Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: mathmod.esrae.ru/46-182
Ссылка для цитирования этой статьи:
Власенко Д.В. Социальная инженерия. сбор информации о человеке с помощью метода OSINT, его типы, значение и способы защиты // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2024. №2

УДК 004.056.5 DOI:10.24412/2541-9269-2024-2-2-12

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. СБОР ИНФОРМАЦИИ О ЧЕЛОВЕКЕ С ПОМОЩЬЮ МЕТОДА OSINT, ЕГО ТИПЫ, ЗНАЧЕНИЕ И СПОСОБЫ ЗАЩИТЫ

Власенко Д.В.
Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, d4nila.vlasenko@yandex.ru

SOCIAL ENGINEERING. COLLECTING INFORMATION ABOUT A PERSON USING THE OSINT METHOD, ITS TYPES, MEANING AND METHODS OF PROTECTION

Vlasenko D.V.
Yuri Gagarin State Technical University of Saratov, Russia, Saratov, d4nila.vlasenko@yandex.ru

Аннотация. В настоящее время все больше людей держат свою личную и деловую информацию онлайн, поэтому метод поиска по открытым источникам OSINT становится все более значимым и широко используемым. В статье рассмотрены типы OSINT, его значение в области информационной безопасности, а также способы защиты, которые применяются или могут применены организациями или обычными пользователями сети Интернет для противодействия социальной инженерии.

Ключевые слова. Информационная безопасность, защита информации, кибербезопасность, социальная инженерия, поиск по открытым источникам

Abstract. Nowadays, more and more people keep their personal and business information online, so every day the OSINT open source search method becomes more significant and widely used. The article discusses the types of OSINT, its importance in the field of information security, as well as protection methods that are used or can be used by organizations or Internet users to counter social engineering.

Keywords. Information security, information protection, cybersecurity, social engineering, open source intelligence

Введение

На сегодняшний день развитие программных и программно-аппаратных средств защиты информации сильно затрудняет получение злоумышленникам получение доступа к информационным системам путем взлома. Поэтому все чаще их целью становится наиболее уязвимый элемент – человек. Самым распространенным методом воздействия на человека является социальная инженерия.

Социальная инженерия представляет собой метод манипуляции межличностными взаимодействиями на основе психологических и социальных механизмов [4]. Например, подобным методом не пренебрегают отделы продаж, навязчиво предлагая людям товары по огромной скидке при покупке чего-то на определенную сумму и аргументируя это тем, что акция ограничена по времени и вообще вы один из немногих, кому эта самая акция доступна. В профессиональной среде пентестеров по социальной инженерии или хакеров целью социальной инженерии является психологическое влияние на человека или группу людей для получения несанкционированного доступа к информации, ресурсам или системам. Один из самых распространенных и эффективных методов сбора информации в рамках социальной инженерии - это использование открытых источников, или метод OSINT. В настоящее время данный метод становится все более эффективным и вследствие этого применяемым. Поэтому рассмотрим его поподробнее с точки зрения защиты.

OSINT расшифровывается как Open-source intelligence или же разведка по открытым источникам [7]. Источниками OSINT являются публично доступные базы данных: газеты, журналы, социальны сетях, форумы, блоги, веб-сайты, реклама и т.д. С помощью метода OSINT можно собрать разнообразную информацию о человеке или компании-жертве, такую как его имя, фотографии, контактные данные, местонахождение, профессиональные связи. При атаке на компании есть большая вероятность выудить у невнимательного сотрудника информацию об используемых технологиях, структуре компании или профессиональном жаргоне, особенно, если организация не придает особого значения обучению сотрудников методам противодействия социальной инженерии. Собранная при помощи метода OSINT информация в дальнейшем может либо поддержать, либо разрушить усилия по социальной инженерии. От количества и качества полученной информации будет предопределена вероятность успеха проводимой операции. Если исполнитель попытается провести атаку, не зная информации о личности жертвы, рабочей обстановке или структуре, то, скорее всего, такая атака приведет к неудаче. Многие ведущие специалисты по социальной инженерии утверждают, что соотношение между

сбором информации и фактическим проникновением может содержаться в промежутке между 30%/70% и 70%/30% [2].

