УДК 004.056.53

ИССЛЕДОВАНИЕ ТЕХНИК ФИШИНГА И МЕТОДОВ ЗАЩИТЫ ОТ НЕГО

О. С. Данько, Т. А. Медведева
Донской государственный технический университет, (г. Ростов-на-Дону, Российская Федерация)

Рассмотрена хронологическая последовательность появления и развития фишинга — вида мошенничества с использованием информационных технологий. На основании изучения и анализа ежегодных отчетов о фишинговой активности визуализированы в виде графиков и диаграмм основные изменения в этой области за последние десять лет. Анализируются основные методы антифишинговой защиты.

Ключевые слова: фишинг, киберпреступность, манипулирование ссылками, фальсификация сайтов, антифишинговая защита.

RESEARCH OF PHISHING TECHNIQUES AND METHODS OF PROTECTION AGAINST IT

O. S. Danko, T. A. Medvedeva
Don State Technical University (Rostov-on-Don, Russian Federation)

The article describes a history of the emergence and development of phishing – a type of fraud using information technology. Based on the study and analysis of annual reports on phishing activity, the main changes over the past ten years are visualized in the form of graphs and charts. The main methods of anti-phishing protection are analyzed.

Keywords: phishing, cybercrime, link manipulation, website forgery, anti-phishing protection.

Введение. В настоящее время происходит активный рост количества киберпреступников и киберпреступлений. В сети Интернет наиболее распространенным преступлением считается мошенничество. В этом случае жертва добровольно и сознательно предоставляет конфиденциальную информацию, которой мошенники могут воспользоваться и нанести материальный вред. Получение информации зачастую происходит посредством фишинга — вида интернет-мошенничества.

С каждым годом количество фишинг-атак растет и их методы модернизируются. Кроме того, на эффективность фишинг-атак влияет человеческий фактор, так как мошенники активно используют социальную инженерию. Следовательно, универсального способа защиты от фишинга не существует и для того, чтобы его предотвращать или предупреждать, необходимо постоянно исследовать его развитие и методы, которые используют злоумышленники.

Цель данной работы — исследование понятия фишинга и его основных техник, а также анализ методов защиты от фишинга.

История появления. Фишинг (от англ. fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого получение идентификационных данных пользователей. Согласно интернет-записям, впервые термин «phishing» был использован и зафиксирован 2 января 1996 г. Упоминание об этом произошло в группе новостей Usenet под названием «AOHell» [1].

В то время, когда американский медийный конгломерат America Online (AOL) был основным поставщиком услуг доступа в интернет, миллионы людей ежедневно входили в систему. Хакеры и те, кто торговал пиратским программным обеспечением, использовали сервис для общения друг с другом, это сообщество называлось «Warez». Именно оно в конечном итоге сделало первые шаги для проведения фишинговых атак.

Первый способ, который использовали фишеры, состоял в краже паролей пользователей и использовании алгоритмов для создания случайных номеров кредитных карт. Несмотря на то, что удачные атаки были редки, их было достаточно, чтобы нанести значительный ущерб. Случайные номера кредитных карт использовались для открытия счетов AOL. Эти учетные записи затем использовались для спама (массовой рассылки сообщений). В 1995 году компания AOL приняла меры безопасности для того, чтобы предотвратить использование случайно сгенерированных номеров кредитных карт.

После этого фишеры создали схему мошенничества, которая стала очень распространенной. Через системы мгновенного обмена сообщениями и электронной почты AOL они отправляли сообщения пользователям, выдавая себя за сотрудников AOL. Эти сообщения запрашивали у пользователей подтверждение их учетных записей или подтверждение их платежной информации.

В конце 2003 года фишеры зарегистрировали десятки доменов, которые выглядели как подлинные сайты, такие как eBay и PayPal. Они использовали почтовые программы, чтобы отправить поддельные электронные письма клиентам PayPal. Этих клиентов приводили на поддельные сайты и просили обновить данные их кредитных карт и другую идентифицирующую информацию.

К началу 2004 г фишинговые атаки стали более изощренными и результативными. За последнее десятилетие разработаны новые, более сложные методы и усовершенствованы существующие.

