АНАЛИЗ МОШЕННИЧЕСКИХ СХЕМ ПРИ ПУБЛИКАЦИИ СТАТЕЙ В НАУЧНЫХ ЖУРНАЛАХ

Лаврич Ю.С.[1] Лось А.Б.[2]

Цель статьи: *Исследование мошеннических схем, применяемых злоумышленниками в отношении авторов научных работ, желающих опубликовать свои результаты в ведущих мировых научных журналах и выработка рекомендаций по противодействию данным деяниям.*

Метод: *Для проведения аналитического исследования применялись методы компьютерной криминалистики, позволяющие определить физические и электронные адреса мошенников на основе открытых поисковых ресурсов.*

Полученный результат: *В работе проведен анализ ряда научных журналов, рекламируемых учредителями как ведущие европейские издания. Проанализированы письма-приглашения, направляемые мошенниками в адрес научных работников, публикующих свои работы в научных журналах, и веб-сайты соответствующих изданий. Благодаря регистрационной информации доменов, установлено действительное местоположение владельцев предлагаемых электронных ресурсов. В результате работы выявлены мотивы, способы, используемые уязвимости и общие подходы в реализации мошеннических схем. На основе полученных результатов высказано предположение о едином владельце всех рассматриваемых ресурсов. Проведен подробный анализ возможных последствий для авторов при попытках сотрудничества с указанными ресурсами и описан алгоритм проверки электронных писем и электронных ресурсов на предмет выявления возможных угроз.*

Ключевые слова: *Мошенничество, научные журналы, вредоносное ПО, кража денежных средств, потеря интеллектуальной собственности, алгоритм выявления угроз, компьютерная криминалистика, рекомендации для сотрудничества.*

DOI:10.21681/2311-3456-2019-5-12-18

1. Введение

Мошенничество – одно из самых популярных, разнообразных и легко реализуемых видов противоправных деяний. С развитием информационных технологий, растет и число компьютерных преступлений [1]. Методы и средства мошеннических схем постоянно обновляются, расширяется область их применения. Научные журналы, как возможный объект реализации указанных схем, не являются исключением. Публикация научных результатов является необходимым этапом работы каждого научного работника. В настоящее время существуют широкие возможности выбора научного журнала, однако, серьезные проблемы существуют и в этой области. Рост интереса к научным исследованиям привел к появлению мошеннических схем и в указанной деятельности [2]. Одной из причин появление такого рода схем является достаточно ограниченное число серьезных научных изданий, долгая процедура публикации, а также высокая стоимость данной процедуры, в которую включены услуги по рецензированию, редактирование перевода, стоимость издательских работ [3]. Ниже в работе приведены результаты исследования ряда журналов, заявляемых учредителями в качестве ведущих европейских изданий, на предмет наличия признаков мошенничества и даны рекомендации по их выявлению.

2. Описание мошеннических схем

Действия злоумышленников часто достаточно сложно распознать. Вначале, как правило, на известный заранее электронный адрес научного сотрудника, приходит письмо с приглашением к публикации в научном журнале. В большинстве своем оно выглядит грамотно и не вызывает подозрений:

- Приветственное сообщение;
- Описание предлагаемого журнала;
- Заключительная часть с контактной информацией.

Ничего не подозревающий ученый переходит по ссылке на официальный веб-сайт журнала. Там он видит красивое оформление и стандартную структуру для подобных сайтов:

- Главная страница – описание журнала, сроки публикации, индексаторы и наличие в мировых базах цитирования;
- Формат подачи заявления на публикацию;
- Архив журнала;
- Информация о членах редакционной коллегии (которая, в данной ситуации, как правило, набирается из неквалифицированных людей [4]).
- Контактная информация

При решении сотрудничества с данным изданием,

1 Лаврич Юрий Сергеевич, ассистент кафедры Компьютерная безопасность МИЭМ НИУ ВШЭ, г. Москва, Россия. E-mail: yuslavrich@edu.hse.ru

2 Лось Алексей Борисович, кандидат технических наук, доцент кафедры Компьютерная безопасность МИЭМ НИУ ВШЭ, г. Москва, Россия. E-mail: alos@hse.ru

автор попадает на замаскированный мошеннический веб-сайт, в структуре которого может быть скрыто различное вредоносное программное обеспечение [5]. Например, веб-страница такого сайта может содержать скрипт для кражи персональных данных пользователя [6], различные вирусы, черви, и, самое популярное в этой сфере, – боты. Обычно боты используются для автоматизации рутинных действий, однако, в настоящее время, среди мошенников они широко используются для поддержания бот-нетов [7] и кражи компьютерных ресурсов.