Типы и методы OSINT

В рамках открытого сбора информации (OSINT) существуют различные типы данных и источников, которые можно использовать для получения полезной информации.

Джо Грей, ветеран ВМС США, основатель и главный инструктор OSINTion, ведущий исследователь Transparent Intelligence Services, в своей книге «Социальная инженерия и этичный хакинг на практике» разделяет OSINT на три типа:

- Относящийся к бизнесу, в ходе которого происходит поиск информации об организации в целом. Например, поиск поставщиков, страховых компаний, клиентах, технологий или даже компаний, предоставляющих услуги по вывозу мусора;
- Относящийся к людям, целью которого является сам человек. Методы, относящиеся к данной категории, можно использовать как для сбора информации о личности человека (его вкусы, предпочтения и т.д.) с целью получения данных о, например, используемом пароле или вопросах для его сброса, так и для всего бизнеса (используемый жаргон, рабочая обстановка, расписание работы) с помощью фотографий с места работы, командировок или резюме;
- Относящийся к «фрагменту кода», использующийся в аналитике кибербезопасности. Данный тип OSINT позволяет идентифицировать виновного в нападении и его мотивы, анализируя части вредоносного кода с целью идентификации самого автора, его электронной почты или страны [2].

Однако настоящее время общепринятыми типами OSINT, с помощью которых могут быть отработаны цели, являются активная и пассивная разведки, и именно правильное сочетание всех вышеуказанных типов позволяет использовать методы OSINT на максимум, исключая ненужные области разведки, что помогает сократить и без того ограниченное количество времени, т.к. в сегодня информация может стремительно изменяться, и старые данные могут стать неактуальными в мгновение ока.

Пассивная разведка является самым часто используемым и самым продолжительным типом OSINT. Во время данного исследования атакующий никак не взаимодействует с жертвой, а только собирает информацию из открытых источников. Здесь отсутствует какое-либо личное общение, переписка или комментарии в социальных сетях в связи с высоким риском быстро провалить атаку.

Например, для поиска информации о бизнесе прекрасно подходит сервис WHOIS, предоставляющий информацию и владельце веб-ресурса, домене или IP-адресе. С развитием технологий злоумышленники придумали и другие

способы разведки с помощью дистрибутива Kali Linux и его инструментов или с использованием картографических или геолокационных инструментов (Google Maps). Данный метод позволяет неплохо изучить улицу или окрестности здания: входы/выходы, ворота, двери, названия компаний, занимающихся вывозом мусора или курьерской доставкой. Отличным решением будет изучение социальных медиа и публичных документов (ВКонтакте, Instagram*, LinkedIN Shodan).

Методы сбора OSINT о людях во многом схожи с предыдущими. С помощью инструментов Kali Linux можно узнать, был ли электронный адрес человека причастен к какой-либо утечке данных. И т.к. люди склонны использовать одну и ту же электронную почту на многих ресурсах, взлом жертвы не составит особого труда. С помощью сайтов по размещению резюме можно узнать об используемых технологиях (если уже известно, что человек работает в той или иной организации, что позволяет сделать вывод о программной составляющей компании) или найти ссылки на другие социальные сети. С помощью социальных сетей возможно изучение повадок жертвы, его интересы и создать досье, что в будущем поможет наладить с ней отношения с целью получения нужной информации. По тегам в медиа можно найти фотографии человека с места работы и сделать выводы о внутреннем распорядке, дресс-коду, об используемых программах в организации или даже количестве символов в пароле, не говоря уже об используемой почте.

