В современном мире существует очень много различных вирусов, которые могут подвергнуть большой опасности работу любого персонального компьютера. Помимо крупных промышленных вирусов, которая создана специально для того, чтобы парализовать работу серьёзных предприятий, существуют также ещё и обыкновенные бытовые вредоносные программы, блокирующие работу тех или иных узлов персонального компьютера.

В любом случае, каждый человек, который так или иначе работает с современными технологиями, обязательно должен знать, какие существуют компьютерные вирусы и каким образом с ними бороться. Вирусы не дают человеку возможности использовать персональный компьютер или любое другое умное устройство по назначению, парализуя определённые элементы как в плане железа, так и софта.

Что такое вирус?

Прежде, чем прикасаться к самым опасным вредоносным программам, стоит определить, что такое компьютерный вирус. Как и вирус в классическом понимании, компьютерный вирус представляет собой нечто вредоносное, что наносит определенный урон работе системы. Только если в организме вирус представляет собой организм, питающийся тканями или клетками носителя, то в компьютерной среде вирусом является вредоносная программа, включающаяся в работу всей системы. В качестве объектов для проникновения вируса могут быть следующие элементы персонального компьютера:

Устройства ввода и вывода изображения, то есть графический ускоритель. Если тот или иной вирус попадет в персональный компьютер и заблокирует данный элемент, то он парализует работу устройства вывода изображения на экран.

Модули памяти. При этом, сюда можно отнести как жёсткий диск, так и модуль Ram.

Также, для многих вирусов приоритетными целями являются загрузочные секторы, в которых можно отложить определённые копии вредоносных программ, дабы не быть обнаруженным антивирусом.

Каждый вирус выполняет ту или иную заложенную функцию. Некоторые вирусы являются просто продуктом вредоносных программ, которые выполняют одну и ту же цикличную операцию, не давая персональному компьютеру выполнять свои обыкновенные задачи и работать в классическом режиме. Персональный компьютер может воспринимать вирусы и другие вредоносные программы как часть системы и ничего с ними делать. При этом, если компьютер не получает определённых указаний от антивируса, то он посчитает вредоносные элементы частью системы. Итак, уяснив, что такое вирусы, следует перейти к нескольким самым популярным вредоносным программам в мире. Их нужно опасаться и пытаться вывести, знай врага в лицо.

Многослойный вирус под кодовым названием Nimda

Данный вирус представляет собой программный червь, который целиком и полностью повреждает определённые файлы персонального компьютера. Первым появлением считается конец сентября 2001 года, когда один из офисных персональных компьютеров был подвергнут полной блокировке после того, как был активирован данный вирус. Его суть заключалась в том, что червь полностью уничтожал или заменял файлы, осуществляя тем самым саботажную деятельность. Непонятно кто его написал, однако известно, что вирус может распространяться несколькими способами, что делает его одним из самых опасных червей в современном интернете. Хоть его и не часто можно встретить в 2019 году, в начале двухтысячных он испортил массу полезных файлов на персональных компьютерах по всему земному шару. Многослойный вирус довольно сложно побороть, однако имеет смысл постоянно обновлять вирусные базы современных антивирусов. Было много случаев, когда вирус можно было побороть, если иметь копии файлов и не полагаться на облачные системы.

Опасный червь Conficker

Возвращаясь к современному интернету, стоит вспомнить еще один не менее известный червь под названием Conficker. Его впервые обнаружили зимой 2009 года, когда были заражены 12,5 млн персональных компьютеров. Самое интересное, что были заражены как корпоративные важные компьютеры, так и обычные домашние машины простых пользователей. Если подсчитывать весь ущерб, который был нанесен данным вирусом, то он будет составлять около 10 млрд долларов. После того, как был оценен ущерб, компания Microsoft пообещала награду энтузиастам, которые сделают надежную блокировку от вируса. Награда составляет 250000 долларов. Кроме того, эти денежные средства можно было получить за слив информации о тех, кто создал данный вирус. Пока что информация не поступила, однако многие разработчики программного обеспечения антивирусов смогли защититься от данной вредоносной программы. Таким образом, угроза миновала многие тысячи пользователей. Этот вирус сложно побороть переустановкой операционной системы. Он блокирует некоторые элементы, заставляя пользователя не только переустанавливать систему, но ещё и переписывать основной жёсткий или твердотельный диск.

Ещё один опасный вирус под названием Storm Worm

Этот вирус является популярным троянским конем, который умеет маскироваться под многие обыкновенные системные файлы. Он был обнаружен в 2007 году на персональных компьютерах 230 тысяч человек по всему миру. Суть в том, что данный вирус распространяется через электронную почту, тем самым маскируясь под обыкновенный спам. Естественно, помимо спама злоумышленники могут подделывать и любые другие сообщения, через которые можно просочиться на персональный компьютер жертвы. На сегодняшний день от вируса пострадало около 10 млн персональных компьютеров. Вирус легко лечится путем сканирования Dr.Web или Касперский, однако до этого он может нанести массу вреда своей назойливой рекламой и рассылкой спама. Как правило, его используют многие недобросовестные маркетологи для того, чтобы рассылать низкокачественный спам и отталкивающую рекламу. После того, как компьютер жертвы будет зараженным вирусом, пользователь лишится своих личных данных, которые будут отправлены злоумышленникам.

