УДК 004.056.5

ЭВОЛЮЦИЯ СЦЕНАРИЕВ АТАКИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В.А. Зорин
НИУ МИЭТ
Россия, Москва, Зеленоград, площадь Шокина, 1
E-mail: v.a.zorin@mail.ru

Ключевые слова: Социальная инженерия, фишинг, вишинг, эволюция методов атаки, генеративные сети, искусственный интеллект.

Аннотация: Настоящая статья разработана на основе практических случаев противодействия атакам злоумышленников, использующих методы социальной инженерии и на основе аналитических обзоров и мнения экспертов в области построения систем информационной безопасности. Приведен сценарий атаки, использующий методы социальной инженерии. Обозначены риски при использовании технологий искусственного интеллекта и генеративных сетей.

1. Введение

Манипуляционный подход, сторонниками которого являются К. Митник, А.А. Сиротский, Т.Ф. Байрушин, А.А. Казыханов, определяет термин «Социальная инженерия» как целенаправленное воздействие с целью получения определенного социального действия. Характеризуется психологическим внедрением информации и изменения посредством данного внедрения определенных психологических реакций людей, таких как привычка, интерес, доверие. Чаще всего манипуляции направлены на достижение ожидаемой материальной или нематериальной выгоды, которая, как правило, оказывается очевидной для субъекта манипулятивного воздействия.

Эволюция манипуляций в контексте социальной инженерии использует все доступные способы.

Метод атаки, используемый в социальной инженерии, обычно состоит из различных сценариев фишинга. Фишинг (fishing) – вид мошенничества, при котором основной целью злоумышленников является получение персональных данных клиентов или работников организации, в частности доступа к мобильным номерам, электронным почтам, данным банковских карт, логинам, паролям. Фишинг является одной из разновидностей социальной инженерии, основанной на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Фишинг, являясь реальной угрозой для организаций, клиентов и работников, пользуется популярностью в Интернете злоумышленниками различного уровня: от мелких Интернет-мошенников, преследующих свою финансовую выгоду, до специализированных крупных группировок, целью которых может быть уничтожение информационных систем и репутации целый корпораций и государственных институтов. Первые фишинговые атаки были отмечены в конце XX в., и на сегодняшний день, по оценке компании «Google» каждый год от фишинга страдают до 12,4 миллионов пользователей сети Интернет.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая именуется «антифишинг».

2. От фишинга до вишинга

На смешу фишингу часто приходит вишинг (vishing) – устная разновидность мошенничества, при которой злоумышленники, используя телефонную коммуникацию, под разными предлогами стимулируют людей к совершению действий якобы в их собственных интересах [1].

Вишинг использует психологические приёмы, направленные на создание стрессовой ситуации и насаждение жертве таких чувств как вина и стыд (нелицеприятные факты из переписок, социальных сетей, случайных свидетельств), страх (боязнь уголовного преследования, людей в форме), азарт и жадность (случайный выигрыш, перспектива «легких» денег) и главный компонент – доверие, который и позволяет совершать манипуляции.

Данный вид мошенничества опасен тем, что он постоянно модифицируется исходя из условий, которые меняются практически сиюминутно и подстраивается под актуальные информационные условия [2].

3. Сценарий злоумышленника

В 2023 году большое количество работников ведомств (органов исполнительной власти и подведомственных организаций) Российской Федерации подверглось атаки мошенников. Алгоритм действий злоумышленников заключался в следующем:

1. **Создание фейковой страницы руководителя ведомства в мессенджере Telegram**.

Выбор данного мессенджера обусловлен возможностью скрыть настоящий номер, на который зарегистрирован аккаунт. В большинстве случаев, когда злоумышленники пользовались мессенджером WhatsApp* (**компания Meta признана экстремистской и запрещена в России*), номера атакующего были виртуальными, либо зарегистрированы на территории недружественных для России стран. При использовании Telegram, злоумышленники оформляли аккаунт таким образом, чтобы была официальная фотография руководителя ведомства и наименование в виде «Фамилия Имя». Иногда в разделе «bio» был указан действительный номер руководителя, но не настоящий аккаунта.

