Вредоносные гости

Т.Ю. Селихова

Имя задачи: Письма счастья

Автор: Селихова Татьяна Юрьевна, учитель информатики и ИКТ средней школы № 4 с. Монастырище Черниговского района Приморского края.

Предмет: Информатика и ИКТ.

Класс: 10.

Тема: Вредоносное программное обеспечение.

Профиль: Общеобразовательный.

Уровень: Общий.

Текст задачи. В 1993 году администратор компьютерной сети Usenet Ричард Депью написал программу, ошибка которой спровоцировала массовую рассылку двух сотен идентичных писем в одну из конференций. Его недовольные собеседники быстро нашли подходящее название для навязчивых рекламных сообщений — спам. Благодаря этому изобретению авторы нигерийского письма в 2005 году получили так называемую анти-Нобелевскую премию в области литературы, а в 2007 году началась массовая рассылка графических файлов, содержащих GIF-анимацию. В последнее время участились случаи получения клиентами крупных банков писем с угрозами разного рода, например, «если вы не сообщите ваши данные в течение недели, ваш счёт будет заблокирован».

Почему эти разные по содержанию письма называют спамом? К какому виду сообщений они относится? Стоит ли бояться спама и зачем с ним бороться? Как защитить свой почтовый ящик и свою нервную систему от подобных рассылок?

а) Выделите ключевые слова для информационного поиска.

б) Найдите и соберите необходимую информацию.

в) Обсудите и проанализируйте собранную информацию.

г) Сделайте выводы.

д) Сравните ваши выводы с культурным образцом.

Возможные информационные источники

Web-сайты:
http://www.kaspersky.ru/index.html
http://www.securelist.com/ru/
http://ru.wikipedia.org
www.viruslist.ru

Культурный образец

http://www.securelist.com/ru/threats/spam?chapter=158

Определение спама

Согласно определению «Лаборатории Касперского», *спам* — это ано-

нимная массовая непрошенная рассылка.

В этом определении важно каждое включённое в него слово.

Анонимная: все страдают, в основном, именно от автоматических рассылок со скрытым или фальсифицированным обратным адресом.

Массовая: эти рассылки именно массовые, и только они являются настоящим бизнесом для спаммеров и настоящей проблемой для пользователей.

Непрошенная: очевидно, подписные рассылки и конференции не должны подпадать под наше определение (хотя условие анонимности и так в значительной мере это гарантирует).

В определение спама часто включают слова «рекламная» или «коммерческое предложение». Это не совсем верно — значительная часть спама не преследует рекламных или коммерческих целей. Есть рассылки политического спама, есть «благотворительные» спамерские письма, есть мошеннические («нигерийские», фишинговые), «цепочечные письма» — письма с просьбой переслать знакомым (страшилки, «письма счастья»), вирусные и прочие, не являющиеся коммерческим предприятием.

Таким образом, все незапрошенные предложения, попавшие в ящик, мы делим на:

1) спам, имеющий все признаки анонимной массовой рассылки.

2) целевые коммерческие предложения.

Первые нужно фильтровать и иногда сразу удалять — согласно политике компании. Вторые также возможно фильтровать, но с ними нужно обращаться более осторожно.

Что такое «фишинг»

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание и password — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платёжных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Атаки фишеров становятся всё более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счёт в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счёт будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить антифишинговые системы («если хотите обезопасить себя от фишинга, пройдите по этой ссылке и введите свой логин и пароль»).

Фишинговые сайты, как правило, живут недолго (в среднем — пять дней).

Так как антифишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать всё новые и новые сайты. Внешний же вид их остаётся неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счёту. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов.

Наиболее частые жертвы фишинга — банки, электронные платёжные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создаёт зомби-сети.