Если автор решается опубликовать статью в подобном журнале, он подает статью на рецензию, которая успешно производится злоумышленником вручную или в автоматическом режиме. Этот этап преступления очень важен, потому что от результата зависит согласие человека на дальнейшую публикацию, которая требует оплаты.

В связи с этим, в большинстве случаев, рецензия выглядит грамотно, как и ожидал заказчик.

Следующий этап – оплата. Как правило, при оплате публикации, пользователя перенаправляют на поддельный сайт платежной системы. В преступной схеме данный веб-сайт очень похож на настоящий сайт: он имеет очень похожее доменное имя, за исключением некоторых букв, и, соответственно, схожее с настоящим оформление [8]. После оплаты срабатывает фишинговый скрипт [9] на кражу реквизитов и CVV-кода кредитной карты [10]. В результате, публикация, скорее всего, произойдет, однако не в том виде, что ожидал автор. Она останется в архиве данного журнала, который нигде не зарегистрирован и не имеет цитирования ни в одном ресурсе.

Таким образом, подобная схема позволяет мошенникам:

- Красть персональные данные с компьютера пользователя;
- Включать зараженный компьютер в сеть бот-нета;
- Внедрять и распространять вредоносное программное обеспечение;
- Красть аппаратные ресурсы;
- Красть денежные средства.

Далее в работе будут приведены результаты анализа ряда, якобы, европейских научных журналов и рекомендации по предотвращению попадания на указанные выше мошеннические схемы.

3. Анализ заявленных европейских научных журналов

Для исследования автору были предложены семь журналов:

1. «Scientific discussion» - Чехия
2. «Danish scientific journal» - Дания
3. «The scientific heritage» - Венгрия
4. «Fundamentalis scientiam» - Испания
5. «Norwegian Journal of development of the International Science» - Норвегия
6. «Znanstvena misel» - Словения
7. «East European Science journal» - Польша

Переходя на сайт каждого из представленных журналов, автора встречает красивое оформление, подробная информация о журнале, редакционной коллегии, сроках выпуска и индексаторах. Первое, что было замечено при анализе каждого из журналов – все они отсутствуют в мировых базах «Scopus»[3] и «Web of Science»[4]. На некоторых веб-сайтах написано, что журналы готовятся к регистрации в этих базах[5], однако данная надпись может «висеть» с момента выпуска сайта (что и было впоследствии замечено при поиске в веб-архиве).

Существенных замечаний по структуре сайтов выявлено не было, никакой назойливой, вирусной рекламы [11], все сделано аккуратно и не вызывает никаких подозрений. Однако более тщательная проверка все же дала повод задуматься о том, что в каждом из представленных журналов внедрены мошеннические схемы:

Первое, что было установлено методами компьютерной криминалистики, так это то, что реальные владельцы каждого из семи журналов являются гражданами Украины. Сайты зарегистрирован там же, в городе Киев. В некоторых случаях поиск выдавал такие страны, как Китай и США. Впоследствии более тщательная проверка показала, что это все та же Украина.

Далее, было установлено, что на веб-сайт каждого из журналов ссылается[6] множество украинских форумов, библиотек (в том числе и национальная библиотека) и университетов. В этих списках присутствуют некоторые российские университеты, но никак не зарубежные, что говорит о том, что журналы не являются международными, как было заявлено.

На те же IP-адреса зарегистрированы[7] более сотни сайтов. В их числе торговые, мошеннические (подделка документов, маски реально существующих сайтов и т.д.), хакерские (криптоботы, сайты продажи исходников вредоносного ПО и т.п.) и другие «научные» журналы.

Чешский журнал генерирует электронные адреса для рассылки пригласительных писем. Например, bounce+... =....ru@emy.in.ua. Здесь же стоит обратить внимание на «ua»!

