Министерство образования и науки РФ
Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий
Высшая школа программной инженерии

КУРСОВОЙ ПРОЕКТ
по дисциплине «ЦИФРОВАЯ ГРАМОТНОСТЬ»

КОМПЬЮТЕРНЫЕ ВИРУСЫ

Выполнил **И.С. Тампио**
Студент гр. 3530904/10002
Руководитель **В.С. Тутыгин**
Доцент, к.т.н.

Санкт-Петербург
2021

Оглавление

Введение

Компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако, в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление "первой ласточки", наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Для отдельных пользователей вирусы грозят утечкой личных данных, данных кредитных карт и аккаунтов, назойливой рекламой в операционной системе, её медленной работой или неработоспособностью, материальными убытками, в связи с чем необходимо обладать базовыми знаниями о противодействии им, чтобы этого избежать.

Вредоносное ПО

Определение вредоносного ПО

Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором определенном классе программ.

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера. Поскольку киберпреступники придумывают все более сложные способы проникновения в системы пользователей, рынок вредоносных программ существенно расширился.

Классификация вредоносного ПО

Вредоносное ПО можно классифицировать по следующим признакам:

- По способу попадания на компьютер пользователя
- По способу заражения
- По выполняемым действиям

Стратегии мошенников по способу попадания на компьютер пользователя

Подставные сайты приложений

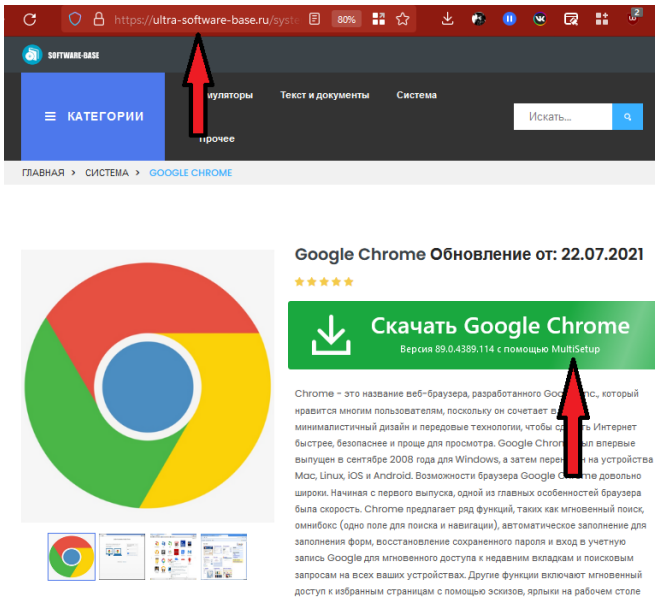

Рис. 1 Пример подставного сайта

Подставные сайты выдают себя за официальные, заставляя пользователя обманом загружать на свой компьютер вредоносное ПО.

Стоит отметить, что нередки случаи, когда подставные сайты попадаются в выдаче первее официальных, в связи с чем пользователю необходимо всегда быть начеку при загрузке исполняемого ПО.

Обычно такие сайты выглядят некачественно, адрес сайта пытается быть похожим на официальный. Пользователю следует скачивать ПО только из официальных источников, во избежание заражения ПК.

Эксплуатирование любопытности пользователя

К данному методу обмана можно привести – бесхозные физические носители (USB-Флешки) и «как бы случайно» отправленные «не туда» письма с файлами, название которых может вызвать интерес у получателя, провоцирующие открытие файла, который содержат в себе вредоносный код.

Возможные способы заражения

По способу заражения файлов вирусы делятся на

- перезаписывающие ("overwriting")
- паразитические ("parasitic")
- компаньон-вирусы ("companion")
- "link"-вирусы
- вирусы-черви
- вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Перезаписывающие

Данный метод заражения является наиболее простым: вирус меняет код файла другой программы на свой. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы легко обнаружить, так как операционная система и приложения перестают нормально функционировать.

Паразитические

Паразитические вирусы очень схожи с перезаписывающими, отличие заключается в том, что при распространении своих копий они изменяют файлы, обязательно оставляя сами файлы при этом полностью или частично работоспособными, что затрудняет выявление вредоносной программы. Основными типами таких вирусов являются вирусы, записывающиеся

- в начало файлов ("prepending"),
- в конец файлов ("appending")
- в середину файлов ("inserting").

Известны два способа внедрения паразитического файлового вируса в начало файла: первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место; вторым способ - вирус создает в оперативной памяти свою копию, дописывает к ней заражаемый файл и сохраняет полученную конкатенацию на диск.

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса. В свою очередь, внедрение вирусов в середину файлов происходит различными методами - путем

переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла ("cavity"-вирусы).

