Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский государственный технический университет имени Н.Э. Баумана

(национальный исследовательский университет)»

(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ: Информатика и системы управления

КАФЕДРА: Компьютерные системы и сети

НАПРАВЛЕНИЕ ПОДГОТОВКИ: 09.04.01 Информатика и вычислительная техника

МАГИСТЕРСКАЯ ПРОГРАММА 09.04.01/04 Компьютерный анализ и интерпретация больших данных.

О т ч е т

по рубежному контролю 3

Дисциплина: Искусство аналитической работы с большими данными

Название: Основные виды фишинга и методы защиты от них

студент группы ИУ6-22М _____ **Астахов С.В.**
(Подпись, дата) (Фамилия И.О.)

студент группы ИУ6-22М _____ **Гендина Н.Б**
(Подпись, дата) (Фамилия И.О.)

студент группы ИУ6-22М _____ **Баканов Р.В.**
(Подпись, дата) (Фамилия И.О.)

студент группы ИУ6-22М _____ **Кадыров Т.И.**
(Подпись, дата) (Фамилия И.О.)

Преподаватель _____ **Березкин Д.В.**
(Подпись, дата) (Фамилия И.О.)

Москва, 2024

Введение

Фишинг является одной из наиболее распространенных и опасных киберугроз в современном мире. Это вид мошенничества, целью которого является получение конфиденциальной информации пользователей, такой как логины, пароли и данные банковских карт, под видом надежных организаций или лиц. Злоумышленники используют различные методы для осуществления фишинговых атак, включая поддельные веб-сайты, фальшивые электронные письма и сообщения в социальных сетях.

Для эффективной борьбы с фишингом необходимо знать его основные виды и способы защиты от них.

В данной работе рассмотрено использование межсайтовой подделки запроса запроса в фишинговых атаках, фишинг с использованием электронной почты, сотовых звонков и дипфейков.

В данном случае, обозначенные выше инструменты не являются взаимоисключающими и могут использоваться на разных этапах реализации атаки или даже параллельно.

Также, в работе рассмотрены основные виды защиты от фишинга, такие как повышение компьютерной грамотности населения и использование специализированного ПО для защиты от фишинга.

1. Межсайтовая подделка запроса

Помимо понятного человеку без технического образования сценария фишинга, когда злоумышленник хочет заполучить тем или иным обманным путем от пользователя его логин и пароль, паспортные данные и т.п., существуют и фишинговые атаки с использование такой технологии, как CSRF.

CSRF (англ. cross-site request forgery — «межсайтовая подделка запроса», также известна как XSRF) — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Для осуществления данной атаки жертва должна быть аутентифицирована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя, которое не может быть проигнорировано или подделано атакующим скриптом.

Данный тип атак, вопреки распространённому заблуждению, появился достаточно давно: первые теоретические рассуждения появились в 1988 году, первые уязвимости были обнаружены в 2000 году. А сам термин ввёл Питер Уоткинс в 2001 году.

Основное применение CSRF — вынуждение выполнения каких-либо действий на уязвимом сайте от лица жертвы (изменение пароля, секретного вопроса для восстановления пароля, почты, добавление администратора и т. д.).

Пример. Атака осуществляется путём размещения на веб-странице ссылки или скрипта, пытающегося получить доступ к сайту, на котором атакуемый пользователь заведомо (или предположительно) уже аутентифицирован. Например, пользователь Алиса может просматривать форум, где другой пользователь, Боб, разместил сообщение. Пусть Боб

создал тег <img>, в котором в качестве источника картинки указал URL, при переходе по которому выполняется действие на сайте банка Алисы:

Боб: Привет, Алиса! Посмотри, какой милый котик: <img src="http://bank.example.com/?account=Alice&amount=1000000&for=Bob">

Если банк Алисы хранит информацию об аутентификации Алисы в куки, и если куки ещё не истекли, при попытке загрузить картинку браузер Алисы отправит куки в запросе на перевод денег на счёт Боба, чем подтвердит аутентификацию Алисы. Таким образом, транзакция будет успешно завершена, хотя её подтверждение произойдет без ведома Алисы.

Защита. Защищаться должны все запросы, изменяющие данные на сервере, а также запросы, возвращающие персональные или иные чувствительные данные.

Наиболее простым способом защиты от данного типа атак является механизм, когда веб-сайты должны требовать подтверждения большинства действий пользователя и проверять поле HTTP_REFERER, если оно указано в запросе. Но этот способ может быть небезопасен, и использовать его не рекомендуется.