В метаданных изображений[8] [12] с некоторых веб-сайтов были обнаружены символы кириллицы. Мало вероятно, что зарубежному редактору удобно пользоваться русским языком на рабочем ПК.

В завершении были обнаружены «левые» индексаторы. В их архивах содержится ненормативная и экстремистская литература.

В этой связи, следует заключить, что каждый из рассматриваемых «европейских» «научных» журналов в действительности, таковым не является. Для получения более точной информации необходимо наличие специальной аппаратуры, полномочий и программного обеспечения. В то же время, одного факта, что заявленная страна одна,

3 Поиск журналов в базе «Scopus». URL: scopus.com/sources

4 Поиск журналов в базе «Web of Science». URL: mjl.clarivate.com

5 Поиск журналов в мировых базах. URL: scimagojr.com

6 Сервис поиска обратных ссылок. URL: smallseotools.com/backlink-checker

7 Сервис поиска веб-сайтов по IP-адресу. URL: suip.biz

8 Сервис поиска метаданных изображения. URL: exif.regex.info/exif.cgi

а реальная другая, достаточно, чтобы выдвинуть гипотезу о соответствующих намерениях владельцев журнала. С большой долей уверенности можно предположить, что всеми представленными журналами владеет одна и та же группа лиц. Действительно, все поиски указывают на принадлежность Украине, и одному человеку не под силу держать активными такое количество сайтов.

4. Рекомендации авторам в части сотрудничества с научным журналом

4.1 Анализ пригласительного письма

При получении на электронную почту письма с приглашением к публикации в научном журнале, его следует внимательно проанализировать.

Любой почтовый сервис предоставляет возможность узнать IP-адрес отправителя. Для получения этих данных, следует нажать на кнопку предоставления дополнительных действий относительно письма. Например, в почте «mail.ru», необходимо нажать на поле «Еще» и выбрать «Служебные заголовки». Откроется новое окно, в котором, на первый взгляд, много непонятного текста. Среди этого текста необходимо найти поле «Received from:». Здесь, в квадратных скобках, будет указан IP-адрес отправителя. Если таких полей много, то следует выбрать последнее из возможных. Имея IP-адрес, можно получить информацию о нем в любом сервисе поиска местоположения по IP-адресу. Физический адрес отправителя обычному пользователю получить невозможно, однако можно получить информацию о его провайдере. Таким образом, можно узнать как страну отправителя, так порой и его город (если провайдер и отправитель находятся в одном городе). Может возникнуть ситуация, когда отправитель использует прокси – увеличивает анонимность пребывания в интернете. В этом случае, поиск по IP-адресу даст неверный результат. Обычно отправители писем знают, как грамотно скрыть свой IP-адрес. В таком случае, никакой дополнительной информации об отправителе в письме получить невозможно и этот пункт анализа можно пропустить.

Пример для сервиса «mail.ru»:

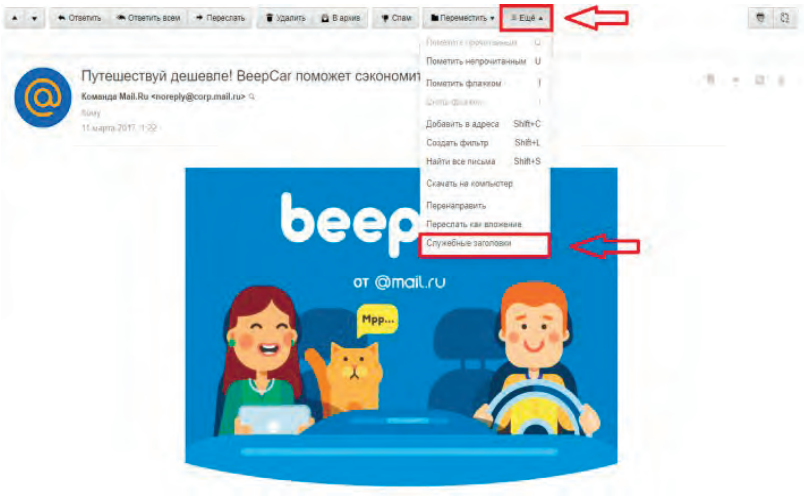

Рис. 1 «Выбор необходимого поля»