Характерной особенностью фишинговых писем является очень высокое качество подделки. Адресат получает письмо с логотипами банка / сайта / провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссылке «Перейти на сайт и залогиниться», но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Ещё одна хитрость фишеров — ссылки, очень похожие на URL оригинальных сайтов. Ведь достаточно наблюдательный пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно отличная от легитимного сайта. Такие «левые» ссылки тоже встречаются, но рассчитаны они на менее искушённого пользователя. Часто они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки.

Поэтому фишинговые URL часто похожи на настоящие. Они могут включать в себя название настоящего URL, дополненное другими словами (например, вместо www.examplebank.com стоит www.login-examplebank.com). Также в последнее время популярный фишинговый приём — ссылка с точками вместо слэшей, внешне очень похожая на настоящую (вместо www.examplebank.com/personal/login стоит www.examplebank.com.personal.login). Можно привести ещё такой фишерский вариант: www.examplebank.com-personal.login.

Также в самом теле письма может высвечиваться ссылка на легитимный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется ещё тем, что в письме может быть несколько второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведёт на сайт мошенников.

Иногда личные данные предлагается ввести прямо в письме. Надо

помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

Вред от спама

Почему со спамом нужно бороться? Начав с относительно скромных по масштабам рекламных рассылок, спам постепенно вырос в серьёзную техническую, экономическую и даже социальную угрозу:

1. Нагрузка на коммуникации. Спам замусоривает каналы связи, создаёт трафик, оплачивать который приходится либо провайдеру, либо пользователю (самому или работодателю, если речь идёт о рабочем почтовом ящике). Ещё три года назад президент Ассоциации документальной электросвязи Александр Иванов оценил ущерб от спама операторов сети Интернет в 55 млн. долларов США. И это только затраты на трафик. А ведь есть ещё физические мощности — почтовые серверы, принимающие и обрабатывающие этот мусор. Есть специалисты, которые эти серверы обслуживают. Эта инфраструктура тоже стоит денег.

2. Потеря времени. Если спам добрался до конечного почтового ящика, то его владелец будет вынужден вручную вычищать мусорную почту. Сотрудник, читающий в день 10–20 писем по работе, вместе с ними может получить 160–180 спамерских сообщений. Время, потраченное на удаление спама — а это пять-шесть часов в месяц, — будет потеряно из рабочего процесса, и оно же будет оплачено из кармана работодателя.

3. Раздражение и недовольство. Удаляя спам, пользователь по сути работает уборщицей, только «электронной» — выгребает мусор. Это не может его не раздражать, вот и ещё один негативный фактор — эмоциональный.

4. Случайная потеря нужного письма в пачке спама. Комментарии в данном случае излишни — кто хоть раз сталкивался с такой ситуацией, всё поймёт.

5. Криминализация спама.

С каждым годом спам всё больше теряет свою рекламную составляющую, и всё больше криминализируется. Предпосылкой этого процесса служит анонимность спам-рассылки, что создаёт иллюзию полной безнаказанности.

Широко известны такие виды криминализированной почты, как нигерийские письма и фишинг. Спамеры проявляют редкую активность в изобретении новых объектов атак и «приманок» для пользователя. Российские спамеры ведут настоящую охоту за логинами-паролями к ящикам бесплатных почтовых служб — Яндекс, Почта и Mail.ru.

Кроме того, услугами спамеров охотно пользуются вирусописатели, которые с помощью спамовых писем распространяют свои творения либо ссылки на заражённые сайты, куда пользователей заманивают под тем или иным предлогом. Результат получения такого спама один: риск заражения компьютера пользователя вредоносной программой.

Эксперты оценивают суммарные убытки от спама в несколько десятков миллиардов долларов ежегодно. В результате защита от спама оказалась не просто желательной, а остро необходимой. Если не ограничить спам и спамеров, то пользование

электронной почтой зайдёт в тупик. Мы просто не сможем применять её по прямому назначению, всё будет завалено спамом.

В современном мире защита от спама — такая же необходимая составляющая общей системы IT-безопасности, как и антивирусная защита.

