Современная социальная инженерия: методы воздействия и противодействия

Я. А. Воронцов, email: jessy-black0990@yandex.ru

Воронежский государственный университет

Аннотация. *В данной работе рассматриваются техники воздействия, используемые злоумышленниками для совершения атак с использованием социальной инженерии, а также методы противодействия подобным атакам. Предпринимается попытка структурировать методы социальной инженерии в историческом контексте и на основе используемого канала коммуникации, выделить характерные черты подозрительных сообщений, а также классифицировать способы защиты от фишинга на основе управленческого и экономического факторов.*

Ключевые слова: *информационная безопасность, социальная инженерия, канал коммуникации, спам, фишинг, подозрительное сообщение, двухфакторная аутентификация.*

Введение

XXI век стал эпохой расцвета киберпреступлений, и если в начале века многие злоумышленники обычно добивались успеха из-за наличия серьёзных уязвимостей в программном обеспечении и несовершенства протоколов безопасности, то ближе к концу второй декады, благодаря появлению международных сообществ профессионалов в области информационной безопасности (здесь и далее – ИБ), отраслевых стандартов (например, семейства ISO 27001) и сертификаций, а также развития технических средств противодействия угрозам, относительная доля «технических» атак стала убывать. При этом стабильный рост абсолютного числа проблем в области ИБ сохранился, не в последнюю очередь из-за того, что злоумышленники сдвинули фокус векторов атак с техники на человека, который является самым слабым звеном в сложных современных IT-системах. В отличие от роботов и алгоритмов, живой оператор IT-системы подвержен атакам с использованием социальной инженерии, т. е. совокупности психологических и социологических приёмов, методов и технологий, которые позволяют злоумышленникам добиваться определенных целей [1, 2].

1. Цели и задачи социальной инженерии

Цели, преследуемые злоумышленниками, можно примерно ранжировать по степени их опасности для жертвы и для окружающих. Более точную классификацию (согласно статьям Уголовного кодекса) можно получить у юристов, специализирующихся в области уголовного права.

1. Розыгрыш, шутка или хулиганство.
2. Дискредитация (желание публично унизить жертву).
3. Кража денег или других материальных ценностей.
4. Кража личных данных жертвы.
5. Кража другой информации, включая конфиденциальную (например, ноу-хау компании, корпоративных учетных записей, государственной тайны и т. п.).

Обычно, в двух последних случаях кража данных является лишь первым шагом полного вектора атаки, цель которой может заключаться как в нанесении ущерба конкретному человеку, включая совершение противоправных действий от его имени, так и получении несанкционированного доступа к корпоративным компьютерным сетям и программному обеспечению.

Чаще всего, злоумышленники используют слабости человека или негативные черты характера – жадность, желание получить что-либо бесплатно («на халяву»), страх (за себя, за своих близких), невнимательность, излишнюю доверчивость [1]. Ключевой задачей социального инженера является атака на подсознание, т. е. фактически временный перевод жертвы в такое состояние, в котором она не способна рационально мыслить, и, таким образом, шире открывает окно возможностей для атаки. Согласно отчёту Microsoft Digital Defense Report за 2022 год, современному злоумышленнику требуется в среднем около 80 минут, чтобы получить доступ к учетным записям жертвы социальной инженерии с использованием поддельного сайта для кражи паролей, и около 100 минут, чтобы начать продвижение по корпоративной сети с использованием украденных учетных данных [3].

2. Типы атак с использованием социальной инженерии

Удобнее всего рассматривать типы социальной инженерии в историческом контексте, поскольку от этого контекста также зависит и используемый злоумышленниками канал связи (коммуникации) [2]:

– Vishing (вишинг) – телефонные звонки, в ходе которых злоумышленник пытается втереться в доверие к жертве и склонить её к совершению действий в своих интересах. Метод получил развитие в эпоху всеобщей домашней телефонизации и получил второе рождение в начале 2000-х в связи с массовым распространением мобильной связи.

– Phishing (фишинг) – использование злоумышленником электронной почты для мошенничества, кражи денег или учетных данных жертвы.

– Smishing (смишинг) – отправка жертве текстовых сообщений с целью вынудить её действовать в интересах атакующего. Метод становится популярным с развитием сервиса коротких текстовых сообщений у сотовых операторов. В настоящее время термин часто подразумевает социальную инженерию посредством любого сервиса обмена текстовыми сообщениями, включая мессенджеры.

Существуют и другие классификации типов атак, которые вводят более специфические сценарии использования конкретных черт характера и человеческих слабостей [1].