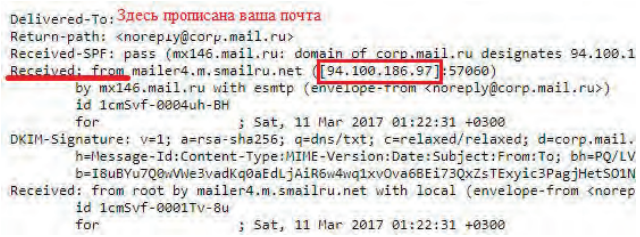

Рис. 2 «Определение IP-адреса отправителя»

Далее следует обратить внимание на почтовый адрес, с которого было прислано письмо. Первая часть адреса (все, что стоит до «@») может быть любой, но должна иметь отношение к отправителю: ассоциации с названием журнала, именем автора и так далее. Стоит задуматься, если первая часть почтового адреса имеет нечитаемый вид или, например, состоит из частей Вашего почтового адреса. В таком случае, можно выдвинуть гипотезу о том, что почтовый адрес отправителя был сгенерирован с использованием «бота». Следует отметить, что используя части адреса получателя, можно сгенерировать огромное число почтовых адресов.

Вторая часть электронного адреса также может быть абсолютно любой. Могут быть использованы всемирно известные почтовые сервисы «Gmail», «Yahoo» и прочие [13]. В то же время могут использоваться какие-нибудь локальные почтовики. Во втором случае никому не известные почтовые сервисы могут использоваться с целью рассылки спама, потому что, в отличие от первых, на них с очень большой вероятностью не накладываются ограничения по пакетной рассылке и количеству зарегистрированных почтовых адресов. В этом случае возникает ситуация использования ботов. Однако всемирно известные почтовые сервисы не являются исключением для использования ботов. Только в этом случае у администратора «бота\ботнета» возникают накладные расходы, потому что популярные почтовые сервисы требуют плату за содержание большого числа

УДК 004.94 DOI: 10.21681/2311-3456-2019-5-12-18

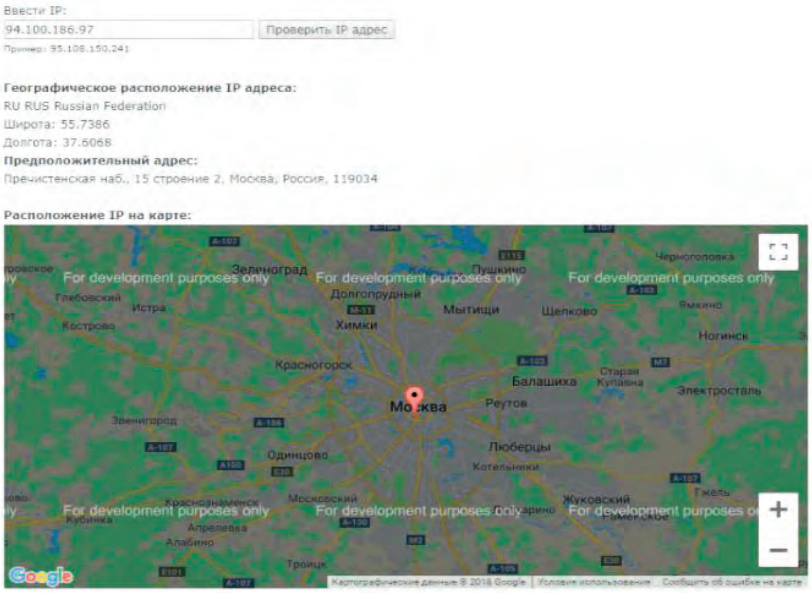

Рис. 3 «Определение местоположения отправителя/его провайдера по IP-адресу»

почтовых адресов. К сожалению, порой и это не является преградой для злоумышленника и, чтобы не использовать никому не известные почтовики (с целью ввести в заблуждение получателя письма), он использует специальные хакерские программы для обхода ограничений, устанавливаемых почтовыми сервисами.