Эволюция содержания писем

Появление средств обнаружения спама, основанных на анализе содержания письма (контентный анализ), привело к эволюции содержания спамерских писем — их готовят таким образом, чтобы автоматический анализ был затруднён. Как и в случае изменения методов рассылки, спамеры вынуждены бороться с антиспам-средствами.

Простые текстовые и HTML-письма

Первые спам-сообщения были одинаковыми — всем получателям рассылался один и тот же текст. Такие сообщения тривиально фильтруются (например, по частоте повторения одинаковых писем).

Персонализированные сообщения

Следующим шагом было добавление персонализации (например, «Hello, joe!» — в начале письма на адрес joe@user.com), что сделало все сообщения разными. Теперь для их фильтрации нужно было выискивать неизменяющуюся строчку и заносить её в список правил фильтра. В качестве метода борьбы были предложены нечёткие сигнатуры — устойчивые к небольшим изменениям текста и статистические обучаемые методы фильтрации (Байесовская фильтрация и т.п.).

Внесение случайных текстов, «шума», невидимых текстов

В начало или конец письма спамер может поместить отрывок из классического текста или просто случайный набор слов. В HTML-сообщение можно внести «невидимый» текст (очень мелким шрифтом или цветом, совпадающим с цветом фона). Эти добавления затрудняют работу нечётких сигнатур и статистических методов. В качестве ответной меры появился поиск цитат, устойчивый к дополнениям текстов, детальный разбор HTML и другие методы углублённого анализа содержания письма. Во многих случаях можно определить сам факт использования «спамерского трюка» и отклассифицировать сообщение как спам, не анализируя его текст в деталях.

«Графические» письма

Рекламное сообщение можно прислать пользователю в виде графического файла — что крайне затруднит автоматический анализ. В качестве ответной меры появились способы анализа изображений, выделяющие из них текст.

Графический спам представляет собой самые разнообразные рассылки. Некоторая часть такого спама — это простые картинки, которые можно детектировать спам-фильтрами. Однако спамеры всё больше прибегают к усложнённым видам графических писем: используют картинки с зашум-

лённым фоном, прыгающими буквами и строчками (т.е. буквы расположены неровно относительно строки), заменяют отдельные буквы на изображения, разворачивают изображение на несколько градусов, используют на картинках редкие шрифты или шрифты разного размера, пытаясь таким образом обойти спам-фильтры. При этом текст на спамерской картинке часто становится практически нечитаем, в результате получатель с трудом может оценить спамерское предложение, и основная цель рассылки не достигается (реклама не работает).

Ещё один технический приём спамеров — использование анимации. Это спам, рассылаемый не в виде обычных статических «картинок» (графических вложений), а в виде анимированной графики. Спамеры используют GIF-анимацию, т.к. она распознаётся и автоматически воспроизводится всеми популярными браузерами. Обычно анимированный спам содержит от двух до четырёх кадров, из которых только один кадр является значимым, т.е. содержит информационную составляющую.

Спамеры регулярно предпринимают попытки обновить технологии генерации графических вложений в спаме. В первом полугодии 2007 года появилось несколько новых способов доставки и демонстрации пользователю спамерской «картинки»:

1. Размещение графических файлов на страницах бесплатного хостинга изображений (например, imageshack.us, imagenerd.com, imgnation.net, hostpic.biz, imgplace.com и т.п.). В теле спамерского сообщения указывалась ссылка на URL с «картинкой». Когда получатель открывал сообщение, в большинстве популярных мейлеров изображение подгружалось с указанного URL.

2. Использование спамерской «картинки» в виде фонового изображения. Графический файл не вкладывался в сообщение, а, опять-таки, публиковался на том или ином сайте. В теле сообщений был указан только URL сайта, помещённый в тэг ‘body’, атрибут ‘background’. В результате изображение могло автоматически подгружаться в некоторых мейлерах, а также в веб-интерфейсах части почтовых служб.

