ТЕХНИКИ MITRE ATT&CK T1593

И.А. Войткус, Е.С. Белоусова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается автоматизация сбора данных киберразведки по технике MITRE ATT&CK T1593. Разработан инструмент для OSINT-разведки на базе low-code платформы n8n, включающий три процесса: поиск скрытых документов, анализ репозиториев и визуальную разведку. Апробация разработанного инструмента была проведена на ресурсах БГУИР и подтвердила высокую скорость профилирования цифрового следа и масштабируемость решения.

Ключевые слова: разведка по открытым источникам; киберразведка; тактика T1593; автоматизированный сбор данных; биометрическая верификация; сбор информации; агрегация данных

AUTOMATION OF OSINT INTELLIGENCE BASED ON MITRE ATT&CK T1593 TECHNIQUE

I.A. Voitkus, E.S. Belousova

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article discusses the automation of cyber intelligence data collection using MITRE ATT&CK T1593 technology. A tool based on the n8n low-code platform has been developed, which includes three processes: search for hidden documents, repository analysis, and visual intelligence. Testing on the BSUIR resources confirmed the high speed of digital footprint profiling and scalability of the solution

Keywords: open-source intelligence; cyber intelligence; T1593 tactics; automated data collection; biometric verification; information collection; data aggregation

Введение

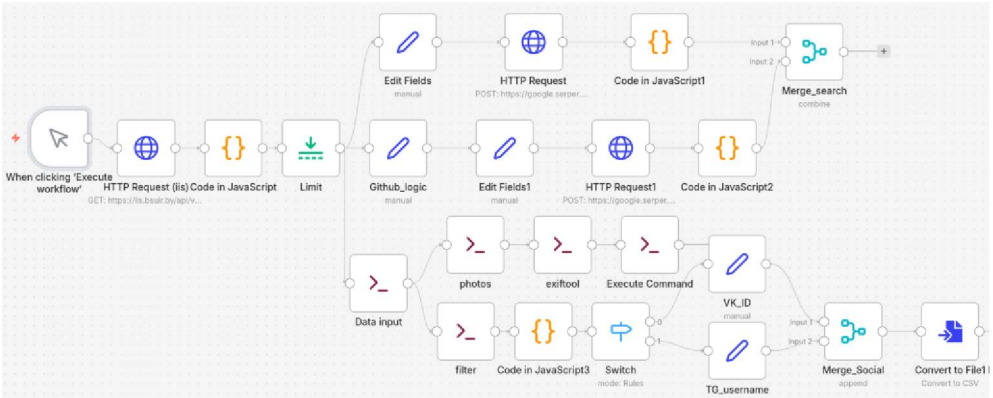
Киберразведка – начальный и ключевой этап реализации киберугроз в рамках модели «Cyber Kill Chain» [1]. Множественные массивы корпоративных и персональных данных, опубликованные на официальных ресурсах и сторонних платформах, формируют «цифровой след»

организации [2]. В матрице MITRE ATT&CK сбор и анализ такой информации описан в технике T1593, включающую подтехники T1593.001 – T1593.003, поиск через поисковые системы, репозитории кода и социальные сети соответственно.

Поскольку ручной анализ таких массивов очень ресурсозатратен, автоматизация процессов критически важна для ускорения аудита и выявления скрытых корреляций. Разработанный автоматизированный OSINT-инструмент реализует три ключевых вектора разведки. Основными этапами работы инструмента для OSINT-разведки являются: автоматизированный поиск по открытым документам и файловым хранилищам и анализ результатов поиска, который основан на следующих процессах: выявления скрытых документов, выявление публичных репозиториев кода и комплексный анализ визуального следа.

Основная часть

Для проверки OSINT-инструмента были выбраны интернет-ресурсы БГУИР из-за их сложной инфраструктуры и большого объема данных о сотрудниках. Изначально планировался парсинг HTML-страниц портала bsuir.by, однако анализ поддоменов выявил систему электронного расписания (iis.bsuir.by). Изучение сетевых запросов приложения расписания позволило обнаружить публичный API-эндпоинт с открытыми данными кадрового состава. Использование этого API вместо парсинга HTML позволило успешно обойти блокировки целевого сервера и извлечь информацию в виде 803 профиля сотрудников в структурированном виде. Единовременная генерация пула запросов такого количества привела бы к срабатыванию триггеров межсетевого экрана. Было принято решение интеграции провайдера Serper.dev, а также провести выборочное тестирование на трех случайных записях пользователей.



Архитектура OSINT-инструмента
Architecture of the OSINT tool

Полученные данные содержат поля имени, фамилии и отчества, для корректной работы поисковых алгоритмов в конвейер была добавлена нода трансформации данных, формирующая единый унифицированный идентификатор. Далее инструмент на втором этапе инициирует разделение данных на три процесса.

Первый процесс осуществляет поиск скрытых документов на поддоменах университета. Система автоматически генерирует запрос через легитимный API-шлюз для предотвращения блокировок, возвращая готовый массив ссылок на найденные файлы. Запрос возвращает готовый список прямых ссылок на найденных документах.

Второй процесс выявляет у субъекта публичные репозитории кода, выступающие потенциальным источником утечек информации. Возникшая при настройке узлов проблема потери контекста была успешно решена архитектурно – путем принудительного проброса переменных через всю цепочку конвейера. На выходе сохраняются отфильтрованные ссылки на профили выявленных субъектов.

Третий процесс выполняет комплексный анализ визуального следа. Инструмент Photon позволил собрать ссылки на социальные сети и доменные адреса, а также конвейер инициирует HTTP-запросы на скачивание графических файлов, формируя оффлайн-базу данных. Консольная утилита ExifTool анализирует структуру каждого файла в поиске скрытых цифровых следов. Локальная верификация с помощью библиотеки машинного зрения DeepFace, сравнивает найденные лица с эталонным фото, гарантируя конфиденциальность вычислений.

Заключение

На платформе n8n разработан и протестирован инструмент для OSINT-разведки. Инструмент позволил собрать базу данных субъектов и провести дальнейшие поиски по ней Предложенная архитектура обладает высокой гибкостью и может быть масштабирована путем интеграции новых инструментов.

Список использованных источников

1. Блэр, Р. Согласование операций безопасности с фреймворком MITRE ATT&CK / Р. Блэр. – Бирмингем: Packt Publishing, 2022. – 268 с. – ISBN 978-1804616697.

2. Озкая, Э. Практическая киберразведка: сбор, обработка и анализ мотивов, целей и атак злоумышленников / Э. Озкая. – Нью-Дели: BPB Publications, 2022. – 452 с. – ISBN 978-9355510372.

References

1. Blair, R. Aligning Security Operations with the MITRE ATT&CK Framework / R. Blair. – Birmingham: Packt Publishing, 2022. – 268 p. – ISBN 978-1804616697.

2. Ozkaya, E. Practical Cyber Threat Intelligence: Gather, process, and analyze threat actor motives, targets, and attacks / E. Ozkaya. – New Delhi: BPB Publications, 2022. – 452 p. – ISBN 978-9355510372.

Сведения об авторах

Войткус И.А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», voitkusvoitkus@gmail.com.

Белоусова Е.С., канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Voitkus I.A., student of Information Security Faculty, Belarusian State University of Information Technology and Radio Electronics, voitkusvoitkus@gmail.com.

Belousova E.S., PhD, Associate Professor, Information Security Department, Belarusian State University of Informatics and Radioelectronics, belousova@bsuir.by.