Убедившись, что электронный адрес не удовлетворяет этим параметрам, можно попробовать найти информацию о его владельце. Таких сервисов существует множество, стоит лишь воспользоваться любым поисковиком (найти информацию о владельце, зная его электронную почту). Известно, что злоумышленники часто оставляют следы, в частности, в социальных сетях, и следует воспользоваться сервисом по поиску привязанного электронного адреса в социальных сетях [14]. Еще можно найти список сайтов, зарегистрированных на данную электронную почту. Таким сервисом, например, является «domainiq.com». Возможно, таким методом получится найти какую-либо личную информацию о владельце. Результатом поиска может оказаться как лицо, относящееся непосредственно к журналу, так и стороннее лицо. Во втором случае вывод сделать сложно, так как это может быть результат работы «ботнета», так и человек, занимающийся рассылкой приглашений, относящийся к журналу. В худшем случае никакой информации не будет найдено и можно сделать вывод, что это «мертвый» электронный адрес, используемый для рассылки спама и подобных действий.

Еще один из способов убедиться в реальности намерений автора письма – связаться с ним напрямую (в случае, если электронный адрес прошел вышеизложенную проверку). Стоит придумать письмо вопросительного характера и подождать ответа. Если ответ оправдает Ваши ожидания, то можно переходить к следующему этапу. Однако не стоит забывать, что отправитель все еще может являться мошенником и сразу доверять ему не стоит.

На следующем шаге следует внимательно проанализировать текст сообщения. Будь то злоумышленник или реальный представитель научного журнала, письмо будет начинаться с уважительного приветствия. Если журнал ориентирован на рассылку приглашений для публикаций, используя резюме авторов, то, как правило, в приветственной части письма будет обращение лично к Вам (авторитетный журнал не откажет себе в этом). Например: «Здравствуйте, Иванов Игорь Петрович. Мы рады...». В крайне редком случае, лишь, когда для спам – рассылки используются открытые или взломанные базы данных, злоумышленники будут знать личную информацию о Вас.

В тексте письма, как правило, должно использоваться представление. Эта информация включает в себе данные об авторе журнала, какие тематики он включает в себя, сроки публикации, авторитетность, контактные данные и тому подобное. Если весь этот текст написан невнятно, с большим количеством орфографических и стилистических ошибок, а, того хуже, частями не переведен с другого языка или вообще не имеет отношения к научным журналам, то сразу можно сделать вывод, что это письмо – спам.

Если в тексте письма имеются ссылки, ни в коем случае не переходите по ним без предварительной проверки. Для этого скопируйте ссылку и проверьте ее в своем антивирусе. Если такой возможности нет, то аналогичную проверку можно провести в онлайн-сервисе антивируса «dr.Web». Если проверка прошла успешно и вирусов не обнаружено, то проверьте, соответствует ли доменное имя (имя сайта, на который предлагают перейти), указанное в письме, реальному доменному имени (после перехода на сайт). Невнимательный пользователь может не заметить разницы между «thisismywebsite.com» и «thisismyvebsite.com». В итоге он окажется на стороннем сайте, который может использоваться злоумышленником в различных целях:

от мошенничества до распространения вредоносного программного обеспечения. Если на этом этапе все в порядке и ничего не вызывает подозрений – стоит перейти к анализу структуры веб-сайта журнала.

4.2 Анализ структуры веб-сайта журнала

Стоит внимательно проанализировать структуру веб-сайта журнала. В настоящее время злоумышленники владеют навыками обхода антивирусных систем. Поэтому проверки веб-сайта на вирусы недостаточно для уверенности в его безопасности. Часто даже авторитетные журналы размещают у себя на сайте рекламу, ведь это способствуют дополнительному заработку. Однако это не должно выглядеть как огромное количество окон с бесполезной, лживой, а порой и пропагандистской информацией. Такой структуре соответствует большинство мошеннических сайтов. Если, перейдя по ссылке из письма, вы столкнулись с подобной ситуацией, ни в коем случае не переходите по рекламным ссылкам и сразу покидайте веб-страницу. В противном случае Вы можете столкнуться с проблемой, описанной в конце третьего этапа анализа.

В случае, если подобная реклама отсутствует на сайте, внимательно проанализируйте предложенную информацию. Она должна иметь отношение только к самому журналу:

Не должно присутствовать ссылок на сторонние ресурсы, не относящихся к журналу или его тематике. Эти ссылки так же могут оказаться вредоносными. Если на сайте имеются какие-либо изображения, не следует сразу открывать их, и уж тем более, скачивать. Закладывание вредоносного кода в изображение – довольно распространенный метод «заражения» компьютера. Перед использованием эти изображения следует проверить в онлайн-сервисах антивирусов.