2. Рассылка персонализированных сообщений работникам организации с информацией о том, что с ними свяжется представитель Службы внутренней безопасности вышестоящего ведомства.

Вероятнее всего работа производилась по базам данным, которые были украдены злоумышленниками в период массовых атак на сервера в начале 2022 года. Сообщение от фейкового руководителя направлено на создание страха неопределенности и важности предстоящего звонка.

3. Звонок фейкового представителя службы внутренней безопасности с аккаунта Telegram.

Звонивший как правило представлялся Службой безопасности и в наименовании звонившего содержалась информация в виде «Имя Отчество» для создания особой важности и статусности звонившего. Жертве атаки сообщалась информация об утечке

информации о персональных данных, в связи с чем на имя жертвы были оформлены «мошенниками» кредиты в банковских организациях. Чтобы пресечь работу «мошенников», необходимо их вычислить при получении денежных средств и пока проводится оперативная работа, жертве требуется оформить кредит в другой организации, чтобы закрыть заявку «мошенника», чтобы в банке не было долга. Легенда подразумевала, что при обращении «мошенника» в банк за деньгами, его сразу поймают.

4. **Звонок от фейкового сотрудника финмониторинга**.

В наименовании звонившего аналогичным образом содержалась информация в виде «Имя Отчество» для создания такой же важности и статусности звонившего. Атакующий создавал видимость подтверждения информации о банковских запросах и кредитах. Направлял жертве поддельные справки якобы от финмониторинга, создавая ощущение реальности и правдоподобия происходящего.

5. Изоляция жертвы и удержание в страхе.

Манипуляции сводились к тому, что о фейковой операции по разоблачению «мошенников» никому нельзя сообщать. Ни родственникам ни близким, ни коллегам, мотивировав тем, что «мошенники» могут прослушивать телефон, а фейковая служба безопасности и фейковый представитель финмониторинга звонили по защищённому каналу связи.

6. Работа с сомнениями у жертвы атаки.

У жертв возникали сомнения в том, что происходящее действительно может каким-то образом помочь сохранить личные средства и помочь поимке «мошенника». Однако существующая традиция в корпоративной культуре российских организаций и органах власти, как правило, дистанцирует рядовых работников от руководителей, в связи с чем жертва не решается звонить настоящему руководителю для уточнения информации. Вместо этого жертва пользуется установленным каналом связи и пишет фейковому аккаунту руководителя о разъяснении степени доверия представителям службы безопасности и финмониторинга, на что получает закономерный ответ злоумышленника о необходимости полного содействия.

Кроме того, жертве сообщали о том, что работники банков могут предупреждать о том, что кредиты могут браться в целях злоумышленников, однако о проводимой операции по поимке «мошенников» им сообщать не следует и во время операции по оформлению кредита жертва должна оставаться на связи со злоумышленниками.

Опыт показывает, что только не в каждом из банковских учреждений предупреждали о возможных действиях злоумышленников. Кроме того, работники банков замотивированы выдавать кредиты, поскольку данный показатель часто присутствует в коэффициентах полезной эффективности и напрямую влияет на формирование денежного вознаграждения.

4. Риски эволюции методов социальной инженерии

Социальная инженерия как метод атаки отмечалась в 2023 году в 42% успешных атак на государственные организации, что сопоставимо с ситуацией в 2022 г. (41%), и данное направление имеет все признаки развития и повсеместного использования злоумышленниками. При этом доля такого метода атаки как эксплуатация уязвимостей на внешнем сетевом периметре компаний, составила лишь 24%.

Стратегия проникновений меняется во всём мире. Причина тому – новые технологии и рост профессионализма хакеров. Например, злоумышленники активно используют генеративные сети, такие как ChatGPT, с помощью которых создают грамотные и вызывающие доверие фишинговые письма [1,2].

Успехи чат-ботов на базе генеративных сетей, а также других технологий из области искусственного интеллекта потенциально ведут к их активному использованию в повышении эффективности методов социальной инженерии.

Злоумышленники решают две основные задачи при эволюции методов: повышение убедительности и обход систем автоматического распознавания. Встречаются как модульные инструменты для создания убедительных фишинговых сайтов и переписок, так и многоэтапные атаки: в которых злоумышленники достигают цели за несколько шагов, применяя совместно различные методы воздействия [3].