Компаньон-вирусы

К категории " компаньон" относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

Link-вирусы

Link-вирусы, как и компаньон-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

OBJ-, LIB-вирусы и вирусы в исходных текстах

Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится исполняемый, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками.

Классификация вирусов по типу действия

- *Рекламное ПО*
- *Шпионское ПО*
- *Программы-вымогатели*
- *Боты (Манеры + доз)*
- *Руткиты*
- *Черви*

Рекламное ПО

Рекламное ПО приводит к появлению рекламы в системе. Так, если в браузере появилось больше рекламы, даже с учётом установленного блокировщика рекламы, или всплывают рекламные сообщения даже вне интернет-браузера, можно считать, что вредоносное ПО - рекламное. Злоумышленник получает прибыль посредством продажи такой рекламы или отправлениям пользователя на сайты других мошенников.

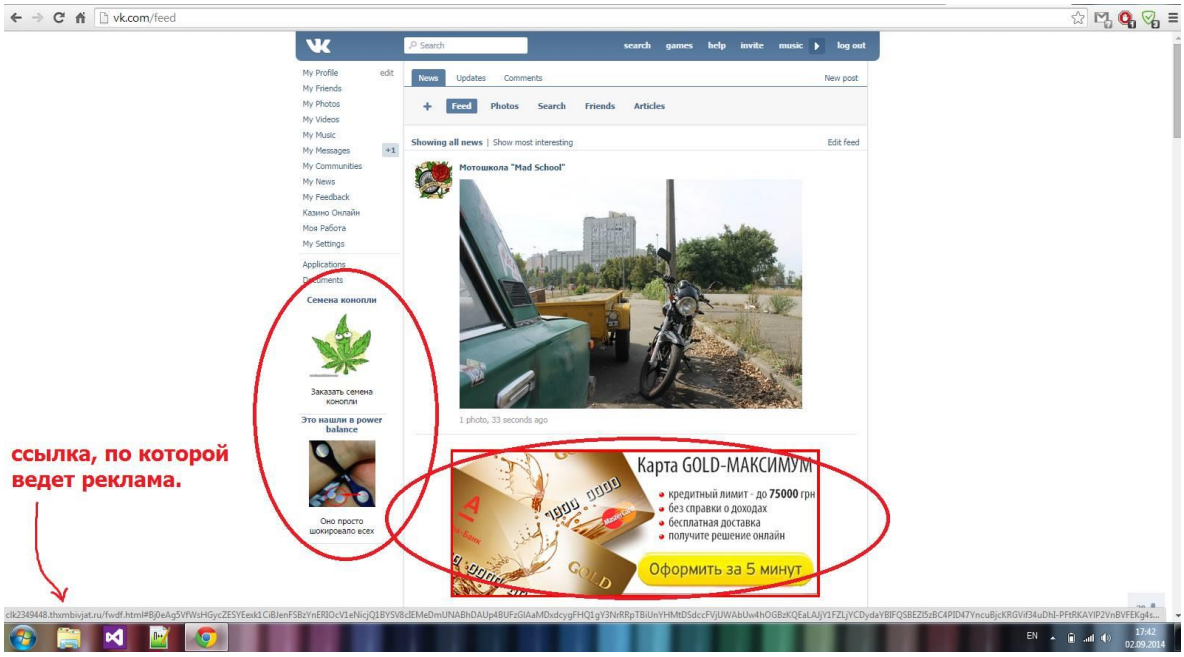

Рис. 2 Влияние рекламного ПО на сайты

Шпионское ПО

Явно эти вирусы себя не проявляют, поэтому простому пользователю о вирусе-шпионе могут начать говорить уже последствия - списания со счетов банковских карт, украденные аккаунты и многие другие. Как правило, антивирусные программы выявляют такие вирусы довольно быстро. Если же не пользоваться антивирусом, то вряд ли вы сможете узнать о слежке без тщательного анализа исходящего интернет-трафика. Одним из наиболее распространённых видов шпионского ПО являются Кей логгеры, отправляющие злоумышленнику ввод пользователя с клавиатуры, тем самым позволяя украсть логины, пароли, данные кредитных карт и другие данные.

Программы-вымогатели

Такие программы редко скрываются и наоборот, ведут себя крайне агрессивно по отношению к пользователю. У них говорящее название - их главной целью является вымогание денежных средств у пользователя под угрозой удаления файлов, уничтожения системы. При этом файлы системы шифруются, чтобы пользователь не мог обойти платёж. Одной из их разновидностей являются Win Locker'ы. Они получили такое название поскольку не позволяют пользователю сделать ничего на своём компьютере до перечисления средств. Одним из самых известных вымогателей был вирус Petya.A, суммарные убытки от него превысили 10 миллиардов долларов США в более чем 60 странах мира.