В случае, если имеются какие-либо ссылки на скачивание данных (например, какой-либо из выпусков журнала), их следует также внимательно проанализировать. Во-первых, стоит обратить внимание на саму ссылку. Если она имеет крайне странное название, особенно включающее в себя такие слова, как «trojan», «bot», «hack» и им подобные, то ни в коем случае не стоит переходить по ней. Во вторых, может возникнуть ситуация, что ссылка нормальная, проверена антивирусами, но скачивается файл, например, «download-archieve-of-journal.rar.exe». В нашем случае это 100% вредоносный файл. Если Вы скачиваете архив с выпусками журнала, то он обязан иметь расширение (то, что стоит после точки в имени файла) «.rar», «.zip» или им подобные. Если рассматривать пример, то загрузится исполняемый файл. На это указывает расширение «.exe». Зачастую неосторожный пользователь не обращает внимания на такие вещи и бездумно скачивает файлы. Операционная система «Windows» скрывает расширение файла. Узнать его можно только при обращении к свойствам этого объекта. То есть, скачав такой файл, он будет виден как «download-archieve-of-journal.rar», а расширение «.exe» будет скрыто операционной системой. Неосторожный пользователь, с надеждой увидеть архив данных, получит, в лучшем случае вредоносный скрипт, а в худшем – неопределенное поведение компьютера. Поэтому всегда важно следить за тем, что скачиваете. Обязательно проверить загруженные файлы антивирусом.

Пройдя вышеизложенную проверку, стоит проверить историю изменений сайта. Это можно сделать в сервисе «Whois»[9], однако более наглядный результат предоставляет веб-архив. Поиск можно совершить на веб-сайте «archive.org/web/web.php»[10].

Результатом будет статистика изменений сайта, а также сами изменения за период его существования. Так можно найти, для чего использовался сайт раньше, какая информация была на нем размещена и так далее. Важным параметром является дата создания сайта и дата конца его регистрации. Злоумышленники, совершив задуманное, закрывают сайт, а потом, например, через несколько лет снова его открывают. Эту информацию также можно найти в веб-архиве и сервисе «Whois». Сервис «Whois» выдает информацию о хостинг-провайдере веб-сайта (того, у кого зарегистрирован это сайт). Если предоставить объективную причину для выдачи информации о владельце сайта, зарегистрированного в данном хостинге, то можно без использования сторонних ресурсов получить практически все данные о человеке.

Если ввести в поисковике «Google» команду «filetype:расширение site:имя сайта» то, найдутся все файлы данного расширения на указанном веб-сайте [15]. Такой командой можно найти все файлы с расширением «doc», «ppt», «xls», «pdf», «rtf», «swf».

Перед скачиванием файлов, обязательно проводить их проверку, описанную выше. Зачастую пользователи указывают свои реальные данные в учетной записи компьютера. Поэтому, посмотрев свойства скачанного файла, можно найти данные о том, кем он был создан. Таким образом, можно найти более подробную информацию о владельце сайта или редакторе.

Если проверка прошла успешно, есть возможность проверить, какие еще веб-страницы зарегистрированы на данный IP-адрес (информация об IP-адресе присутствует в результате поиска в сервисе «Whois»). Подобный поиск позволяет реализовать, например, сервис «suip.biz». Результатом будет являться список веб-страниц, зарегистрированных на тот же адрес, что и исследуемый научный журнал. Первым делом в глаза должны бросаться сайты, не имеющие отношения к научной деятельности. Смысл в том, что в большинстве своем мошенники регистрируют целый спектр веб-страниц различной направленности, чтобы реализовывать свои схемы во всевозможных сферах. Если же данная проверка не вызвала подозрений, то анализ можно считать законченным, а журнал «чистым» от мошенничества.