3. Спам с вложениями формата PDF. Этот вид вложений не открывается и не подгружается автоматически. Чтобы увидеть спамерский контент, пользователь должен самостоятельно открыть вложение.

4. Спам с вложением формата FDF. В некотором смысле это аналог PDF-вложений, тем более что открыть и увидеть вложение можно с использованием всё того же Adobe Acrobat Reader.

Все эти новинки оказались достаточно эффективными в момент появления, но уже спустя несколько месяцев, а иногда и недель спам-фильтры подстроились под новые спамерские приёмы.

Перефразировка текстов

Одно и то же рекламное сообщение составляется во множестве вариантов одного и того же текста. Каждое отдельное письмо выглядит как обычный связный текст, и только имея много копий сообщения, можно установить факт перефразировки. Таким образом, эффективно настроить фильтры можно только после получения существенной части рассылки.

Сегодня широко используются три последних метода — далеко не все антиспам-средства могут с ними нормально бороться, что даёт возможность доставлять спам тем пользователям, которые используют недостаточно продвинутые средства фильтрации.

«Нигерийские» письма

«Нигерийский» спам — это разновидность компьютерного мошенничества, попытка под неким вымышленным предлогом получить доступ к банковскому счёту пользователя или иным путём получить с него деньги.

В качестве стандартного предлога в «нигерийских» письмах выступает необходимость обналичить крупную сумму денег. Спамер обычно утверждает, что он располагает миллионами долларов, но они приобретены не совсем законным способом или же хранятся в обход закона. Например, это украденные иностранные инвестиции или гранты ООН. Далее автор письма объясняет, что по этой причине он не может разместить деньги на счету в банках своей страны, и что ему срочно требуется счёт в зарубежном банке, куда можно перечислить «грязные» деньги. Ещё одна типичная версия — деньги нажиты легитимным путём либо получены в наследство, однако в связи с политической нестабильностью в стране обналичить их невозможно.

Так или иначе, у получателя «нигерийских» писем просят помощи в обналичивании крупной суммы денег. В качестве вознаграждения за помощь предлагается от 10 до 30% от заявленной в письме суммы.

Идея мошенничества заключается в том, что доверчивый пользователь предоставляет автору письма доступ к своему счёту. Нетрудно предугадать результат — все деньги с этого счёта будут сняты и уйдут в неизвестном направлении. Либо мошенники просят небольшую по сравнению с будущим вознаграждением сумму денег (несколько тысяч долларов), которая якобы необходима для успешной реализации плана, и, получив её, исчезают. Ещё один вариант — мошенники уговаривают пользователя приехать в Нигерию или другую нестабильную страну, где уже начинается настоящее вымогательство, шантаж и угрозы.

Этот вид спама отличается от многих других тем, что спамеры вынуждены поддерживать обратную связь с получателями писем, поэтому в «нигерийских» письмах обратный адрес или даже контактный телефон доступны для связи, что позволяет правоохранительным органам разных стран успешно отслеживать мошенников. Известны случаи арестов и судебных процессов над организаторами подобных рассылок.

«Нигерийскими» письма называются потому, что этот вид мошенничества был изобретён в Нигерии, за что нигерийские спамеры даже получили в 2005 году так называемую анти-Нобелевскую премию в области литературы. Ещё одно название, используемое в англоязычных документах, — «scam 419». Оно также связано с Нигерией: 419 — это номер статьи нигерийского закона, запрещающей, в частности, этот вид мошенничества.

Почему именно Нигерия? Эта страна имеет печальную репутацию одной из самых коррумпированных в мире. За время хаоса и военных дик-

татур, сменявших друг друга в течение двадцати лет, в стране укоренилась преступность. По уровню доходов от внешних валютных операций в настоящее время мошенничество в Нигерии занимает четвёртое место.

До сих пор тысячи людей во всём мире получают письма от мнимых бывших диктаторов, несуществующих нигерийских бизнесменов или служащих нигерийских министерств. Однако «нигерийские» письма уже давно рассылаются мошенниками разных стран.