Следует сделать прогноз, что производители средств защиты информации будут развивать соответствующие технологические решения с применением технологий искусственного интеллекта. Вполне логичным шагом должна быть имплементация продуктов в области безопасности, нацеленных на противодействие применения искусственного интеллекта злоумышленниками. Например, применение графовой нейронной сети, способной распознавать подозрительные транзакции и отличать злоумышленников от честных пользователей [4].

Кроме того, должно быть популяризированы российские приложения, которое способны опознать злоумышленников в начале телефонного разговора и предупредить об этом пользователя. Примечательно, что в случае, если пользователь не обратит внимание на уведомление и продолжит общение, приложениям доступна функция разрыва сеанса связи [5].

При атаке методом социальной инженерии важнейшим фактором является доверие жертвы к злоумышленнику. При этом чем более персонализированным является контент, тем выше уровень доверия и больше вероятность, что жертва выполнит требования, атакующего: перейдёт по ссылке, установит вредоносную программу, выполнит денежный перевод. Злоумышленники для подобных атак уже сейчас активно используют искусственный интеллект для анализа жизни и бизнеса пользователей, подготовки персонализированного контента, создания имитаций голоса и видео, способных вызвать доверие и побудить на требуемую реакцию. На данный момент известны случаи, когда человек не смог отличить настоящий контент от поддельного, созданного нейросетями по технологии дипфейков, что привело к материальным либо репутационным потерям. Например, в Китае злоумышленник, изменив голос, выдал себя за близкого друга предпринимателя и убедил его сделать перевод на сумму порядка 600 000 долларов США. По данным аналитиков, количество подобных случаев в 2023 году увеличилось в три раза по сравнению с 2022-м [3].

Дипфейки способны создавать образы фейковых аккаунтов, которые будут вызывать больше доверия у жертвы. При этом дипфейки потенциально могут дискредитировать реальных в том числе руководителей организаций и ведомств, в котором работает потенциальная жертва. В 2023 году активно использовались злоумышленниками в качестве как одного из инструментов для социальной инженерии, так и механизма пропаганды на фоне сложной геополитической обстановки.

Применение алгоритмов нейролингвистического программирования со стороны злоумышленников несут риски эволюции целей злоумышленников от финансового обогащения и финансирования запрещённых организаций до разрешения личности вплоть до физического уничтожения жертвы или манипуляции жертвы для атаки на иные физические лица, либо объекты инфраструктуры.

Эволюция методов социальной инженерии в то же время требует качественного подхода к обучению персонала так называемой кибергигиене и постоянного повышения квалификации. Обучение и просвещение персонала в области информационной безопасности должно внедряться во всех отраслях народного хозяйства. Особое внимание следует уделять представителям старшего поколения,

воспитанного в духе доверия и обладающего низким уровнем использования электронных средств и гаджетов в повседневной жизни.

5. Заключение

В настоящей статье рассмотрены сценарии атаки с применением методов социальной инженерии. Приведен сценарий атаки, основанный на практических случаях противодействия атакам злоумышленников, использующих методы социальной инженерии и на основе аналитических обзоров и мнения экспертов в области построения систем информационной безопасности. Рассмотрен сценарий атаки, использующий методы социальной инженерии с расширенным описанием целей и способов воздействия. Обозначены риски при использовании злоумышленниками технологий искусственного интеллекта и генеративных сетей в методах социальной инженерии. А также приведены прогнозы по развития средств противодействия злоумышленникам.

Список литературы

1. https://www.kaspersky.ru/resource-center/definitions/vishing (дата обращения 10.01.2024).
2. Санина Л.В., Чепинога О.А., Ржепка Э.А., Палкин О.Ю. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения // Baikal Research Journal. 2021. Т. 12, № 2.
3. https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast/ (дата обращения 20.12.2023)
4. https://minobrnauki.gov.ru/press-center/news/nauka/68435/ (дата обращения 10.01.2024).
5. https://iz.ru/1192463/olga-kolentcova/spetcialnaia-inzheneriia-neiroset-opoznaet-moshennika-vo-vremia-razgovora (дата обращения 10.01.2024).