Активная разведка, в свою очередь, предполагает воздействие на цель. В этом типе предполагается прямое взаимодействие с системой или человеком, о котором собирается информация. Однако здесь же и возрастает риск быть обнаруженным.

Активной разведкой в отношении к организации может быть использование «шумных» методов для сбора технических данных: сканирование портов, уязвимостей программного обеспечения или попытка получения доступа к открытым портам. Данные методы оставляют много следов в виде лог-файлов, поэтому они являются не самыми желательными.

В отличие от активного взаимодействия с ресурсами организации, воздействие социальной инженерии на человека может выходить за пределы сервера или ПК. При взаимодействии с человеком важно принимать особые методы осторожности, чтобы не быть заранее скомпрометированным или не нанести вред жертве, что скорее всего приведет к завершению дальнейших действий. В свою очередь, пассивный OSINT помогает придумать повод для контакта с жертвой. Так как темой данной статьи также является информация о методах защиты от социальной инженерии, рассмотрим этот раздел подробнее.

Как правило, злоумышленники, занимающиеся социальной инженерией, в жизни являются отличными психологами. В основном они используют некоторые психологические концепции, позволяющие влиять на жертву как с положительной стороны (получение доверия), так и отрицательной (шантаж,

угрозы). К данным концепциям относят: влияние, манипуляции, взаимопонимание, симпатию и эмпатию.

Роберт Чалдини, американский психолог, описывает взаимосвязь между влиянием и манипуляцией с помощью шести принципов влияния [1]:

- Авторитет (когда кто-то более влиятельный просит или заставляет поверить, что так же поступает авторитетная фигура);
- Привлекательность (когда-то человек старается выглядеть в глазах жертвы милым и обаятельным). Именно поэтому на деловой встрече менеджер не придет неопрятным;
- Срочность или дефицит (именно этот метод был описан в примере с отделом продаж во введении данной статьи)
- Постоянство и последовательность (люди склонны к стабильности и не любят перемены);
- Социальное доказательство (когда-то злоумышленник ставит в пример кого-то более влиятельного или статусного в надежде, что жертва под предлогом обстоятельств поверит ему в надежде на, например, повышение или социальное одобрение);
- Взаимность (люди склонны помогать тем, кто когда-то помог им).

Все вышеописанные психологические уловки позволяют злоумышленникам выглядеть в глазах жертвы максимально авторитетными и привлекательными людьми. Анализируя их, нетрудно сделать вывод, почему активные методы OSINT являются достаточно удобными и эффективными способами получения информации.

Как правило методы активного OSINT включают в себя: фишинг (а также целевой фишинг), вейлинг, вишинг, приманки или сбор мусора. Рассмотрим их подробнее.

Фишинг (от англ. – ловля рыбы) - это отправка поддельного электронного сообщения для получения влияния над жертвой с целью получения информации, для открытия вредоносного файла или перехода на специально созданный злоумышленником веб-ресурс. Обычно фишинговые письма не адресованы конкретному человеку (об этот речь пойдет далее), а рассылаются массово, в надежде, что кто-то поведется. Этот способ можно сравнить с пулеметной очередью. Если жертва «ведется» на этот метод, то объем утечки информации может быть колоссальным. Как правило, фишинговые письма рассылаются от лица отдела кадров, службы безопасности, IT-подразделения или от лица генерального директора (авторитетный принцип влияния). Открыв вредоносную ссылку или загрузив вирусный файл, жертва позволяет злоумышленнику проникнуть в систему и выполнять в ней различные действия или предоставить хакеру нужную информацию.

Согласно отчету от «Лаборатории Касперского» в 2022 году 48,63% писем по всему миру и 52,78% писем в Рунете были спамом, а в I квартале 2023 года количество инцидентов увеличилось на 7% по сравнению с показателем

предыдущего квартала и стало на 10% больше, чем в начале 2022 года. Однако данные за 2023 год показывают, что фишинг идет на спад. [10].