5. Заключение

В настоящей статье рассмотрены мошеннические схемы, разработанные с целью получения денежных

9 Сервис «Whois». URL: nic.ru/whois

10 Веб-архив. URL: archive.org/web/web.php

средств и личных данных научных работников, публикующих свои труды в различных научных изданиях. На ряде конкретных примеров исследования сайтов научных журналов, авторы которых выдают их за серьезные европейские издания, выявлены попытки привлечь авторов с указанными выше целями незаконного получения денежных средств, несанкционированного доступа к личным данным и к управлению персональным компьютером. На конкретных примерах авторами показано, что в современных условиях быстрого развития информационных технологий, электронные письма и веб-страницы в Интернете, в таких, казалось бы, простых ситуациях, как публикации статей в научных журналах, также могут являться средством совершения компьютерных мошеннических действий. Следствием отсутствия внимания к элементарным правилам безопасности могут стать не только потеря денежных средств, но и более серьезные проблемы, связанные с утратой личных данных, заражением компьютера вредоносным программным обеспечением и другие серьезные проблемы.

Литература

1. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016. № 1(35). С. 86-94.
2. Gül Pamukçu Günaydın , Nurettin Özgür Doğan. A Growing Threat for Academicians: Fake and Predatory Journals // The journal of academic emergency medicine. 2015. P. 94-96.
3. Кувалин Д.Б. Научный журнал в современной России: возможные модели поведения // Экономическая политика. 2017. Т.12, № 6. С. 221.
4. Sorokowski P., Kulczycki E., Sorokowska A., Pisanski K. Predatory journals recruit fake editor // Nature. 2017. Vol. 543. P. 481-483. DOI: 10.1038/543481a.
5. Галимов Р.Р., Газизова А.А. Анализ методов распространения вредоносных программ // Наука и современность: сборник материалов V-ой международной научно-практической конференции. М: Издательство НИЦ «Империя», 2016, С. 41.
6. Райтман М.А. Как найти и скачать в Интернете любые файлы // 4-е изд., перераб. и доп. Спб.: БХВ-Петербург, 2015. С. 96-97.
7. Чуканов К.В., Чичикин Г.Я. Вредоносное ПО // European science. 2018. № 9(41). С. 34.
8. Жердев П.А., Бондарчук А.С. О способе совершения мошенничества в сфере компьютерной информации как основном элементе криминалистической характеристики //Актуальные проблемы науки и практики: сб. науч. тр; Дальневосточ. Юрид. Ин-т МВД России. Хабаровск : РИО ДВЮИ МВД России, 2018. № 1. С. 75.
9. Михайленко И.А. К вопросу о способах мошенничества в сети интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5(13). С. 101.
10. Изотов Д.С., Быкова Н.Н. Виды мошенничества с банковскими картами // Вестник НГИЭИ. 2015. № 3(46). С. 50.
11. Пятаева Е.В. Основные инструменты внедрения нарушителем в информационную систему вредоносного кода через рекламу и контент // Наука и инновации в современных условиях: сборник статей Международной научно - практической конференции. В 4 ч. Ч.3 / Уфа: АЭТЕРНА, 2017. 203 с.
12. Смирнов К.О. Исследование цифровых изображений с помощью EXIF-стандарта // Интерактивная наука. 2017. № 12. С. 243-246. DOI: 10.21661/r-116526.
13. Beall J., Criteria for Determining Predatory Open-Access Publishers // 3rd edition. 2015. P. 5
14. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети интернет // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 209-216.
15. Бибина Е.С., Осадчая А.Д. Методы поиска уязвимостей веб-приложений // Nauka-Rastudent.ru. 2016. № 3(27). 24 с.

ANALYSIS OF FRAUDAL SCHEMES WHEN PUBLICATING ARTICLES IN SCIENTIFIC JOURNALS

Lavrich Y.S.[11], Los A.B.[12]

Abstract.

Purpose: Study of fraudulent schemes used by malefactors against authors of scientific papers who wish to publish their results in the world's leading scientific journals and make recommendations on how to counteract these acts.

Research methods: To conduct an analytical study, computer forensic techniques were used, which allowed to determine the physical and electronic addresses of fraudsters based on open search resources.

