РАСШИРЕНИЕ БАЗОВОГО ФУНКЦИОНАЛА MALTEGO С ПОМОЩЬЮ ФРЕЙМВОРКА CANARI

Давлатов Ш.Р.

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

Кучинский П.В. – доктор технических наук

Сбор и анализ информации является неотъемлемой частью любого качественного аудита информационной безопасности автоматизированных систем. В данной работе рассматривается инструмент Maltego, который широкоприменяетсядля сбора данных и автоматического построения связей между различными объектами исследования. Приводится пример расширения базового функционала Maltego с помощью фреймворкаCanari на основе языка программирования Python.

Maltego является проприетарным программным обеспечением, который используются для построения и анализа связей между различными объектами информационной системы. Его особенностями являются: визуализирование, обработка и комбинирование информации для более детального анализа данных, полученных из открытых источников информации. С помощью Maltegoможно также проводить автоматический анализ источников данных с целью построения взаимосвязей между обнаруженными объектами (люди, профили социальных сетей, электронные почты, организации, документы, картинки,геолокации, веб-сайты, домены, DNS имена, IP адреса и другие интернет инфраструктуры). Данный инструмент широко используется специалистами по информационной безопасности на начальных этапах проведения аудита информационной системы:сбор первичнойинформации;автоматизацияпроцессаанализа данных; тестирование объекта защитына проникновение (например, для определенной сети организации нужно выявить - какиеданные доступны в открытом доступе внешнему миру: порты, IPадреса, NS записи и другие). Данная информация в руках злоумышленников может представлять значительный рискдля автоматизированной системы организации [1].

В основе работыMaltego лежит идея создания трансформаций, принцип работы которой напоминает функцию от одного аргумента.Результатом применения трансформациинад входным объектом должен быть набор (один илинесколько)выходных Maltego-сущностей. Таким образом, создается граф зависимостей между объектами исследования, узлы которой находятся в соотношении 1:1 (один к одному) или1:n (один ко многим).Самым главным преимуществом программы Maltegoявляется возможность гибкой настройки и адаптации под любые уникальные требования [2]. Один из вариантов расширения базового функционала Maltegoявляется использование фреймворкаCanari (исходный код доступенв открытом видена веб-сервисеGitHub: *https://github.com/redcanari/canari3*).Данный фреймворк распространяется под лицензией GNU (GeneralPublicLicense) v3.0,что дает пользователям все права для копирования, модифицирования и распространения программы. Рассмотрим пример построения новой Maltego-трансформации(рисунок 1), которая на вход принимаетдоменное имя и на выходе генерирует новые сущности: IP адрес, NSсервер и список похожих доменов.

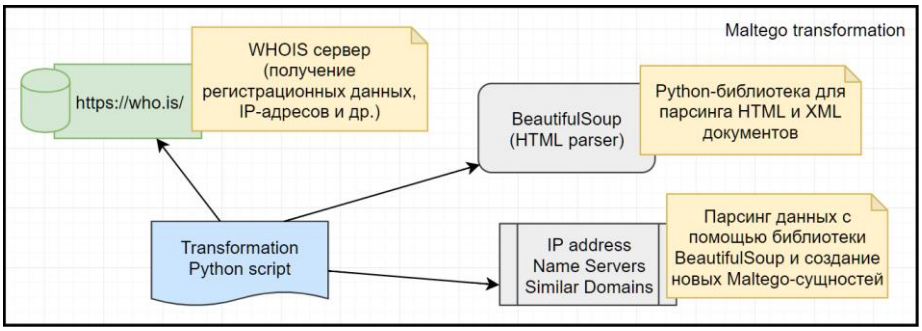

Рисунок 1 –Архитектура новой трансформации для Maltego

Для создания новой трансформации на базе фреймворкаCanari, необходимо создать Pythonкласс, который содержит обязательный метод *do_transform* [3]**.** Базовая логика трансформации должна быть реализована в даннойфункции. Рассмотрим детально алгоритм работы метода *do_transform*:

```
url = 'https://who.is/whois/' + request.entity.value
html_doc = urlopen(url).read()
soup = BeautifulSoup(html_doc, 'html.parser')
```