По аналогии с фишингом, также существует и свишинг – отправка короткого смс сообщения на телефон.

Целевой фишинг – это подвид обычного фишинга, при котором фокус социальной инженерии происходит на конкретную цель. По данным Symantec Internet Security Threat Report в 2019 году показатель использования целевого фишинга различными организационными группами (включая национальную разведку) составил 65% [11].

Вейлинг (от англ. - китобойный промысел) – это разновидность фишинга, направленная человека, занимающего высокое положение в организации (как правило топ-менеджеры или главы подразделений). Злоумышленники подходят к таким атакам, используя более изощрённые способы, поскольку интересы у этих людей отличаются от обычного сотрудника. Злоумышленник может отправить письмо от имени отдела кадров, персонализируя сообщение, упомянув имя и должность, а также некоторые другие ключевые особенности человека, втираясь к нему в доверие. Обычно подобные люди обладают большими правами в системе, чем обычные пользователи; следовательно – ущерб, нанесенный при успешной атаке, увеличивается многократно.

Вишинг – это телефонный звонок жертве и последующим общением. Данный метод требует от злоумышленника неплохих навыков импровизации, поскольку реальный разговор в любой момент может пойти не в ту сторону. Преимуществом вишинга в сравнении с фишингом является скорость. Как правило во время таких звонков применяется подмена номера, так что определить звонившего будет не так просто. Схема атаки следует одному сценарию – нападающий создает ситуацию, позволяющую надавить на чувства жертвы. Во время звонка нарушитель будет пытаться установить с ней взаимопонимание, нередко включая в свой разговор выдуманные истории, схожие с историей жертвы, которые он узнал во время пассивного поиска. Обычно звонившие говорят, что занимаются проведением опросов, сотрудниками службы безопасности банка, являются представителями компании-поставщика или курьерами.

Согласно статистике за 2018 год, мошеннические звонки составляли примерно 30% от общего количества звонков, а 75% жертв утверждают, что нарушители заранее имели какую-то личную информацию о них [12].

Иногда, чтобы получить дополнительную информацию и человеке злоумышленники используют приманки. Обычно в качестве ловушки выступают USB-накопители, внешние HDD и CD-диски. Более изобретательным является вариант с QR-кодом. Чтобы подобные приманки выглядели более правдоподобно, их кладут в пакет или наклеивают привлекательные надписи (списки на увольнение, повышение зарплаты сотрудников и т.д.) и оставляют у входа в офис, подкидывают в сумки или выбрасывают у автомобиля сотрудника.

Внутри подобного устройства могут находиться вредоносные файлы, документы с ссылками, или вовсе этим может оказаться не накопитель, а USB-киллер – устройство, уничтожающее компьютер.

Самый «грязный» и малоэффективный способ активной разведки. Целью для поиска информации выступают пакеты с мусором у или на территории организации. Переодевшись сотрудником клининговой компании или компании, занимающейся вывозом мусора, злоумышленник может получить доступ к ближайшим урнам. Анализируя остатки, можно получить оттуда черновики важных документов, отчеты или финансовые выписки, что в дальнейшем может помощь нарушителю собрать еще больше информации.

Значение метода OSINT для информационной безопасности

Метод OSINT может использоваться не только в среде хакеров или преступных организаций, действия которых были описаны ранее, он также оказывает огромное влияние «белую» сторону информационной безопасности.

Разведка на основе открытых источников может использоваться организациями, выполняющих заказы на проверку сотрудников компании противодействия социальной инженерии, правительствами. Сбор информации OSINT также может помочь в анализе количества информации, которую компании могут непреднамеренно предоставить преступникам. OSINT может использоваться в судебных разбирательствах, предоставляя дополнительные сведения о пострадавшем или подозреваемом, может помочь в академических исследованиях, предоставляя информацию о тенденциях развития в той или иной отрасли. Активными пользователями OSINT являются журналисты, собирая дополнительные доказательства, собирая информацию по целому ряду тем, включая бизнес или преступность.

