Смирнова К.А.,

студентка бакалавриата

Шуйский филиал Ивановского государственного университета,

ksyunya-smirnova-99@mail.ru

Компьютерные вирусы и антивирусные программы

Аннотация. В статье говорится о том, что такое компьютерные вирусы, и как знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать.

Ключевые слова: компьютерный вирус, антивирусная программа, обнаружение, локализация, защита.

Smirnova K.A.,

undergraduate

Shuy branch of Ivanovo State University,

ksyunya-smirnova-99@mail.ru

Computer viruses and antivirus programs

Annotation. The article says that these are computer viruses, as well as their features in the structure and distribution of computer viruses, which will facilitate their detection and localization.

Keywords: computer virus, antivirus program, detection, localization, protection.

Навряд ли нужно припоминать, что компьютеры начали реальными ассистентами человека и в их отсутствии сейчас не возможно ограничиться ни торговая компания, ни национальное предприятие. Но в связи с этим в особенности обострился вопрос защиты данных.

Вирусы, возымевшие обширное продвижение в компьютерной технической, всполошили целый свет. Многочисленные юзеры пк взволнованы слушками о том, что с поддержкой компьютерных вирусов преступники ломают сети, грабят банки, похищают умственное имущество...

На сегодняшний день массовое использование личных пк, к огорчению, обнаружилось сопряженным с возникновением самовоспроизводящихся

программ-вирусов, мешающих стандартной работе компьютера, рушащих файловую текстуру дисков и наносящих вред хранимой в пк данных. Все чаще в средствах массовой информации возникают известия о разного рода пиратских шалостях компьютерных хулиганов, о возникновении все наиболее безупречных саморазмножающихся программ. Совсем не так давно инфицирование вирусом текстовых файлов значилось вздором - в настоящее время этим уже никого отнюдь не удивишь. Стоит только припомнить появление "первой ласточки", наделавшей большое количество шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 также 7.0. Невзирая на установленные в множества государствах законы о борьбе с компьютерными правонарушениями также исследование специализированных программных средств охраны с вирусов, число новейших программных вирусов регулярно увеличивается. Это потребует от юзера индивидуального пк познаний о натуре вирусов, методах инфицирования вирусами, а также защиты от них.

Хочется одновременно отметить, что излишне опасаться вирусов никак не нужно, в особенности если пк приобретен не так давно, и большое количество данных на жестком диске еще не скопилось. Вирус компьютер никак не подорвет. В настоящее время популярен только лишь единственный вирус (Win95.CIH), который может подпортить "железо" пк. Прочие же имеют все шансы только ликвидировать сведения, не более того. В литературе крайне упорно пропагандируется, что покончить с вирусами возможно только при поддержке трудных (также дорогих) противовирусных программ, и будто бы только лишь под их охраной вы сможете ощущать себе в абсолютной защищенности. Это не совсем так - ознакомление с отличительными чертами структуры и методами введения компьютерных вирусов сможет помочь своевременно их выявить и ограничить, в том числе и в случае, если под рукой не очутится оптимальной противовирусной программы.

Что же такое компьютерный вирус?

Компьютерный вирус – это намеренно написанная незначительная согласно масштабам программа, которая способна «приписывать» себя к иным программам, и кроме того, осуществлять разнообразные ненужные воздействия на пк. Программа, внутри которой располагается вирус, именуется «зараженной». Если подобная программа начинает работу, в таком случае сперва руководство обретает вирус. Вирус обнаруживает и

«заражает» прочие программы, а также осуществляет какие-нибудь вредоносные воздействия (к примеру, губит комп.данные либо таблицу размещения файлов в диске, «засоряет» эксплуатационную память и т. д.). Вирус – это программа, имеющая возможность к самовоспроизведению. Подобное умение считается одним-единственным качеством, свойственным абсолютно всем видам вирусов. Вирус никак не способен действовать в «полной изоляции». Данное обозначает, что на сегодняшний день невозможно вообразить для себя вирус, который бы так, либо по-другому не применял код иных программ, сведение о файловой структуре или даже попросту имена иных программ. Причина данного достаточно ясна: вирус обязан каким-нибудь методом гарантировать передачу себе управления.[3]

Кто и почему пишет вирусы?

Кто же пишет вирусы?

С точки зрения коммерческой версии вирусы создаются квалифицированными и опытнейшими программистами, прекрасно разбирающимися в защите нынешнего ПО. Преимущество — данные разработчики программного обеспечения прекрасно понимают аппарат деятельности правоохранительных организаций, занимающихся расследованием компьютерных правонарушений. Их основная задача — прибыль. Именно такого, сконцентрированного на заработок, вредоносного ПО в Сети больше всего.

