Стриженко И.Ю.

Основные принципы и инструменты OSINT разведки

General ways and instruments of OSINT recon

Кафедра информационной безопасности ШЕН ДВФУ

Ключевые слова: OSINT, разведка, анализ данных, Maltego.

Аннотация:

В век цифровых технологий общество постоянно загружает огромное количество информации о себе в открытый доступ. Каким образом можно работать с такой информацией и как делать это наиболее эффективно? В данной статье был произведен анализ двух выступлений по поводу OSINT разведки и сформированы основные принципы обработки информации для получения эффективного результата.

Смысл OSINT-разведки в том, чтобы суметь использовать огромное количество информации для построения очень подробного досье на конкретные сущности, будь то люди или организации в зависимости от конкретной задачи.

Проблема заключается в огромном количестве доступной информации. Если не иметь четкого представления о том, какую задачу необходимо решить или на какой вопрос ответить, можно запутаться и окружить себя информацией, которая не имеет никакого отношения к решаемой задаче.

Разведка необходима для построения четкого образа и плана действий в соответствии с поставленной задачей. Для того чтобы она прошла эффективно, необходимо ставить конкретные задачи, связанные с проблемой, уметь задавать правильные вопросы, находить закономерности в данных и проявлять смекалку при поиске необходимой информации.

Большинство информации можно найти в специальных базах данных или с помощью API. Люди и организации предоставляют огромное количество информации о себе в социальных сетях, и эту информацию можно вытащить с помощью API-запросов. Вся полученная информация может быть проанализирована и отсортирована, чтобы найти связи, незаметные для обычного человека.

Одной из задач исследователя является сбор «сырой» информации для дальнейшего поиска закономерностей в контексте решаемой проблемы. Инструментом для этого может послужить Maltego. Эта программа позволяет графически отобразить результат исследования, которыми можно поделиться с другими людьми.

Maltego представляет собой программу-холст, на который можно размещать информацию и затем использовать специальные алгоритмы, называемые «transforms», чтобы обработать информацию. Это ПО предусматривает обработку выгрузки, преобразования, анализа и визуализации данных. Оно делает запросы в различные API, чтобы искать закономерности и отображать их на виртуальном “холсте”.

На презентации в Pasadena City College на тему «Maltego - Cyber Weapons Lab - Research like an OSINT Analyst» [1] приводили в пример 2 расследования проведенных с помощью Maltego.

В первом расследовании получали ответ на вопрос: «Произошла ли утечка персональных данных у кого-нибудь из работников газеты The Guardian?».

Для ответа на поставленный вопрос необходимо было решить следующие задачи:

1) Установить web домены email-адресов работников The Guardian;

2) Достать список email-адресов работников The Guardian;

3) Сравнить список email-адресов работников The Guardian с данными об утечке и разделить работников на скомпрометированных и не скомпрометированных;

4) Составить список работников, чьи данные были найдены в утечке;

5) Составить список инцидентов, в которых произошла утечка данных этих работников;

6) Составить список типов информации, которая была скомпрометирована.

Программа Maltego смогла найти домен email-адресов, вытащить список email-адресов работников с помощью PGP преобразования, далее с помощью трансформации haveibeenpwned.com программа смогла определить чьи email-адреса были скомпрометированы. Из 27-ми пользователей данные 7-ми были скомпрометированы. Один из работников потерял все свои данные, включая пароли, информацию о кредитных картах и прочее из-за небезопасной работы приложения спортзала, в котором он занимался. Далее в расследование были добавлены адреса остальных пользователей, чьи данные были утеряны. Повторное применение преобразования показало, что эти адреса засветились в 5-ти крупных утечках. В результате было установлено, что персональные данные 7 работников газеты The Guardian появлялись в 5 различных инцидентах утечек информации.

Такое расследование показало конкретные случаи утечки информации, в которых участвовали рабочие, и какая информация была утеряна. По этой информации можно определить человека, использующего самые слабые методы безопасности, и атаковать конкретно его.

Во втором расследовании была установлена связь некоммерческой организации с саентологами через расследование источников прибыли данной организации.

Так как многие организации стараются получить прибыль с их онлайн собственности, можно использовать инструмент анализа гиперссылок в Maltego, чтобы найти другие сайты, использующие те же самые партнерские ссылки. В результате преобразования было установлено, что тот же самый партнерский код что и у рассматриваемой организации был замечен на сайте организации саентологов. Таким образом, из-за того, что организации не трудятся менять партнерские коды для своих различных проектов, можно составить список потенциальных проектов, в которых эти организации могут участвовать. И на основании этих данных можно принять нужное решение о сотрудничестве с такими организациями.

На мероприятии SEVillage в рамках конференции DEF CON 27 Ryan MacDougall выступил с докладом «OSINT in the Real World» [2]

Райан утверждает, что в повседневной жизни основные навыки OSINT-разведки учат замечать закономерности и использовать их в свою пользу. В докладе рассказчик демонстрирует 2 примера из своей практики:

Он столкнулся с ситуацией, когда захотел проверить, как зовут родителей друга его ребенка и устраивает ли его то, что его сын общается с этой семьей. С помощью Google Maps был найден адрес семьи. На основании открытых данных о собственниках было установлено 3 владельца: 1 мужское имя и 2 женских. Произведя поиск по имени и названию бизнеса, связанного с мужем, он определил имя второго родителя, факт того, что она работает вице-президентом банка. Также фотография профиля совпадала с внешностью матери. В итоге были найдены имя и фамилия членов семьи ребенка, с которым общается сын докладчика, а также установлено кем эти люди являются.

Второй пример заключается в пробивке рабочего, которого порекомендовали докладчику для выполнения строительных работ. По его имени и номеру телефона был найден сайт, посвященный его бизнесу. Поиск по названию бизнеса и его имени дал зацепку о записях на сайтах с резюме; с помощью поиска кэш версий этого сайта удалось вытащить сохранившуюся информацию о том, что данный строитель давно основал свой бизнес, работает один и имеет много положительных отзывов, поэтому вся эта информация позволила с уверенностью сказать, что его можно нанимать.

Подход второго докладчика отличался от первого отсутствием четкой схемы действий, но у обоих есть четко поставленная задача, вопрос сформулирован корректно и на него можно дать точный ответ, все действия логичны и последовательно вытекают друг за другом, в конце собранные данные обработаны, пропущены через контекст и на выходе был получен

ответ на поставленный вопрос. Такая информация подкреплена фактами, контекстом, любой может посмотреть на нее и сказать, что с ней нужно делать.

Эти принципы, которыми руководствовались оба докладчика, соответствуют описанным принципам в исследовательских работах, посвященных OSINT-разведке. [3][4][5]

Список используемых источников

[1] Maltego - Cyber Weapons Lab - Research like an OSINT Analyst - YouTube

[2] SEVillage at Def Con 27 - OSINT in the Real World - Security Through Education (social-engineer.org)

[3] Sondarva, Shweta & Sharma, Dr & Dholariya, Prof. (2021). Prevention to Sensitive Information Disclosure via OSINT. International Journal of Scientific Research in Science, Engineering and Technology. 109-114. 10.32628/IJSRSET218317.

[4] García, Francisco. (2021). Private Investigation and Open Source INTelligence (OSINT). 10.5772/intechopen.95857.

[5] Bazzell M. Open source intelligence techniques: resources for searching and analyzing online information. – IntelTechniques. com, 2016.