Противодействие OSINT может осуществляться разными способами, в зависимости от того, кто пытается получить доступ к информации и какую информацию они ищут.

Для организаций многие известные специалисты предлагают три основных метода: программы повышения осведомленности, мониторинг репутации и реагирование на инциденты [2].

1) Программы повышения осведомленности – это мероприятия, при которых пользователям организации предоставляются рекомендации по противодействию социальной инженерии и инструкции, если сотрудник подозревает, что является жертвой атаки. Один из подходов – информирование пользователей об общих тенденциях в индустрии информационной безопасности.

Чтобы не нагружать сотрудника излишней информацией, организации предлагают изначально обращать внимание на простые ошибки злоумышленников: неправильные контактные данные, устаревшая информация, протокол http, отсутствие зеленого значка в адресной строке и т.д.

Также нелишним, по мнению специалистов по информационной безопасности, будет информирование пользователей о последствиях, с которыми может столкнуться организация в результате успешной атаки.

2) Мониторинг репутации также иногда называют упреждающим мониторингом OSINT, мониторингом бренда или мониторингом даркнета.

При реализации программы мониторинга организация сама должна выбрать, на какие параметры ей стоит отводить внимание. Обычно под этим подразумевают информацию, которая может представлять риски для бизнеса. Нередкими бывают случаи, когда компания поручает OSINT третьей стороне. Когда аутсорс компания проводит мониторинг репутации, организация может избавиться от опасения, что организация следит за сотрудниками. При заключении договора подробно оговариваются все стороны сделки: время, возможности, этическая сторона и последствия при успешной атаке для работников.

3) Реагирование на инциденты – это набор определенных мероприятий, которые реализует организация при успешной атаке на нее.

Одна из стратегии – создать электронный ящик для сбора фишинговых писем. Если такое письмо обнаруживается, команда безопасности должна его проанализировать и выбрать оттуда любую имеющуюся информацию. Когда реагирование перешло на этап восстановления, должны быть учитаны предыдущие ошибки и созданы меры противодействия.

Очень часто обычные люди сами непреднамеренно передают свои данные злоумышленникам. Самый популярный общедоступный источник для хакеров – социальные сети. Пользователи не задумываясь оставляют в них персональную информацию о себе: имя, фамилия, дата рождения, город, школа, ближайшие родственники в списке друзей – зачастую все эти данные может увидеть любой желающий. Также многое о нас могут рассказать опубликованные изображения. Благодаря выложенной для на страничку фотографии адрес дома человека узнают не только друзья, но и «случайные прохожие». Только по одному фото можно собрать множество информации: когда, где и кто с кем встретился. Помимо этого, по убранству дома можно будет сделать предположения о достатке, способах заработка и т. д. И все это – лишь небольшая часть информации, которую могут получить злоумышленники.

Полностью защититься от OSINT никому не под силу, однако можно ограничить объем информации о себе в интернете. Самый простой способ защиты заключается в закрытии профилей в социальных сетях и проверке настроек приватности своих аккаунтов. Это поможет скрыть личные данные от посторонних глаз. Рекомендуется также тщательно следить за своими публикациями в интернете и информацией о себе, которую вы оставляете или уже оставили в сети. Также стоит внимательно присмотреться к публикации фотографий. Важным моментом защиты от поиска OSINT является удаление

лишних аккаунтов в интернете. Немаловажным советом будет фильтрация того, что человек пишет в личных сообщениях, беседах, говорит во время телефонного разговора. Не стоит направо и налево распространять свой адрес, номер телефона или карты.

Если же человек подозревает, что стал жертвой социальной инженерии, например, злоумышленника, представляющегося сотрудником банка, то стоит сбросить звонок и написать в техническую поддержу, который обязательно должен быть указан в приложении банка, чтобы удостовериться, что тот звонок исходил от нарушителя.