Описание основных методов. В настоящее время существует множество методов фишинга. Следует добавить, что фишинг-атака может использовать социальную инженерию и состоять из комбинации методов, приведенных ниже.

Email/Spam — наиболее распространенный вид фишинга. Применяет подход «spray and pray», т. е. одно и то же электронное письмо отправляется миллионам пользователей, в надежде, что фишинг-атака закончится успехом [2].

Malware — фишинговые мошенничества, связанные с вредоносными программами, которые требуют, чтобы они были запущены на компьютере пользователя. Например, ransomware — вредоносная программа, которая отказывает в доступе к устройству или файлам до тех пор, пока не будет выплачена некоторая денежная сумма. Такая программа как keylogger используется для идентификации ввода с клавиатуры. Информация отправляется хакерам, которые смогут расшифровывать пароли и другие виды информации. Вредоносная программа trojan проникает в компьютер под видом легитимного программного средства, но на самом деле осуществляет несанкционированный доступ к учетной записи пользователя. Затем полученная информация передается киберпреступникам. Вредоносное программное обеспечение обычно прикрепляется к электронному письму, отправленному пользователю фишерами, или может быть также прикреплено к загружаемым файлам.

Malvertising — это вредоносная реклама, содержащая сценарии, предназначенные для загрузки вредоносных программ или принудительного размещения нежелательного контента на устройстве пользователя.

Vishing (Voice Phishing) — метод фишинга, в котором мошенник делает телефонные звонки пользователю. Цель состоит в том, чтобы получить конфиденциальную информацию через телефон.

Smishing (SMS Phishing) — метод, который осуществляется через телефонную службу коротких сообщений (SMS). Например, текст такого сообщения пытается склонить жертву к раскрытию личной информации с помощью ссылки, которая ведет на фишинговый сайт.

Spear Phishing — является более целенаправленной атакой, при которой мошенники знают, какого конкретного человека или организацию они преследуют. Злоумышленники исследуют цель, чтобы сделать атаку более персонализированной и увеличить вероятность попадания жертвы в их ловушку.

Whaling —метод не очень отличающийся от Spear Phishing, но целевая группа становится более специфичной и ограниченной. Этот метод нацелен на руководящие должности, которые считаются важными фигурами в информационной цепочке любой организации, обычно известные как «Whale» («Кит») в терминах фишинга.

Phishing through Search Engines — метод, включающий поисковые системы, где пользователь направляется на сайты, которые могут предлагать недорогие продукты или услуги. Когда пользователь пытается купить продукт, он вводит данные платежной карты или электронного кошелька, которые собираются фишинговым сайтом.

Web Based Delivery — является одним из самых сложных методов фишинга. Также известный как «man-in-the-middle», когда хакер находится между оригинальным сайтом и фишинговой системой. Фишер отслеживает детали во время транзакции между подлинным веб-сайтом и пользователем, причем пользователь об этом не знает.

Pop-Ups — всплывающие сообщения являются одним из самых простых методов для результативного проведения фишинг-атак. Они позволяют злоумышленникам получать регистрационные данные, отправляя пользователям всплывающие сообщения и в конечном итоге приводя их на поддельные веб-сайты. Один из вариантов фишинговых атак, также известный как «in-session phishing», работает путем отображения всплывающего окна во время сеанса онлайн-банкинга и выглядит как сообщение от банка.

Session Hijacking — метод захвата сеанса, при котором фишер использует механизм управления веб-сеансом для кражи информации у пользователя.

Content Injection — это метод, при котором фишер изменяет часть контента на странице надежного веб-сайта. Это делается для того, чтобы ввести пользователя в заблуждение и отправить его на страницу за пределами подлинного веб-сайта, где пользователю предлагается ввести личную информацию.

Clone phishing — это тип фишинговой атаки, при которой законное и ранее доставленное электронное письмо, содержащее вложение или ссылку, используется для создания почти идентичного или клонированного электронного письма [4]. Вложение или ссылка в электронном письме заменяются вредоносной версией, а затем отправляются с адреса электронной почты, подделанного, чтобы казаться исходящим от первоначального отправителя. Как правило, для этого требуется, чтобы либо отправитель, либо получатель были предварительно взломаны третьей стороной.