Спамеры оперативно реагируют на ситуацию в мире, отслеживая очаги нестабильности. Поэтому постоянно появляются новые разновидности «нигерийских» писем — например, «кенийские» или «филиппинские». Во время войны в Ираке активно шли спамерские рассылки «иракского» спама. Это письма, в которых речь идёт о деньгах, украденных во время военных действий в Ираке. Авторы таких писем обычно подписываются вымышленными или настоящими именами высокопоставленных иракских лиц. Нередко письмо написано от имени жены или вдовы какого-либо иракского чиновника.

Подавляющее большинство «нигерийского» спама идёт на английском языке, но в 2004–2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни. Внимание спамеров привлекло нашумевшее дело ЮКОСа и пользователям Рунета было предложено обналичить миллионы Ходорковского.

Когда дело ЮКОСа стало известно и на западе, спамеры вновь перешли к рассылкам на английском языке. Очевидно, на такую приманку, как проценты за обналичку, пока больше «клюют» зарубежные пользователи. Либо среди доверчивых россиян не так много людей со своими счетами в банках, куда можно переводить крупные суммы денег. Либо у нас не так много доверчивых пользователей, как кажется.

Профилактика спама

Проблемы с рекламными рассылками (спамом) у частного пользователя начинаются в тот момент, когда его email-адрес попадает в базу данных к спамерам. Выполнение приводимых ниже рекомендаций специалистов поможет максимально отдалить этот момент.

Откуда спамеры узнают ваш адрес

Спамеры находят email-адреса своих жертв различными способами:

- сканируя веб-сайты;
- сканируя доски объявлений, форумы, чаты, Usenet News и так далее;
- подбирая «лёгкие» адреса (jonh@, mary@, alex@, info@, sales@, support@) по словарю имён и частых слов;
- подбирая «короткие» адреса (aa@, an@, bb@, abc@) простым перебором.

Исходя из этого частному пользователю можно порекомендовать следующие меры:

1. Заведите себе два адреса — частный для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках) и публичный — для публичной деятельности (форумов, чатов и так далее).

2. Адрес для переписки никогда не должен публиковаться в открытом доступе.

3. Адрес для переписки не должен быть лёгким в запоминании или «красивым». Ваше имя или красивое слово — не подходят. Vasily.M.Pupkin-IV — подходит вполне. Чем длиннее адрес и чем менее он удобочитаем — тем лучше.

4. Если нужно сообщить свой приватный адрес (в конференции, на сайте) — делайте это способом, непригодным для автоматического прочтения сборщиком адресов. «Ivan-точка-Susanin-собака-mail-точка-ру» — хороший способ. «Ivan.Susanin at mail.ru» — гораздо хуже, Ivan.Susanin@mail.ru — никуда не годится. Если речь идёт о публикации на сайте, можно опубликовать адрес в виде картинки.

5. Адрес для публикации нужно заранее считать временным. Не стоит его жалеть — вы всегда можете завести новый. Как правило, спам начинает приходить на него через несколько дней после публикации. Поскольку этот адрес могут использовать не только спамеры (туда будет приходить и нормальная почта), стоит его периодически просматривать. Вы можете читать почту, приходящую на него, раз в неделю или раз в месяц.

Регистрации на сайтах

Некоторые интернет-магазины, конференции, форумы и т.п. требуют регистрации с указанием работающей электронной почты. Иногда переданные таким образом адреса попадают к спамерам. Далеко не всегда это злой умысел, но пользователям от этого не легче. Поэтому:

6. При регистрациях всегда указывайте публичный адрес. Он всё равно может считаться потерянным. Можно на каждую регистрацию заводить новый адрес на бесплатных почтах — тогда вы будете знать, кто из магазинов и форумов «продал» ваш адрес спамерам.

Спам всё равно приходит. Что делать?

