ФИШИНГОВАЯ АТАКА

Коневши Р.Н.[1], Тимохович А.С.[2]

[1]Коневши Роман Николаевич – бакалавр,
направление: информационная безопасность;
[2]Тимохович Александр Степанович – кандидат педагогических наук, доцент,
кафедра безопасности информационных технологий,
Институт информатики и телекоммуникаций,
Сибирский государственный университет науки и технологий им. академика М.Ф. Решетнева,
г. Красноярск

Фишинг - это атака, осуществляемая злоумышленниками с помощью широковещательной рассылки большого количества схожих или одинаковых по содержанию сообщений, имеющих в себе вредоносные вложения или ссылки, ведущие на вредоносный сайт [2].

Так как фишинг является не основной целью, а лишь средством для получения несанкционированного доступа к какой-либо информации, необходимо показать «классический» ход атаки с использованием фишинга. Последовательность шагов описана на рисунке ниже.



Рис. 1. Поэтапная схема атаки с помощью фишинга

Анализ

На первом этапе собираются необходимые данные о субъекте атаки, такие как:

- Личные интересы;
- Особенности характера;
- Увлечения;
- Используемые сетевые ресурсы.

Это необходимо для большей эффективности атаки, и является самым длительным и трудоемким процессом в проведении атаки, так как это может занять достаточно большое количество времени, но злоумышленники не часто пренебрегают данным этапом, так как именно от этого в большинстве случаев зависит успешность атаки и дальнейшие действия атакующих.

Например, если объект увлекается автомобилями, можно найти его сообщения на форумах и, проанализировав его сообщения, понять, как составить заголовок письма, для того, что бы объект обязательно открыл его и перешел по ссылке или открыл вложенный файл.

Недостаточный анализ моет полностью скомпрометировать атаку. Например, если у субъекта нет водительского удостоверения или машины, то атака с письмом из ГАИ о штрафе за парковку в неположенном месте, будет априори неудачной.

Но иногда злоумышленники пренебрегают данным этапом, используя общечеловеческие качества, такие как жадность, милосердие или простое любопытство. Но данные атаки, как правило, не направлены на определенного объекта, а на группу объектов, и процент успешности таких атак достаточно мал. Например, практически каждому человек на телефон приходило сообщение о том, что его дочь или сын или ещё какой-то родственник, и некоторые люди, находясь в состоянии аффекта идут к ближайшему банкомату и переводят деньги, но большинство людей игнорируют подобного рода сообщения.

Подготовка

На этапе подготовки злоумышленники разрабатывают вредоностные средства, которые будут прикрепляться к письму или сайты, ссылки на которые будут находиться в письме. Так же формируется письмо, которое будет оправлено человеку.

Например, в ходе анализа злоумышленник узнал, что объект атаки очень мнительный и не открывает никакие письма с незнакомых адресов, так же не реагирует на сообщения или звонки с незнакомых номеров. Но ещё в ходе анализы злоумышленник узнал, что данный объект является постоянным пользователем на форума, посвященному проблемам администрирования сервера на базе OS «Linux». После регистрации на данном форуме злоумышленник нашел вопрос от данного субъекта в одной из тем, который был оставлен недавно и ещё не имел ответа, на что злоумышленники формируют ссылку и отправляют ему ответ, в котором написано: «Не так давно сталкивался с подобной проблемой, решение оказалось достаточно нетривиальным, описывать это очень долго так что, вот ссылка» и прилагают к письму ссылку на вредоносный сайт, на который объект атаки переходит, заражая свой компьютер.

Проведение

Данный этап предполагает отправку сообщения, если атака направлена на одного объекта, или множества сообщений, если атака направлена на группу объектов, содержащее в себе вредоносное вложение или ссылку.

После проведения этого этапа злоумышленник с полной долей уверенности может сказать, насколько хорошо были проведены предыдущие два этапа и наглядно «увидеть» успешность данной атаки.

Получение результата

Этот этап может быть и заключающим, если полученная информация в процессе атаки являлась основной целью. Если, например, злоумышленники планировали получить данные банковских счетов или заразить компьютер вирусом вымогателем, для получения денег, то на этом этапе можно считать, что атака завершена, но есть случаю, когда на этом этапе атака не заканчивается, а лишь является подготовительным этапом к получению более важной для злоумышленника информацией.