Results: In this paper, there were analyzed a number of scientific journals advertised by the founders as the leading European editions. Analyzed the invitation letters sent by fraudsters to scientists who publish their work in scientific

11 Yuri Lavrich, Assistant of the Computer Security department NRU HSE, Moscow, Russia. E-mail: yuslavrich@edu.hse.ru

12 Alexey Los, Ph.D., Professor of the Computer Security department NRU HSE, Moscow, Russia. E-mail: alos@hse.ru

journals and websites of relevant editions. Thanks to the registration information of the domains, the actual location of the owners of the proposed electronic resources has been established. As a result of the work, motives, methods, used vulnerabilities and common approaches in the implementation of fraudulent schemes were revealed. On the basis of the results obtained, an assumption was made about a single owner of all considered resources. Detailed analysis of the possible consequences for the authors when trying to cooperate with the indicated resources was carried out and an algorithm for checking emails and electronic resources to identify possible threats was described.

Keywords: Fraud, scientific journals, malware, theft of money, loss of intellectual property, threat detection algorithm, computer forensics, recommendations for collaboration.

References

1. Evdokimov K.N. Struktura i sostoyanie komp'yuternoj prestupnosti v Rossijskoj Federacii // Yuridicheskaya nauka i pravoohranitel'naya praktika. 2016. № 1(35). P. 86-94.
2. Gül Pamukçu Günaydın , Nurettin Özgür Doğan. A Growing Threat for Academicians: Fake and Predatory Journals // The journal of academic emergency medicine. 2015. P. 94-96.
3. Kuvalin D.B. Nauchnyj zhurnal v sovremennoj Rossii: vozmozhnye modeli povedeniya // Ekonomicheskaya politika. 2017. T.12, № 6. P. 221.
4. Sorokowski P., Kulczycki E., Sorokowska A., Pisanski K. Predatory journals recruit fake editor // Nature. 2017. Vol. 543. P. 481-483. DOI: 10.1038/543481a.
5. Galimov R.R., Gazizova A.A. Analiz metodov rasprostraneniya vredonosnyh programm // Nauka i sovremennost': sbornik materialov V-oj mezhdunarodnoj nauchno-prakticheskoj konferencii. M: Izdatel'stvo NIC «Imperiya», 2016, S. 41.
6. Rajtman M.A. Kak najti i skachat' v Internete lyubye fajly // 4-e izd., pererab. I dop. Spb.: BHV-Peterburg, 2015. P. 96-97.
7. Chukanov K.V., Chichikin G.Y. Vredonosnoe PO // European science. 2018. № 9(41). P. 34.
8. Zherdev P.A., Bondarchuk A.S. O sposobe sovershenіya moshennichestva v sfere komp'yuternoj informacii kak osnovnom elemente kriminalisticheskoj harakteristiki //Aktual'nye problemy nauki i praktiki: sb. Nauch. Tr; Dal'nevostoch. Yurid. In-t MVD Rossii. – Habarovsk : RIO DVYUI MVD Rossii, 2018. № 1. P. 75.
9. Mihajlenko I.A. K voprosu o sposobah moshennichestva v seti internet // Sibirskie ugolovno-processual'nye i kriminalisticheskie chteniya. 2016. № 5(13). P. 101.
10. Izotov D.S., Bykova N.N. Vidy moshennichestva s bankovskimi kartami // Vestnik NGIEI. 2015. № 3(46). P. 50.
11. Pyataeva E.V. Osnovnye instrumenty vnedreniya narushitelem v informacionnuyu sistemu vredonosnogo koda cherez reklamu i kontent // Nauka i innovacii v sovremennyh usloviyah: sbornik statej Mezhdunarodnoj nauchno - prakticheskoj konferencii. V 4 ch. Ch.3/ - Ufa: AETERNA, 2017. – 203 p.
12. Smirnov K.O. Issledovanie cifrovyh izobrazhenij s pomoshch'yu EXIF-standarta // Interaktivnaya nauka. 2017. № 12. P. 243-246. DOI: 10.21661/r-116526.
13. Beall J., Criteria for Determining Predatory Open-Access Publishers // 3rd edition. 2015. P. 5.
14. Vvedenskaya O.Y. Osobennosti sledoobrazovaniya pri sovershenii prestuplenij posredstvom seti internet // Yuridicheskaya nauka i pravoohranitel'naya praktika. 2015. № 4(34). P. 209-216.
15. Bibina E.S., Osadchaya A.D. Metody poiska uyazvimostej veb-prilozhenij // Nauka-Rastudent.ru. 2016. № 3(27). 24 p.