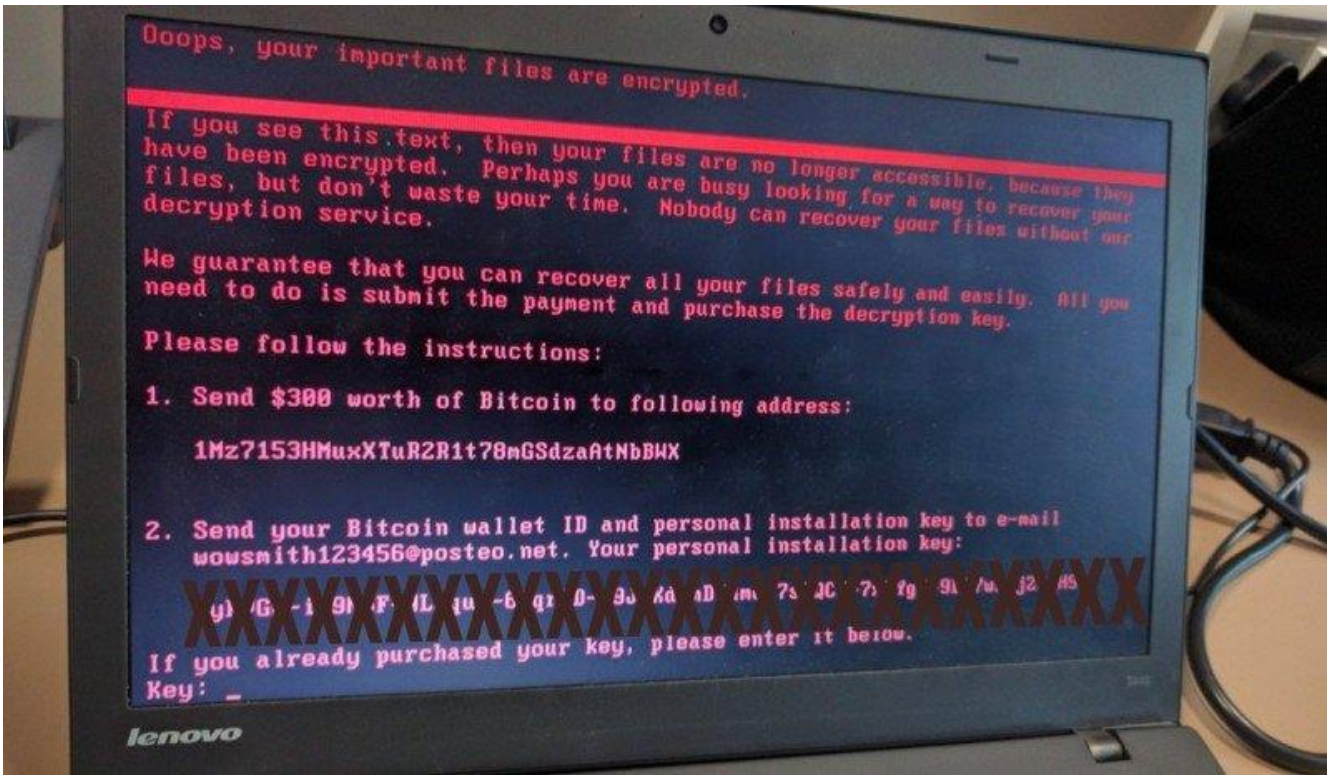

Рис. 3 Вирус-вымогатель Petya.a

Боты или Руткиты

Признаком таких вирусов является высокая периодичная или постоянная нагрузка на компьютер (просматривается в диспетчере задач). В таких случаях компьютер пользователя становится частью ботнета и на нём злоумышленник может удалённо исполнять команды для своих целей, в частности, установка других вирусов и использование вычислительной мощности компьютера в DDOS атаках или майнинга криптовалюты.

Черви

От вас вашим друзьям и коллегам не по вашей воле отправились сообщения с сомнительным содержанием, а на остальных устройствах в компьютерной сети появились файлы, которые пользователь не скачивал? Это признаки червя. Главная цель червей - дальнейшее распространение самих себя по компьютерным сетям, заражение как можно большего количество устройств. Зачастую для максимальной эффективности черви совмещены с другими вирусами (например Petya.A), вследствие чего могут возникать целые «эпидемии».

Противодействие вредоносному ПО

Существует миф, что вирусы могут нанести физический вред вашему компьютеру или навсегда заразить компьютер. Это неправда, поскольку компьютерные вирусы сохраняются только на жёстких дисках. Из чего вытекают следующие методы «вылечить» заражённый ПК.