Если спама приходит немного и с ним ещё можно мириться, то следует придерживаться простых правил:

1. Никогда не отвечайте спамеру. Возможно, ничего плохого не произойдёт. Но может случиться и так, что ваш ответ прочитает «робот» и пометит ваш адрес как «живой» — в результате спама будет приходить ещё больше.

2. Не пытайтесь воспользоваться ссылкой «отписаться», если вы не уверены, что она сработает. Возможно, вас действительно отпишет данный конкретный рассыльщик. Но при этом ваш адрес могут пометить как действующий... и спама станет больше. Узнать, что случится, можно, только попробовав. Но хотите ли вы этого?

Если мириться со спамом уже никак нельзя:

3. Смените свой «частный» адрес. На некоторое время это поможет.

Я никому не давал адрес, кроме самых близких знакомых, но на него приходит спам.

К сожалению, ваш адрес мог быть украден из адресной книги вашего знакомого почтовым вирусом (который рассылается по адресной книге). Какого-либо разумного способа уберечься от этого не существует — даже если у всех знакомых есть антивирус-

ная программа, у неё должны быть обновлённые базы данных и т.д.

Мне нужен адрес, куда всякий желающий мог бы написать!

Если вы хотите всё-таки иметь общеизвестный и общедоступный адрес, приготовьтесь получать туда сотни спам-сообщений в сутки. Если не повезёт — то тысячи в сутки. Если от такого адреса вы не хотите отказываться, то остаётся последний совет:

4. Используйте антиспам-фильтр — или на сервере, выбрав провайдера с услугой фильтрации спама, или у себя на компьютере, выбрав средство, подходящее для вашего почтового клиента. Современные фильтры обладают достаточно высоким качеством (процент фильтруемого спама у хороших и хорошо настроенных фильтров достигает 95–99%), и их использование резко снизит остроту проблемы.

Методический комментарий

Задача направлена на расширение знаний учащихся то теме «Вредоносное программное обеспечение» и на формирование навыков безопасного поведения в глобальной сети.

Ключевыми являются слова: «спам», «нигерийское письмо»; фразы: «массовая рассылка», «защита почтового ящика от массовых рассылок».

Имя задачи: Троянский конь

Автор: Селихова Татьяна Юрьевна, учитель информатики и ИКТ средней школы № 4 с. Монастырище Черниговского района Приморского края.

Предмет: Информатика и ИКТ.

Класс: 9.

Тема: Вредоносное программное обеспечение.

Профиль: Общеобразовательный.

Уровень: Общий.

Текст задачи. Сегодня вряд ли найдётся пользователь ПК, который не слышал бы о существовании троянских программ. Некоторые относят их к вирусам, другие считают, что это особая категория вредоносного ПО. Впрочем, пользователь может и не ощущать явного вреда от этих программ, так как они устанавливаются либо под видом полезных продуктов, либо вообще незаметно для человека.

Установите, является ли троянская программа вирусом? Чем грозит появление такой программы на компьютере? И почему именно троянская, а не римская или греческая?

а) Выделите ключевые слова для информационного поиска.

б) Найдите и соберите необходимую информацию.

в) Обсудите и проанализируйте собранную информацию.

г) Сделайте выводы.

д) Сравните ваши выводы с культурным образцом.

Возможные информационные источники

Web-сайты:

http://www.securelist.com/ru/glossary?glossid=152528302

http://www.compress.ru/article.aspx?id=10521&iid=430

www.viruslist.ru

Культурный образец

www.wikipedia.ru

Троя́нская программа (также — троян, троянец, троянский конь,

трой) — вредоносная программа, проникающая на компьютер под видом безвредной.

«Троянские кони» не имеют собственного механизма распространения и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам, и «червей», которые копируют себя по сети. Впрочем, троянская программа может нести вирусное тело, тогда запустивший троянца превращается в очаг «заразы».

http://webcity-software.ru/ — WEBCITY™Business Network Лицензионное программное обеспечение Троянские программы.