Разрушитель BIOS под названием Чернобыль

Этот вирус был разработан не со злого умысла, а как демонстрация уязвимости BIOS в Windows 95 и 98. Его сделал тайваньский студент в качестве демонстрации того, как злоумышленники могут заблокировать работу масс компьютеров. Несмотря на свои нейтральные намерения, студент нанес ущерб в 1 млрд долларов, после чего добровольно сдался. На сегодняшний день автор работает в компании Gigabyte, разрабатывая программное обеспечение для них.

Вирус Петя - бич современного мира компьютерных технологий

В 2016 году был вирус с кодовым именем Петя. Данный вирус относится к так называемым вредоносным программам вымогателям, которые блокируют все системы, переписывают файлы и вымогают определённое количество денег в качестве выкупа. Распространяется различными путями, среди которых можно выделить:

Распространение по электронной почте путем рассылки спама или подделки деловых документов жертвы.

Рассылка сообщений с различными просьбами.

Размещение провокационного контента на сайтах. После того, как жертва даст соответствующие разрешения в браузере, специальный вирус проникнет на жесткий диск или твердотельный накопитель, тем самым заразив персональный компьютер и все машины в сети.

Вирус Петя заражает персональные компьютеры под управлением операционной системы Windows, делая корпоративные машины максимально уязвимыми. Самое главное, что ни одна из имеющихся в сети антивирусных компаний не смогла найти достойный отпор этому вредоносном программному обеспечению. Особенность вируса Петя заключается в том, что программа не блокирует разделы жесткого диска, а просто-напросто переписывает их в другой код. Таким образом, на дешифровку файлов уходит огромное количество времени, электроэнергии и денежных средств. Создатели вируса делали упор на то, что корпоративные персональные компьютеры не будут противиться вирусной атаки, что вынудит их владельцев заплатить выкуп в биткоинах. Массовые заражения были как в начале 2016, так и конце 2017 года. От вируса пострадали люди по всему земному шару. При этом, большая часть жертв были из корпоративного сегмента. На территории Российской Федерации были заражены персональные компьютеры таких организаций, как Сбербанк, Роснефть, Башнефть и Хоум Кредит. Заражение не распространяется на компьютере под управлением операционной системы Mac OS.

Именно поэтому главным оружием против подобного рода вирусов являются разные операционные системы, которые должны быть установлены на нескольких персональных компьютерах человека. Пока что не было пресечено ни одной попытки похитить данные с помощью вируса Пети.

Что такое сетевые черви и как с ними бороться?

В компьютерной среде есть очень много различных обозначений вирусов и прочих вредоносных программ. Во главе угла в рейтинге самых вредоносных и опасных вирусов стоят так называемые черви. Именно о них и стоит поговорить подробнее.

Черви — это специальные компьютерные программы, которые целиком и полностью распространяются через сеть Интернет. Помимо сети Интернет, для распространения используются различные локальные сети и всевозможные оффлайн способы передачи. Официально червями стали заниматься ещё с середины восьмидесятых годов в фирме Ксерокс. Специалисты данной компании были поражены тем фактом, что их ценная информация может быть целиком и полностью похищена с основных персональных компьютеров и отдаленных дата-центров организации. Для того, чтобы защитить те или иные файлы, а также приватные документы, специалисты проводили различные эксперименты, которые дали определенные результаты. Так, например, были получены сведения о том, как распространяются черви по компьютерам. Пока что существуют следующие типы способов распространения:

Прежде всего, черви распространяются путем поиска уязвимостей. При этом, поиск осуществляется вручную и передаётся через сеть Интернет самому червю. Если злоумышленники узнали о том, что существуют определенные бреши в системе управления или администрирования, то червь непременно воспользуется этой лазейкой и проникнет в святая святых системы.

Также, для проникновения в систему и поиска уязвимости используется социальная инженерия. Злоумышленникам гораздо проще взломать почтовый ящик и похитить оттуда те или иные сведения о том, какими уязвимостями страдает та или иная система жертвы. Также есть вариант проникнуть на личную страницу высокопоставленного человека и от имени другого пользователя узнать определенные данные.

Червь ищет уязвимость, проникают вглубь системы и выполняет поставленную задачу. После того, как червяк похитит необходимые данные или проведёт саботаж или иную деятельность, программа перестает работать и в некоторых случаях даже не отображается в реестре. Эффективным способом защиты является установка самых последних вирусных баз в антивирус. А чтобы максимально обезопасить себя, нужно диверсифицировать риски. Это делается путем установки на разные носители разных операционных систем. Идеальный вариантом будет установить на один ПК Windows, а на другой Linux. Этот простой шаг поможет обезопасить множество операций.

Список литературы:

1. Н.Н.Безруков "Классификация компьютерных вирусов MS-DOS и методы защиты от них", Москва, СП "ICE", 2009.
2. Безруков Н.Н. "Компьютерные вирусы", Москва, Наука, 2010.
3. Мостовой Д.Ю. "Современные технологии борьбы с вирусами" // Мир ПК. - №8. - 2009.