Filter evasion — метод, при котором фишеры используют изображения вместо текста, чтобы затруднить антифишинговым фильтрам обнаружение текста, обычно используемого в фишинговых письмах. В ответ более сложные антифишинговые фильтры способны восстанавливать скрытый текст в изображениях с помощью OCR (оптического распознавания символов).

Link Manipulation — с помощью данного метода, мошенник отправляет ссылку на вредоносный веб-сайт [3]. Когда пользователь нажимает на нее, он открывает сайт фишера вместо того, что указан в ссылке.

Фишеры могут использовать поддомены. Например, смотря на URL-адрес www.mybank.user.com, неосведомленное лицо посчитает, что ссылка приведет его к разделу «user». На самом деле ссылка ведет в раздел «mybank», т. к. иерархия доменов всегда идет справа налево.

Существует способ скрыть фактический URL-адрес под обычным текстом. Вместо отображения фактического URL-адреса фишеры используют такие предложения, как «нажмите здесь» или «подпишитесь». На самом деле URL-адрес, скрывающийся за текстом, ведет на фишинговые сайты. Более убедительное электронное письмо может даже отображать фактическую ссылку, но ведет она на фишинговый сайт.

Другой метод манипулирования ссылками заключается в том, что мошенники покупают домены с различными вариантами написания популярного домена, например: facebok.com, googlle.com, yahooo.com и т. д. Затем они обманывают пользователей, создавая похожие сайты и запрашивая личную информацию. В следующем методе злоумышленник вводит пользователя в заблуждение относительно ссылки, используя преимущества похожих символов. Например, латинские буквы «c», «o» и «x» могут заменяться на аналогичные буквы кириллицы.

Website Forgery — метод при котором вредоносный веб-сайт выдает себя за подлинный. Подделка в основном осуществляется двумя способами: межсайтовым скриптингом и подменой сайта.

Межсайтовый скриптинг (XSS) — это атака, при которой хакер внедряет вредоносный код в веб-приложение или веб-сайт. Это очень распространенная и широко используемая техника, при которой жертва не является прямой мишенью. Скорее всего, злоумышленник использует уязвимость в веб-приложении или веб-сайте, который посещает пользователь. В конечном итоге вредоносный сценарий доставляется в браузер жертвы. Другой метод, заключается в следующем: создается веб-сайт, который выглядит похожим на законный сайт, к которому пользователь действительно намеревается получить доступ. Поддельный веб-сайт имеет похожий пользовательский интерфейс и дизайн, часто имеет похожий URL-адрес.

Статистика. На основании квартальных отчетов рабочей группы по вопросам антифишинга APWG Phishing Activity Trends Report за последние десять лет авторами визуализированы изменения количества фишинг-сайтов в виде временного ряда с восходящей линией тренда. На рис. 1 приведен график, показывающий изменения количества уникальных фишинговых сайтов, которые определяются уникальными базовыми URL-адресами [5].

Рис. 1. Диаграмма уникальных фишинг-сайтов

HTTPS является расширением протокола передачи гипертекста HTTP для поддержки шифрования данных в целях повышения безопасности в сети. На рис. 2 показано стремительное увеличение процентного количества фишинг-сайтов, использующих данный протокол.

