УДК 343.72

СПОСОБЫ РАСПОЗНАВАНИЯ И ПРЕДОТВРАЩЕНИЯ ФИШИНГОВЫХ АТАК

А.С. ПЕТРОВСКАЯ
(Представлено: канд. юрид. наук, доц. Ю.Л. ПРИКОЛОТИНА)

Фишинговые атаки, начальным этапом которых являются действия злоумышленника, использующего методы социальной инженерии, на данный момент являются одним из самых распространенных видов кибер-атак. Статья посвящена способам их распознавания и предотвращения.

В настоящее время одним из самых распространенных методов получения конфиденциальной информации является фишинг (термин образован от игры слов password harvesting fishing – «ловля паролей»). Фишинг можно охарактеризовать как тип компьютерного мошенничества, который использует принципы социальной инженерии с целью получения от жертвы конфиденциальной информации [1]. По мнению Ю.М. Резника, социальная инженерия характеризуется манипулятивными воздействиями на индивида и представляет собой внедрение инженерного подхода в социальную область, использование инженерной деятельности, в частности создание и обслуживание разного рода систем, их конструирование и проектирование. В более узком смысле социальную инженерию возможно определить как область научных знаний и прикладной деятельности для создания и обслуживания социальных систем искусственного типа [1]. Киберпреступники обычно осуществляют свои действия при помощи электронной почты, сервисов мгновенных сообщений или SMS, посылая фишинговое сообщение, в котором напрямую просят пользователя предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносного программного обеспечения при нажатии ссылки и т.д.), благодаря чему получают желаемое при полном неведении со стороны жертвы [2].

Фишинговые атаки, судя по всему, являются предпочитаемой злоумышленниками формой завладения данных, поскольку требуют меньше времени, чем взлом и при этом приносят значительный доход лицу, совершившему данное умышленное деяние.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. Так, хотя на многих сайтах, требующих конфиденциальной информации, опубликованы специальные предупреждения о том, что они никогда не просят сообщать свои конфиденциальные данные в письмах, пользователи продолжают отправлять свои пароли мошенникам таким способом.

Безопасность основывается на знании о том, кому и чему доверять. Важно знать, когда не следует доверять человеку на слово, и когда человек, с которым мы ведем общение, действительно является тем, кем себя называет. Тот же принцип актуален и в отношении онлайн-взаимодействия и использования веб-сайта: когда гражданин уверен, что веб-сайт, который он использует, является законным или безопасным для предоставления его информации?

В связи с этим, возникает вопрос: каким образом человек может распознать фишинговую атаку, если он обнаружил подозрительное сообщение от злоумышленника?

1. Письмо содержит ссылку, по которой должен перейти атакуемый. Последний должен перейти на определенный веб-ресурс, где, используя уязвимости самого сайта или браузера пользователя, мошенники попытаются внедрить вредоносное программное обеспечение. Для осуществления таких действий злоумышленниками специально создаются фишинговые сайты, время жизни которых невелико. Чаще всего они являются точными копиями известных сайтов, повторяя их дизайн, структуру и функциональность. При переходе по ссылке пользователь становится жертвой различных видов XSS-атак. Суть данных атак заключается в выполнении скрипта в браузере и последующем его взаимодействии с сервером злоумышленника. Эти операции позволяют получить доступ к данным браузера и дают возможность применять к нему эксплойты, а также получать cookie, данные авторизации или, например, выполнять HTTP-запросы от имени пользователя [3]. Важно отметить, что на сегодняшний момент «фишеры» рекламируют свои ресурсы в социальных сетях и поисковых системах и выводят в топы ссылки на свои фишинговые сайты.

2. Внутри письма размещено вредоносное вложение. В качестве вложения в фишинговое письмо злоумышленник может поместить имитацию отчета коллеги за предыдущий месяц, задание от руководителя или сообщение от банка, приславшего пользователю иск за неуплату по кредиту. Вложения бывают в форматах *.doc или *.pdf. Файлы формата *.pdf часто содержат объекты JavaScript. Поэтому для злоумышленника достаточно просто создать некоторый скрипт, который использовал бы одну из уязвимостей движка от Adobe [4]. В документах Microsoft Office вредоносное ПО может загружаться при помощи макросов, которые содержит файл. При открытии документа исполнение макроса позволяет установить соединение с сервером злоумышленника и начать загрузку. Для защиты от данного вида писем в рамках политики безопасности в организациях необходимо отключать поддержку макросов. Но, если пользователь не соблюдает политику безопасности, то при использовании социальной инженерии, злоумышленник может заставить его отключить защиту от макросов [5].

На данный момент большинство способов эксплуатации уязвимостей пакета прикладных программ Microsoft Office не требуют использования макросов. Например, используя самую популярную уязвимость 2017 года CVE-2017-0199 [6], при открытии вложенного *.rtf файла можно подгрузить HTA приложение, поддерживающее исполнение сценариев со стороннего сервиса и запустить его. Помимо рассмотренных случаев существует множество других офисных продуктов и форматов, с которыми они работают. Но принцип атаки один и тот же – запустить скрытый сценарий, который позволит загрузить ПО злоумышленника на атакуемый компьютер. Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и Offensive Ware Multi Exploit Builder (OMEB) [7].

3. В электронном письме просят подтвердить персональную информацию: если получаем электронное письмо, которое выглядит подлинным, но кажется совершенно неожиданным, то это явный признак того, что письмо могло прийти от поддельного и ненадежного отправителя.

4. Неправильно написанные слова, плохая грамматика или странный фразеологический оборот также являются предупреждающим знаком попытки фишинга.

5. Сообщения, оказывающие серьезное давление: если нам кажется, что сообщение предназначено для того, чтобы мы запаниковали и немедленно предприняли какие-то меры, то, наоборот, действуем крайне осторожно – скорее всего, мы столкнулись с распространенной среди кибер-преступников техникой [6].