Методы защиты от фишинга

Для защиты от фишинга необходимо помнить несколько простых правил, которые свидетельствуют о том, что вероятнее всего, данное письмо является фишингом:

1. Вы не знаете отправителя лично или не вели с ним переписки ранее;
2. В письме срочная проблема или вопрос, которая требует срочного решения;
3. Странное содержимое файла:

a. Внутри файла или архива – приложение, скрипт с раширением .js или что-то другое, не соответствующее содержанию письма;

b. Офисный документ требует включить макросы или отключить защищенный просмотр;

4. В тексте письма к вам не обращаются лично, а используют общие формулировки. [1]

Фишинг является достаточно серьезной угрозой компьютера, а в сочетании со сложностью в автоматизации его выявления, можно с уверенностью говорить, что практически каждый пользователь сети интернет может быть атакован данным видом атаки.

Список литературы

1. «Как узнать фишинговое письмо» // Блог компании Антифишинг. [Электронный ресурс]. Режим доступа: http://blog.antph.ru/all/how-to-know-phishing/ (дата обращения 14.05.2017).

2. «Фишинг» // Википедия. [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3/ (дата обращения 14.05.2017).

НЕРАЗРУШАЮЩИЙ КОНТРОЛЬ И ВОЗМОЖНОСТЬ ЕГО ПРИМЕНЕНИЯ В АВТОРЕМОНТНОМ ПРОИЗВОДСТВЕ

Васильев А.А.[1], Горин Л.Н.[2], Игошин Д.Н.[3]

[1]Васильев Алексей Анатольевич – старший преподаватель;
[2]Горин Леонид Николаевич – старший преподаватель;
[3]Игошин Денис Николаевич – старший преподаватель,
кафедра технического обслуживания, организации перевозок и управления на транспорте,
Институт транспорта, сервиса и туризма,
г. Воротынец

Аннотация: *в статье проведен анализ неразрушающего контроля деталей автомобильного транспорта. Выявлены наиболее эффективные методы, применяемые в автомобильном хозяйстве. На основе анализа методов неразрушающего контроля можно развивать учебно-материальную базу и вести качественную подготовку специалистов, связанных с производственной деятельностью с обнаружением различных дефектов на отдельных деталях.*
Ключевые слова: *дефекты, детали, методы неразрушающего контроля.*

В ходе подготовки специалистов по техническому обслуживанию и ремонту автомобильного транспорта необходимо дать молодым людям глубокие знания по использованию неразрушающего контроля деталей и различных изделий [1]. Неразрушающий контроль позволяет вести проверку качества продукции без какого-либо нарушения ее целостности и пригодности в дальнейшем к использованию по прямому назначению. Современные автомобильные детали в процессе их эксплуатации подвергаются различным воздействиям, вызывающим определенные изменения физических характеристик материалов, из которых они изготовлены [2]. Результатами этих изменений являются различные дефекты. Определить и выявить дефекты можно в результате определенных исследований с применением различных методов, которые основаны на использовании проникающих веществ, излучений, колебаний и т.д. [5]. К ним относятся явления капиллярности, течепускания, воздушных пузырьков, излучений рентгеновских и гамма-лучей, различных звуковых колебаний, магнитных и электромагнитных полей и другие [3, 4, 6].

Существующие методы обнаружения различных дефектов неразрушающим методом позволяют сделать вывод, что имеется довольно большой арсенал методов и средств неразрушающего контроля. Соответственно следует отметить, что они не могут претендовать на звание универсальных методов, но каждый из них может быть применен наиболее эффективно для обнаружения конкретного дефекта. Поэтому целесообразно изучать и познавать достоинства и недостатки методов неразрушающего контроля, уметь применять их в конкретной ситуации. Находить решение проблемы применением совокупности методов. Решение задач, таким образом, в условиях производства и при эксплуатации техники приведет к повышению ее качества и надежности. Применяя неразрушающий контроль на различных этапах технологического процесса изготовления и ремонта различных изделий можно вести обработку результатов контроля, которые дадут возможность устанавливать и устранять причины брака, корректировать технологические процессы.