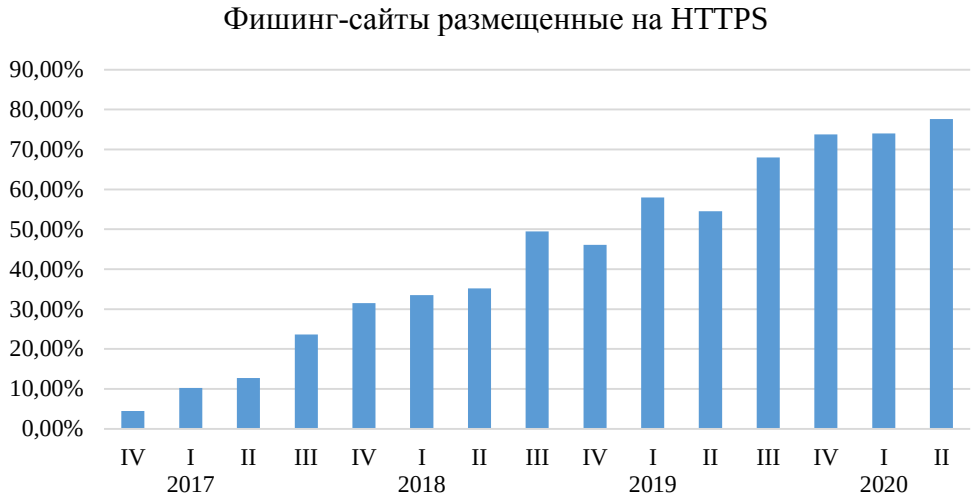

Рис. 2. Диаграмма фишинг-сайтов, использующих протокол HTTPS

На последующих трех круговых диаграммах показано, как изменялось соотношение отраслей, которые подвергались фишингу. На рис. 3 представлены результаты за 2010 г., на рис. 4 — за 2015 г., на рис. 5 — за 2019 г. В данных диаграммах использованы следующие обозначения: ISP (англ. Internet Service Provider) — Интернет провайдер; SaaS (англ. software as a service) — программное обеспечение как услуга.

Рис. 3. Соотношение отраслей, которые подвергались фишингу в 2010 г.

По данным за 2010 г. видно, что основными целями мошенников были финансовая отрасль и платежные системы, в сумме они составляют 70,10 %.

Целевые отрасли 2015 г.

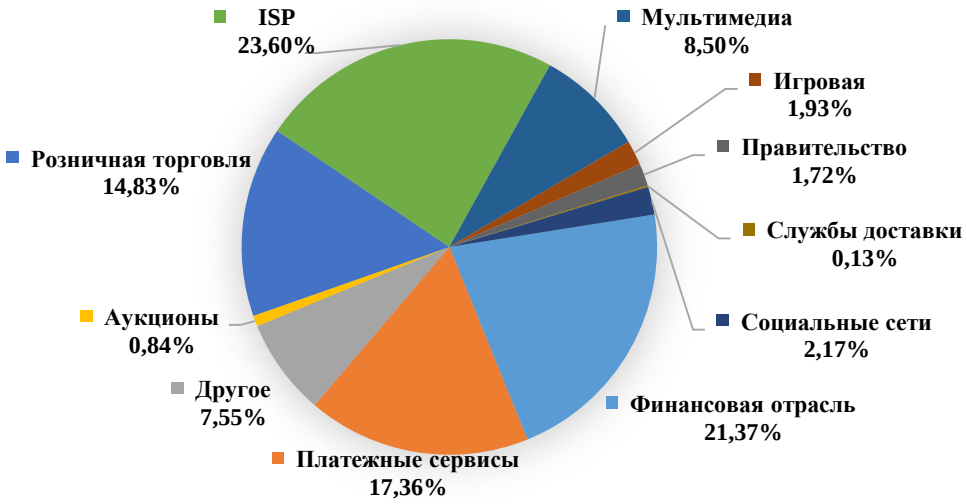

Рис. 4. Соотношение отраслей, которые подвергались фишингу в 2015 г.

В 2015 г. фишеры практически в равных долях атакуют финансовую отрасль и ISP, платежные системы и сферу розничной торговли. Увеличился интерес к мультимедийной отрасли.

Целевые отрасли 2019 г.