Стоит обратить внимание на публикации знакомых или друзей, проверить их на наличие нежелательной информации и, в случае ее присутствия, попросить их ее удалить.

Также стоит следить за безопасностью личных и рабочих устройств: установка сложные пароли, настройка двухфакторной аутентификации. Это поможет предотвратить утечку данных в результате подбора паролей.

И это лишь небольшое количество рекомендаций по уменьшению объема личной информации на просторах интернета.

К счастью, злоумышленники не будут тратить много времени на поиск информации об обычном. Но если человек медийная личность или занимает высокую должность в компании, то ему следует задуматься о своей цифровой безопасности.

Заключение. Таким образом был рассмотрен типы и методы OSINT, а также описаны базовые рекомендации противодействию методам OSINT. Собранная с помощью этого метода информация может быть использована для идентификации уязвимостей с целью предотвращения атак на человека или организацию, или для проведения атак на них. К сожалению, в настоящее время еще нет конкретных методов защиты от социальной инженерии. Поэтому необходимо принимать меры по защите своей личной информации и обучать людей основам кибербезопасности.

Библиографический список

1. Белова, Е. В. Психология управленческой деятельности : учебное пособие / Е. В. Белова. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 158 с. — ISBN 978-5-89160-202-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180301 (дата обращения: 25.11.2023). — Режим доступа: для авториз. пользователей.
2. Грей, Д. Социальная инженерия и этичный хакинг на практике : руководство / Д. Грей ; перевод с английского В. С. Яценкова. — Москва : ДМК Пресс, 2023. — 226 с. — ISBN 978-5-97060-980-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/314927 (дата обращения: 27.11.2023). — Режим доступа: для авториз. пользователей.
3. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717 (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей.5.
4. Хэднеги, К. Искусство обмана. Социальная инженерия в мошеннических схемах / К. Хэднеги ; перевод А. Соломина. — Москва : Альпина Паблишер, 2020. — 430 с. — ISBN 978-5-9614-1072-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140447 (дата обращения: 01.12.2023). — Режим доступа: для авториз. пользователей.
5. Дворянкин О.А. (2022) OSINT, пентест и нетсталкинг. [Электронный источник]. – URL: https://cyberleninka.ru/article/n/osint-pentest-i-netstalking-informatsionnye-tehnologii-interneta/viewer (дата обращения 04.12.23).
6. Сидорова М.Е., Кузьмин А. Р. (2023) Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности. [Электронный источник] – URL: https://vestnik-rosnou.ru/sites/default/files/61_PDFsam_N1.pdf (дата обращения 04.12.23).
7. OSINT: в чем опасность и как защититься [Электронный источник] – URL: https://www.kaspersky.ru/blog/osint-open-source-intelligence/35955/ (дата обращения 03.12.23).

8. OSINT или разведка по открытым источникам [Электронный источник] – URL: https://habr.com/ru/companies/deiteriylab/articles/595801/ (дата обращения 04.12.23).
9. OSINT: источники, программы и реальный кейс поиска [Электронный источник] – URL: https://vc.ru/s/reputaciya-moskva-72334/815539-osint-istochniki-programmy-i-realnyy-keys-poiska (дата обращения 04.12.23).
10. Отчет «Лаборатории Касперского» о спаме и фишинге в 2022 году [Электронный источник] – URL: https://securelist.ru/spam-phishing-scam-report-2022/106719/
11. 50+ фишинг-статистики и фактов за 2023-2023 гг .: рост фишинга с SSL-защитой [Электронный источник] – URL: https://heritage-offshore.com/vpn-i-konfidencialnost/50-fishing-statistiki-i-faktov-za-2017-2018-gg/
12. Статистика вишинга 2023: затраты на голосовые фишинговые атаки [Электронный источник] – URL: https://clickfraud.ru/statistika-vishinga-2023-zatraty-na-golosovye-fishingovye-ataki/.