Отдельно в данном контексте стоит рассмотреть различия спама и фишинга. Спам, т. е. массовая рассылка не релевантной для получателя информации без его согласия, исторически возник раньше, ещё в доцифровую эпоху, и изначально распространялся через обычные почтовые ящики в виде рекламных листовок. Многие характерные приёмы (например, массовость рассылки, использование угроз, эксплуатация доверчивости и наивности получателей и т. д.), которые в настоящее время используются злоумышленниками для атак с применением социальной инженерии, были опробованы именно на спам-рассылках. Не всякий спам является вредоносным, но при этом почти любой фишинг можно отнести к спаму.

3. Как не стать жертвой злоумышленников

Вероятность того, что человек, даже не будучи активным пользователем сети Интернет, рано или поздно столкнётся приёмами социальной инженерии, высока – дело в утечках данных, которые периодически случаются как у крупных коммерческих компаний (например, у Яндекса и у СДЭК в 2022 году), так и у государственных сервисов [4]. Используя номер телефона и электронную почту как уникальные идентификаторы, злоумышленники могут обогащать уже имеющиеся у них данные после каждой новой утечки.

Поэтому, раз уж встреча с методами социальной инженерии – это всего лишь вопрос времени, то для идентификации подозрительных сообщений стоит придерживаться ряда правил.

– Во-первых, стоит всегда помнить об официальных каналах связи внутри организации и для внешних коммуникаций. Любое сообщение, полученное не по официальному каналу, следует воспринимать критически.

– Если получатель ожидает сообщения от отправителя, но после получения сомневается в его аутентичности, то рекомендуется связаться

с отправителем, используя другой доверенный канал связи (например, корпоративный мессенджер для проверки валидности почтовой рассылки).

– Следует знать о красных флагах, которые позволяют с высокой долей вероятности отнести сообщение в категорию подозрительных [5]:

- формат общения через мессенджеры или по телефону, нацеленный на управление эмоциями жертвы (например, сообщение о якобы угрозе близкому человеку);
- предупреждающие плашки от клиента электронной почты или от мессенджера о ненадёжности отправителя сообщения;
- орфографические, пунктуационные и грамматические ошибки в заголовке и тексте;
- намеренно неверное написание домена электронной почты отправителя;
- неперсонализированное обращение отправителя или необычный, отличающийся от принятого в организации, формат подписи;
- использование фраз или подписи в конце сообщения, которые свидетельствуют о коммуникации от имени якобы «авторитетного» или «доверенного» источника;
- само сообщение содержит в себе запрос на предоставление конфиденциальных данных, доступа к учетной записи или платёжной информации, при этом в случае непредоставления этой информации отправитель угрожает негативными последствиями (например, блокировкой учетной записи или банковского счёта, пропажей денег, арестом и т. п.).

– Перед открытием любых ссылок из подозрительного электронного письма рекомендуется навести курсор мышки на ссылку, чтобы дождаться появления всплывающей подсказки, которая покажет настоящий адрес ресурса. Этот пункт также касается ссылок, которые вставлены в текст сообщения в виде QR-кода – рекомендуется не использоваться автоматический переход по ссылкам в программе для сканирования кодов.

– Если письмо содержит вложения, то рекомендуется воспользоваться антивирусным ПО для их сканирования. Исполняемые файлы во вложении (*.exe) или файлы-ссылки (*.lnk) с высокой долей вероятности говорят о вредоносности сообщения.

– Обо всех подозрительных коммуникациях нужно сообщать или в отдел ИБ организации (если дело происходит в корпоративном окружении), или провайдеру электронной почты или мессенджера с

помощью стандартной функции «Сообщить о фишинге/подозрительном сообщении».

– В случае, если до конца не удаётся установить достоверность сообщения, его следует трактовать как подозрительное и действовать с ним в соответствие с предыдущим пунктом.

4. Противодействие атакам с использованием социальной инженерии.

Большинство специалистов в области ИБ отмечают, что не существует такого подхода, который позволил бы на 100% предотвратить социальную инженерию. Поэтому главное при противодействии – системность и многоканальность, т. е. воздействие на потенциальных жертв разными способами. При этом также стоит принять популярную в области ИБ точку зрения о том, что атакующая сторона всегда находятся на шаг впереди защищающейся, поэтому жертва может столкнуться с не знакомыми ранее новыми техниками атаки.

Практически все предлагаемые ниже методы противодействия социальной инженерии будут действовать одинаково хорошо как в контексте защиты личных данных и домашних компьютеров, так и при защите корпоративных и государственных сетей и систем хранения данных. Для простоты классификации стоит выделить симметричные методы, связанные с анализом подозрительных сообщений, и асимметричные, которые позволяют снизить риск успешной атаки, при этом не воздействуя непосредственно на источники проблемы.