Другим распространённым способом защиты является механизм, при котором с каждой сессией пользователя ассоциируется дополнительный секретный уникальный ключ, предназначенный для выполнения запросов. Секретный ключ не должен передаваться в открытом виде, например, для POST-запросов ключ следует передавать в теле запроса, а не в адресе страницы. Браузер пользователя посылает этот ключ в числе параметров каждого запроса, и перед выполнением каких-либо действий сервер проверяет этот ключ. Преимуществом данного механизма, по сравнению с проверкой Referer, является гарантированная защита от атак CSRF. Недостатками же являются требование возможности организации пользовательских сессий, требование динамической генерации HTML-кода страниц сайта, а также необходимость защиты от XSS и других атак, позволяющих злоумышленнику получить уникальный ключ.

2. Фишинг с использованием электронной почты

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная 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.

На заре интернет-эпохи фишинг с использованием электронной почты был весьма широко распространен, т.к. в отличии, от, например, телефонного мошенничества, автоматизировать регистрацию фейковых почтовых ящиков и организовать спам-рассылки было проще, чем организовать мошеннический колл-центр. Однако, со временем компьютерная грамотность интернет пользователей значительно выросла, а крупные компании ввели алгоритмы защиты от фишинга в своих продуктах.

Защита. Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) специалисты советуют связаться с компанией,

от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, эксперты рекомендуют самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении.

Другим направлением борьбы с фишингом является создание списка фишинговых сайтов и последующая сверка с ним. Подобная система существует в браузерах Internet Explorer, Mozilla Firefox, Google Chrome, Safari и Opera. Firefox использует антифишинговую систему Google. Opera использует чёрные списки PhishTank и GeoTrust и списки исключений GeoTrust. По результатам независимого исследования 2006 года Firefox был признан более эффективным в обнаружении фишинговых сайтов, чем Internet Explorer.

В 2006 году появилась методика использования специальных DNS-сервисов, фильтрующих известные фишинговые адреса: этот метод работает при любом браузере и близок использованию hosts-файла для блокировки рекламы.

Специализированные спам-фильтры могут уменьшить число фишинговых электронных сообщений, получаемых пользователями. Эта методика основывается на машинном обучении и обработке естественного языка при анализе фишинговых писем.

3. Телефонное мошенничество

Телефонное мошенничество (англ. vishing, от voice phishing[1]) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка или правоохранительных органов, покупателя и т.д.), под разными предлогами выманивают у держателя платёжной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим банковским счётом / платёжной картой.

Бывает следующих типов:

- прямое выманивание денег, когда мошенники звонят от имени родственника и просят деньги;
- шантаж, когда мошенники звонят от имени работника правоохранительных органов;
- банковское мошенничество, когда на мобильный телефон звонят мошенники, представляющиеся сотрудниками банка или службы безопасности;
- также мошенники могут применять звонки, чтобы вынудить установить мошенническое приложение или перейти по ссылке в СМС.

Защита. Методы защиты аналогичны методам защиты от фишинга по электронной почте:

- информирование населения о мошеннических схемах и способах их распознавания;
- установка специализированного программного обеспечения, такого как Kasperski WhoCalls.

4. Фишинг с использованием дипфейков

Кроме давно известных видов фишинга, мир стоит перед угрозой использования технологий ИИ в злоумышленнических целях. В будущем возможно будет применять дипфейки для генерации видео и аудио-сообщений от лица близких с просьбой передать какую-либо конфиденциальную информацию

Несмотря на то, что на данный момент не существует надежных и универсальных технологий распознавания дипфейков, стоит предположить, что для если подобное явление приобретет хоть сколько-то массовый характер, качество сгенерированных материалов будет уступать дипфейкам звезд и политиков, буду использоваться несколько базовых нейросетей и т.д., что повысит точность распознавания.

Защита. Помимо пока что недостаточно развитых технологий распознавания дипфейков предлагается:

- информирование населения о мошеннических схемах и способах их распознавания, в том числе об угрозе использования дипфейков; просьба повторно отправить сообщение в другом приложении или подтвердить личность сообщением личного факта;
- отключение возможности перехвата потока записи видео-сообщений со стороны разработчиков мессенджеров и мобильных ОС (невозможно отправить видео-сообщение видео не с камеры устройства).

Заключение

Несмотря на свою долгую историю, фишинг является одной из актуальных угроз в сфере кибер-безопасности.

Для эффективной борьбы с фишингом необходимо знать его основные виды и способы защиты от них.

В данной работе рассмотрено использование межсайтовой подделки запроса запроса в фишинговых атаках, фишинг с использованием электронной почты, сотовых звонков и дипфейков.

В данном случае, обозначенные выше инструменты не являются взаимоисключающими и могут использоваться на разных этапах реализации атаки или даже параллельно.

Также, в работе рассмотрены основные виды защиты от фишинга, такие как повышение компьютерной грамотности населения и использование специализированного ПО для защиты от фишинга.