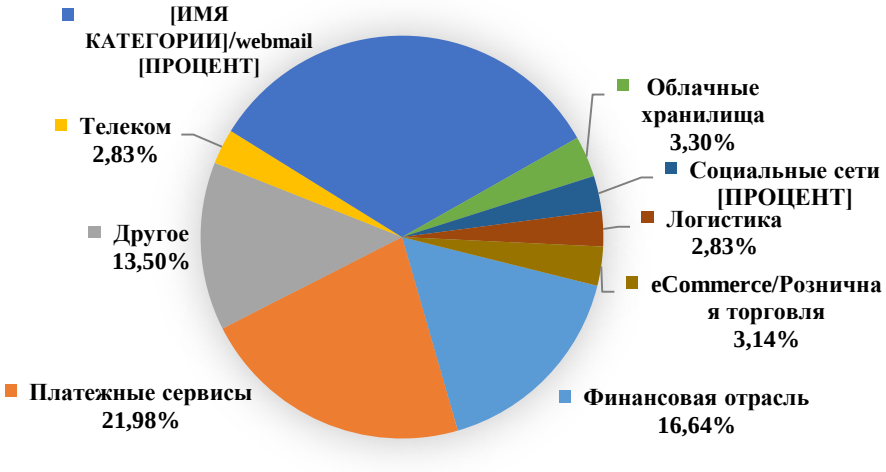

Рис. 5. Соотношение отраслей, которые подвергались фишингу в 2019 г.

С 2019 года ISP входит в сферу SaaS/webmail, к которой интерес фишеров увеличился. Фишинг-атаки на эту отрасль занимают около трети всех атак. Еще треть занимают платежные системы и финансовая отрасль. Кроме этого, доля сферы розничной торговли сократилась с 14,83 % до 3,14 %.

Следует отметить, что фишеры выбирают жертв не случайным образом. Они анализируют мировые тенденции и события, например, условия в период пандемии COVID-19 2020 года. Воспользовавшись природными катаклизмами, экономическими спадами, предстоящими мероприятиями и тому подобным, фишеры создают новые схемы мошенничества, продвигая поддельные благотворительные возможности и несуществующие продукты.

Анти-фишинговая защита. Для предотвращения ввода пользователями конфиденциальной информации на фишинг-сайтах используются различные технологии. В настоящее время популярные браузеры оснащены защитой от фишинга. Многие компании,

специализирующиеся на разработке систем защиты от кибер-угроз, создают программное обеспечение, включающее в себя фильтры фишинг-сайтов.

Популярным решением для предупреждения пользователя о небезопасном сайте является использование базы со списком адресов фишинг-сайтов. Проблема заключается в том, что современные фишеры создают и распространяют фишинг-сайты быстрее, чем адреса данных сайтов успевают попасть в «черный список».

В дополнение к технологии, основанной на списках, используется машинное обучение, где по совокупности различных характеристик сайта определяется уровень доверия к нему. Рассматриваются как внешний вид сайта, так и его регистрационные данные. URL-адрес сайта также содержит в себе много информации, которую можно извлечь и использовать.

Задача определения уровня доверия к интернет-ресурсу сложно поддается формализации и алгоритмически сложно реализуется. Несмотря на это, некоторые алгоритмы могут применяться в комплексе различных методов. Например, так можно определять степень подобия между фишинговым доменом и доменом из «белого списка» и использовать этот признак в многокритериальной задаче.

Заключение. Рассмотренные методы фишинг-атак демонстрируют, насколько изобретательны злоумышленники, а анализ диаграмм подтверждает актуальность проблемы фишинга. Эффективная защита от фишинга возможна только при комплексном использовании различных технологий.

Библиографический список

1. History of Phishing / phishing.org. Available from: https://www.phishing.org/history-of-phishing (accessed: 07.09.20).
2. Phishing techniques / phishing.org. Available from: https://www.phishing.org/phishing-techniques (accessed: 07.09.20).
3. Phishing tools and techniques / Infosec Resources. Available from: https://resources.infosecinstitute.com/topic/phishing-tools-and-techniques/ (accessed: 07.09.20).
4. Phishing / Wikipedia. Available from: https://en.wikipedia.org/wiki/Phishing (accessed: 07.09.20).
5. Phishing activity trends reports / Anti-Phishing Working Group. Available from: https://apwg.org/trendsreports/ (accessed: 20.09.20).

Об авторах:

Медведева Татьяна Александровна, доцент кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, доцент, med.ta1@yandex.ru

Данько Ольга Сергеевна, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), olgadanko.mail@gmail.com

Authors:

Medvedeva, Tatyana A., Associate Professor, Department of Computer Engineering and Automated Systems Software, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), Cand.Sci., Associate Professor, med.ta1@yandex.ru

Danko, Olga S., Student, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), olgadanko.mail@gmail.com