Для начала рассмотрим асимметричные методы, поскольку они являются наиболее эффективными с экономической точки зрения и обеспечивают максимальное снижение риска успешной атаки при минимуме затрат на реализацию:

– Установка двухфакторной аутентификации для ключевых учетных записей (например, социальные сети, электронная почта – личная и корпоративная). При наличии технической возможности рекомендуется отказаться от использования SMS-кодов в качестве второго фактора и пользоваться специальными аппаратными брелоками или генераторами одноразовых кодов (например, Yubikey) [3].

– Использование специализированного ПО для хранения паролей. Данная мера позволяет иметь уникальные пароли для каждого веб-ресурса и отказаться от порочной практики повторного использования паролей. Кроме того, использование менеджера паролей позволит избежать необходимости ротации паролей на всех используемых жертвой веб-ресурсах, если она всё-таки подверглась успешной атаке.

Большинство прямых методов противодействия базируются на повышении бдительности потенциальных жертв и постоянной их тренировке на наглядных примерах, а также на технических мерах защиты. Хорошей аналогией прямых методов являются меры, которые используют медики для предотвращения крупных эпидемий и пандемий – пропаганда здорового образа жизни и вакцинация, а также изоляция и карантин для уже заболевших.

– Периодический выпуск бюллетеней с актуальной информацией об угрозах социальной инженерии. Хороший тренд задали банки, которые периодически напоминают своим клиентам об угрозах, связанных с социальной инженерией, и об ответных мерах, которые клиенты должны предпринимать клиенты для того, чтобы не оказаться в числе жертв. В случае возникновения нового вектора атаки крайне рекомендуется обновить содержимое бюллетеня и провести внеочередную рассылку-оповещение.

– Тестирование сотрудников предприятий на устойчивость к социальной инженерии. Тема тестирования стала особенно популярной в 2020 году в связи с эпидемией COVID-19 и переводом множества сотрудников на удалённый режим работы. Стоит отметить, что среди наиболее популярных провайдеров в области обучения кибербезопасности (Phishing Box, KnowBe4, InfoSec IQ, SANS Institute) нет консенсуса по поводу использования унифицированных метрик, поэтому инструменты для проведения тестов обычно позволяют определить три ключевые метрики – процент открывших/прочитавших письмо (Open Rate), процент проваливших тест (Click/Failure Rate) и процент оповестивших отдел ИБ об атаке (Report Rate) [6]. Тем не менее, как показывают некоторые зарубежные исследования, низкий процент провалившихся не является хорошим показателем устойчивости организации в целом к социальной инженерии [7].

– Использование технических средств защиты против злоумышленников [3]. Сюда можно отнести системы защиты электронной почты, антивирусное ПО с системой фильтрации сетевого контента, брандмауэры нового поколения (NGFW), унифицированные решения по управлению угрозами (UTM). Большинство данных средств пассивно или активно сканирует сетевой трафик и, в случае обнаружения попытки доступа к подозрительному ресурсу, блокирует переход по опасному адресу. Для поддержания работоспособности подобных решений используются как «чёрные списки», так и репутационные оценки ресурса, которые динамически вычисляются провайдерами технических решений.

Список литературы

1. Ромачев, Р. В. Практический курс HUMINT для частной разведки / Р. В. Ромачев. – М. : Горячая линия – Телеком, 2022. – 340 с.: ил

2. Осторожно, это ловушка: что такое социальная инженерия [Электронный ресурс] : REG.RU / Блог. – Режим доступа: https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/

3. Microsoft Digital Defense Report 2022 [Электронный ресурс] : State of Cybercrime / Microsoft Security. – Режим доступа: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-state-of-cybercrime

4. На крючке: как изменился фишинг в 2022 году, и на чато мошенники ловили своих жертв [Электронный ресурс] : Хаб «Информационная безопасность» / Хабр. – Режим доступа: https://habr.com/ru/company/solarsecurity/blog/708694/

5. Социальная инженерия глазами жертвы [Электронный ресурс]: Хаб «Информационная безопасность» / Хабр. – Режим доступа: https://habr.com/ru/post/707426/

6. Lewis J. How to measure a phishing test program [Электронный ресурс]: Cira.ca blog. – Режим доступа: https://www.cira.ca/blog/cybersecurity/phishing-test-metrics-measurement

7. Shipley D. The hard truth about phishing simulation click rates [Электронный ресурс]: LinkedIn Pulse. – Режим доступа: https://www.linkedin.com/pulse/hard-truths-phishing-simulation-click-rates-david-shipley/