Троянские программы — это программы, используемые злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. Действие троянской программы может и не быть в действительности вредоносным, но трояны заслужили свою дурную славу за их использование в инсталляции программ типа Backdoor. По принципу распространения и действия троян не является вирусом, так как не способен распространяться саморазмножением.

Троянская программа запускается пользователем вручную или автоматически — программой или частью операционной системы, выполняемой на компьютере-жертве (как модуль или служебная программа). Для этого файл программы (его название, иконку программы) называют служебным именем, маскируют под другую программу (например, установки другой программы), файл другого типа или просто дают привлекательное для запуска название, иконку.

Троянские программы часто используются для обмана систем защиты, в результате чего система становится уязвимой, позволяя таким образом неавторизированный доступ к компьютеру пользователя.

Троянская программа может в той или иной степени имитировать (или даже полноценно заменять) задачу или файл данных, под которые она маскируется (программа установки, прикладная программа, игра, прикладной документ, картинка). В том числе злоумышленник может собрать существующую программу с добавлением к её исходному коду троянских компонентов, а потом выдавать за оригинал или подменять его.

Схожие вредоносные и маскировочные функции также используются компьютерными вирусами, но в отличие от них, троянские программы не умеют распространяться самостоятельно. Вместе с тем троянская программа может быть модулем вируса.

Название «*троянская программа*» происходит от названия «**троянский конь**» — деревянный конь, по легенде подаренный древними греками жителям Трои, внутри которого прятались воины, впоследствии открывшие завоевателям ворота города. Такое название, прежде всего, отражает скрытность и потенциальную коварность истинных замыслов разработчика программы.

Тела троянских программ почти всегда разработаны для различных вредоносных целей, но могут быть также безвредными. Они разбиваются на категории, основанные на том, как трояны внедряются в систему и

наносят ей вред. Существует шесть главных типов:

- удалённый доступ;
- уничтожение данных;
- загрузчик;
- сервер;
- дезактиватор программ безопасности;
- DoS-атаки.

Целью троянской программы может быть:

- закачивание и скачивание файлов;
- копирование ложных ссылок, ведущих на поддельные веб-сайты, чаты или другие сайты с регистрацией;
- создание помех в работе пользователя (в шутку или для достижения других целей);
- похищение данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам (в том числе третьих систем), выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях, криптографической информации (для шифрования и цифровой подписи);
- шифрование файлов при кодовирусной атаке;
- распространение других вредоносных программ — таких, как вирусы;
- вандализм: уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведение из строя или отказ обслуживания компьютерных систем, сетей и т.п., в том числе в составе ботнета (организованной группы зомбированных компьютеров), например, для организации DoS-атаки на целевой компьютер (или сервер) одновременно со множества заражённых компьютеров или рассылки спама. Для этого иногда используются гибриды троянского коня и сетевого червя — программы, обладающие способностью к скоростному распространению по компьютерным сетям и захватывающие заражённые компьютеры в зомби-сеть;
- сбор адресов электронной почты и использование их для рассылки спама;
- прямое управление компьютером (разрешение удалённого доступа к компьютеру-жертве);
- шпионаж за пользователем и тайное сообщение третьим лицам сведений — таких, как, например, привычка посещения сайтов;
- регистрация нажатий клавиш (Keylogger) с целью кражи информации такого рода как пароли и номера кредитных карточек;
- получения несанкционированного (и/или дарового) доступа к ресурсам самого компьютера или третьим ресурсам, доступным через него;
- установка Backdoor;
- использование телефонного модема для совершения дорогостоящих звонков, что влечёт за собой значительные суммы в телефонных счетах;
- дезактивация или создание помех работе антивирусных программ и файрвола.

Методический комментарий

Задача направлена на изучение программного материала и расширение знаний учащихся по теме «Вредоносное программное обеспечение».

Ключевыми являются слова: «вирус», «троянец»; фразы: «вредоносные программы», «троянская программа».