Сначала отправляется запрос на *who.is*сервер (в нашем примере, данный ресурс является основным источником информации), для получения регистрационных данных о домене. Ответ сервера записывается в переменной *html_doc*какhtml-документ и с помощью библиотеки *BeautifulSoup*парсится для дальнейшего доступа к его узлам в императивном стиле.Применяястандартныеметоды*find*и *find_all,*можно найти в документе теги с заданным условием поиска. Вторым аргументом передается лямбда-функция, которая ищет вхождение заданной строки (*'/nameserver' и '/whois-ip'*) в ссылке тега. Таким образом, мы получаем NSсервер,IPадрес и список похожихадресов, которые соответствуют входному домену:

```
ns = soup.find('a', href=lambda href: href and '/nameserver' in href)
ip = soup.find('a', href=lambda href: href and '/whois-ip' in href)
similar_domains = soup.find_all('a', href=lambda href: href and '/whois/bsuir' in href)
```

Для генерации новыхвыходных объектовMaltegonеобходимо конкатенировать аргумент*response*с новыми созданными сущностями. Из стандартной библиотеки Canariимпортируютсяфункции-генераторы *URL и IPv4Address*. На вход каждой функции передается текстовое представление имениNSсервера, IPадреса и списка доменов для генерации соответствующих сущностей на выходе:

```
response += URL(ns.text)
response += IPv4Address(ip.text)
for domain in similar_domains:response += Domain(domain.text)
```

Последней инструкцией функции*do_transform*обязательно должнобыть возвращение результата -*returnresponse.* Для того, чтобы протестировать работу данного скрипта необходимо выгрузить его для программы Maltego путем набора команды *canaricreate-profiledemo*в терминале операционной системы, где *demo*является именем корневой папки проекта.

Для проверки результата применения трансформации, в новой вкладке Maltegonужно создать входную сущность - доменное имя (в качестве примера введем *bsuir.by)*. Как видно из рисунка 2 – разработанная функцияна выходе генерирует сущности трех типов: NSсервер с найденным значением *ns.bsuir.by*, IPадрес сервера, который обслуживает домен – *46.216.181.36*, а также, список доменовс префиксом *bsuir-*. Для более детального анализа, можно запустить созданную трансформацию для всех выходных доменов по отдельности. Maltegoавтоматически построит все взаимосвязи между объектами с подробной информацией о соединениях.

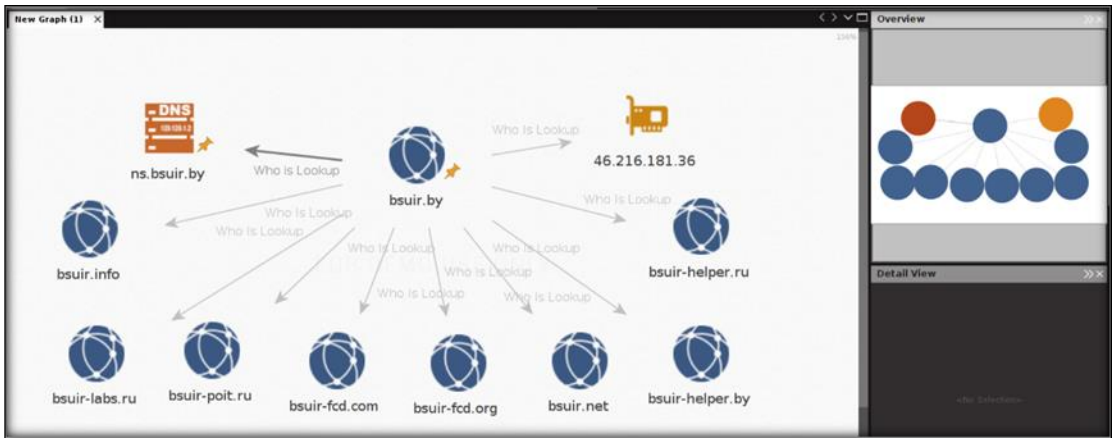

Рисунок 2 – Результат применения новой трансформации для Maltego

Таким образом, в данной работе был рассмотренинструмент для сбора и анализа данныхMaltego, который широко используется в сфере компьютерной безопасности. Предлагаемый вариант расширения базового функционала на базе фреймворкаCanariпозволяет с легкостью настроить программу под любые уникальные требования, которые необходимы специалистам по информационной безопасности для проведения более качественного и детального аудита безопасности информационных систем.

Список использованных источников:

25. ДавлатовШ.Р. Система сбора, анализа и визуализации данныхоб устройствах в сети Интернет // Доклады БГУИР, № 6, 2018, С. 19-25.

26. MaltegoOSINTBlog [Электронный ресурс], режим доступа: https://maltego.blogspot.com – Дата доступа: 08.02.2019

27. CanariFramework'sdocumentation[Электронный ресурс], режим доступа: http://www.canariproject.com/en/latest/ – Дата доступа: 05.02.2019