В недавней фишинговой кампании группа 74 (также известная как Sofact, APT28, Fancy Bear) нацелилась на профессионалов в области кибербезопасности. Было написано электронное письмо, якобы связанное с конференцией Cyber Conflict U. S. conference и мероприятиями, организованными United States Military Academy Army Cyber Institute, NATO Cooperative Cyber Military Academy и NATO Cooperative Cyber Defence Centre of Excellence. Хотя CyCon– это настоящая конференция, вложение являлось документом, содержащим вредоносный макрос Visual Basic для приложений (VBA), который загружал и запускал вредоносное программное обеспечение, называемое Seduploader [8]. Хотя атакуемыми были специалисты по безопасности, которые имеют обширные знания в области инструментария злоумышленников, атака была проведена успешно и злоумышленником удалось получить личные данные большого количества специалистов по безопасности.

Еще одним ярким примером фишинговой атаки является атака Energetic Bear, которая включает в себя рассылку фишинговых писем с вредоносным содержимым. Основными целями этой атаки являются предприятия топливно-энергетического комплекса и другие промышленные предприятия. Проведение такой атаки помогает злоумышленнику провести сканирование скомпрометированных систем на наличие уязвимостей.

Говоря о распознавании фишинговых атак, немаловажным будет сказать и о структуре фишинговой атаки.

Фишинговая атака предполагает несколько этапов (рисунок). Первым этапом, как и в любых других видах атак, является планирование. На данном этапе проводится разведка, анализ уязвимостей и выбор уловки.

Следующим шагом является выяснение нужных адресов электронной почты: злоумышленники покупают списки на других теневых ресурсах и получают конкретный список для рассылки писем по действующим адресам либо путем внедрения вредоносного программного обеспечения, которое собирает адреса.

Затем регистрируется домен и создается фальшивый веб-сайт, с правдоподобным видом, на который будут перенаправляться жертвы и на этом же этапе происходит составление фишинговых писем.

После этого мошенники реализуют атаку: отправляют письма и внедряют вредоносное программное обеспечение. Далее производится сбор информации, злоумышленники получают учетные данные или другие сведения о банковских счетах жертв, с помощью которых крадут данные и (или) денежные средства, они используют информацию в своих целях и шантажируют пользователей. Заключающим этапом структуры целевой фишинговой атаки является сокрытие присутствия злоумышленника в системе. Этот этап направлен на маскирование злоумышленника и, в отдельных случаях, на внедрение вредоносного программного обеспечения, который позволит скрыть метаданные злоумышленника и повлиять на системные журналы и журналы безопасности, которые могли зафиксировать те или иные действия злоумышленника в системе.

Рисунок. – Структура фишинговой атаки

Узнав о способах распознавания и процесса реализации фишинговых атак в информационном пространстве, требуется ответить на вопрос: как предотвратить совершение новых форм атак?

Основным способом предотвращения атак, основанных на методах социальной инженерии, является обучение физических лиц, индивидуальных предпринимателей и юридических лиц. Все лица должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации, а также о способах предотвращения утечки данных. Кроме того, у каждого субъекта, в зависимости от подразделения и должности, должны быть инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить субъект для получения той или иной информации от другого пользователя [9].

Кроме этого, намного чаще фишинговые атаки совершаются именно в компаниях, где каждому сотруднику от компании предоставляются авторизационные данные. Поэтому особое внимание требуется уделить следующие правилам информационной безопасности для них:

1. Пользовательские учетные данные являются собственностью компании. Всем сотрудникам в день приема на работу должно быть разъяснено то, что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.
2. Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности. Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.
3. Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации. Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.
4. На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение. На компьютерах сотрудников также необходимо установить брандмауэр.
5. В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак. Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фитиновых атак.
6. Все сотрудники должны быть проинструктированы, как вести себя с посетителями. Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетители в службу безопасности.
7. Необходимо максимально ограничить права пользователя в системе. Например, можно ограничить доступ к web-сайтам и запретить использование съемных носителей. Ведь, если сотрудник не сможет попасть на фишинговый сайт или использовать на компьютере флеш-накопитель с «троянской программой», то и потерять личные данные он также не сможет [9].

Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии – это обучение сотрудников и пользователей, в принципе. Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку. Предупрежден – значит вооружен!

ЛИТЕРАТУРА

1. Резник, Ю.М. Социальная инженерия: предметная область и границы применения / Ю.М. Резник // Журнал СОЦИС. – 1994. – № 2. – С. 87–95.
2. Социальная инженерия, или как «взломать» человека [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/. – Дата доступа: 13.07.2021.
3. Verizone. 2020 Data Breach Investigations Report [Электронный ресурс]. – Режим доступа: https://enterprise.verizon.com/resources/reports/dbir/. – Дата доступа: 28.09.2021.
4. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing [Электронный ресурс]. – Режим доступа: https://dl.acm.org/citation.cfm?Id=3025831. – Дата доступа: 28.09.2021.

5. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks [Электронный ресурс]. – Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3171727. – Дата доступа: 28.09.2021.
6. National vulnerability Database [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln/detail/cve-2017-0199. – Дата доступа: 28.09.2021.
7. High-Tech Crime Trends 2017 [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/resources/threat-research/2017-report.html. – Дата доступа: 28.09.2021.
8. Типы фишинговых атак и способы их выявления [Электронный ресурс]. – Режим доступа: https://www.osp.ru/winitpro/2019/03/13054903. – Дата доступа: 28.09.2021.
9. Социальная инженерия – как не стать жертвой [Электронный ресурс]. – Режим доступа: https://efsol.ru/articles/social-engineering.html. – Дата доступа: 28.09.2021.