Переустановка системы с форматированием жёстких дисков

Поскольку вирус содержится в файловой системе операционной системы, переустановка системы с удалением всех файлов на жёстком диске позволит вылечить компьютер.

Данный метод имеет следующие недостатки:

- Если компьютер заражён вымогателем-шифровальщиком, в большинстве случаев данные восстановить не удастся.
- Если компьютер заражён винлокером, не шифрующим данные, данные можно извлечь, открыв жёсткий диск компьютера, подключив его к другому компьютеру как дополнительный.
- Метод требует установки системы и повторной её настройки, что может быть трудоёмким и времязатратным процессом.
- Более того, переустановка системы пусть и является несложным процессом, для простого пользователя она может быть непонятной и сложной.

С другой стороны, все эти недостатки компенсируются тем, что состояние системы возвращается к исходному, заводскому состоянию и работает в 100% случаев.

Отдельные случаи рекламного ПО

Как ни странно, некоторое вредоносное ПО, добавляющее рекламу в систему, содержит деинсталляторы, позволяющие их без лишних проблем удалить. В таком случае необходимо просто запустить программу деинсталлятор и удалить вирус.

Использование антивируса

Главной задачей программ-антивирусов является выявление вредоносного ПО посредством сравнения сигнатуры программы с теми, что хранятся в базе данных антивируса. Антивирус, конечно, не является гарантированным способом удаления и выявления вирусов, однако для большинства вредоносного программного обеспечения они работают и являются простым средством лечения компьютера.

У данного метода тоже есть свои недостатки:

- Для своевременного выявления вредоносного ПО антивирусу требуется сканировать множество файлов и целые диски, причём на регулярной основе, что сильно нагружает систему.
- Наличие антивируса на компьютере не предотвращает его от заражения.

Однако, помимо сканирования файловой системы антивирус тщательно анализирует все настройки операционной системы вплоть до состояния реестра и интернет-трафика, что позволяет выявлять более скрытные вирусы. Более того, такой метод является превентивным и быстрым, простым для пользователя, что делает его идеальным для рядового пользователя компьютера.

Заключение

В заключение хотелось бы сказать, что заражения компьютера это в первую очередь ошибка пользователя. Человеческий фактор в данном деле играет главную роль. Недаром существует отдельный раздел информационной безопасности социиальная инженерия, посвященный эксплуатации людей. Поэтому будь то в компаниях или в семье, необходимо знать и соблюдать правила базовой информационной безопасности – не скачивать файлы с подозрительных сайтов, не открывать неизвестные документы, тем более от незнакомцев.

Конечно, полностью предостеречь себя от заражения нельзя, ровно как человек не может гарантированно себя обезопасить от простуды, и поэтому важно знать, как «лечить» компьютер. Простому пользователю, знающему как установить антивирус это под силам.

Стоит сказать, что излишние меры по борьбе с вирусом, вроде ежедневных проверок антивирусом всего жёсткого диска или форматирования компьютеров компании при малейшем подозрении на вирус не являются целесообразными, поскольку такие опасения могут привести к крупнейшим денежным, временным, информационным и вычислительным тратам.

В конце концов, я бы посоветовал каждому неопытному пользователю, желающему себя обезопасить установить Dr. Web – это легковесный антивирус, не требующий значительных ресурсов компьютера для работы.

Кроме того, даже если ваш компьютер заразил вирус, а антивирус его не распознал, методы борьбы с отдельными вирусами описаны на многих сайтах, что можно найти в интернете.

Список иллюстраций

Список литературы

1. Платонов, В.В. Методы функционирования компьютерных вирусов и защиты от них: Руководство к практическим занятиям — СПб., 2003. – 42 с.
2. Проникновение через USB // xakep.ru URL: https://xakep.ru/2014/07/07/usb-penetration-testing/ (дата обращения: 17.10.2021).
3. NotPetya: World's First $10 Billion Malware // Apex Technology Services URL: https://www.apextechservices.com/ (дата обращения: 17.10.2021).
4. 'Petya' ransomware: Everything you need to know // Windows Central URL: https://www.windowscentral.com/ (дата обращения: 17.10.2021).
5. The Concept Virus // Flashing Cursor URL: http://www.chebucto.ns.ca/~af380/ConceptMacro.html (дата обращения: 17.10.2021).
6. What’s the Difference between a Virus and a Worm? // kaspersky URL: https://usa.kaspersky.com/resource-center/threats/computer-viruses-vs-worms (дата обращения: 17.10.2021).
7. Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы // kaspersky URL: https://www.kaspersky.ru/ (дата обращения: 17.10.2021).
8. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е изд. — СПб.: Питер, 2013. — 816 с.

Предметный указатель