На мой взгляд, основную их массу формируют учащиеся и подростки, которые только что усвоили язык ассемблера, стремятся попробовать собственные силы, однако не могут найти для них наиболее благородного использования. Радостен тот факт, что существенная доля подобных вирусов их создателями зачастую никак не расширяется, и вирусы через определенный период «умирают» совместно с дискетами, на которых хранятся. Подобные вирусы пишутся скорее всего только лишь для самоутверждения.
Другую категорию оформляют также молодое поколение (больше - учащиеся вузов), которые еще не целиком овладели искусством программирования, однако уже приняли решение посвятить себя написанию и популяризации вирусов. Только одна фактор, толкающий похожих людей на написание вирусов, это комплекс неполноценности, который выражает себя в компьютерном хулиганстве.

Из-под пера аналогичных «умельцев» зачастую выходят либо множественные вариации «классических» вирусов, или вирусы весьма простые и с огромным количеством погрешностей (подобные вирусы можно именовать «студенческими»). Существенно облегчилась жизнедеятельность таких вирусописателей уже после выхода конструкторов вирусов, присутствие поддержки которых можно формировать новые вирусы, в том числе и при минимальных познаниях об операционной системе и ассемблере, или даже если в целом не обладая об этом практически никакого представления. Их жизнедеятельность сделалась еще проще уже после выхода в свет макро-вирусов, так как взамен сложного языка Ассемблер для написания макро-вирусов в достаточной мере ознакомиться довольно простой Бейсик.
Став старше и опытнее, но так также не став взрослым, многие из таких вирусописателей оказываются в третьей, более опасной категории, которая формирует и запускает в общество «профессиональные» вирусы. Данные вирусы основательно продуманные и отработанные программы формируются высококлассными, зачастую весьма одаренными программистами. Подобные вирусы зачастую применяют довольно уникальные методы, не задокументированные и мало кому известные методы вторжения в системные области сведений. «Профессиональные» вирусы зачастую сделаны по технологии «стелс» и(или) считаются полиморфик-вирусами, заражают не только лишь комп.данные, но и загрузочные раздела дисков, а в некоторых случаях и выполняемые файлы Windows и OS/2.

Достаточно существенную долю в моей коллекции занимают «семейства» - группы из нескольких (в некоторых случаях наиболее десятка) вирусов. Представителей каждой их подобных компаний можно отметить согласно одной характерной черте, которая именуется «почерком»: в некоторых разнообразных вирусах попадаются одни и те же алгоритмы и способы программирования. Зачастую все без исключения или практически все представители семейства принадлежат одному создателю, и в некоторых случаях достаточно смешно наблюдать за «становлением пера» такого мастера - от почти «студенческих» усилий сформировать хоть что-нибудь, схожее на вирус, вплоть до абсолютно работоспособной реализации «профессионального» вируса.[5]
Согласно моему суждению, причина, заставляющая подобных людей обращать собственные возможности на подобную нелепую работу все та же - совокупность неполноценности, в некоторых случаях гармонирующий с

неустойчивой нервной системой. Показателен тот факт, что такое написание вирусов зачастую смешивается с иными пагубными увлечениями. Таким Образом, весной 1997 года один из наиболее популярных в обществе создателей вирусов по кличке Talon (Австралия) скончался в возрасте 21 года от смертельной дозы героина.

Несколько отдельно стоит 4-ая категория создателей вирусов - «исследователи». Данная категория заключается в достаточно смекалистых программистов, которые увлекаются открытием принципиально новейших способов инфицирования, скрытия, противодействия антивирусам и т.д. Они же изобретают методы введения в новейшие операционные системы, конструкторы вирусов и полиморфик-генераторы. Данные программисты пишут вирусы не для непосредственно вирусов, а скорее для «исследования» потенциалов «компьютерной фауны». Зачастую создатели аналогичных вирусов не запускают собственные творения в жизнь, но весьма стремительно пропагандируют собственные мысли посредством множественных электронных изданий, приуроченные к формированию вирусов. При этом угроза от подобных «исследовательских» вирусов не падает - попав в руки «профессионалов» из третьей категории, новые мысли весьма стремительно реализуются в новейших вирусах.
Отношение к создателям вирусов у меня тройственное. Во-первых, все без исключения, кто пишет вирусы либо содействует их популяризации, представлены «кормильцами» антивирусной индустрии, ежегодный оборот которой я расцениваю равно как минимум 2 сотни млн. $ или даже больше того (при этом не нужно выпускать из виду, что потери от вирусов составляют ряд сотен млн. $ каждый год и в разы превосходят затраты в антивирусные программы). Чем больше вирусов пишется, тем больше доход получают фирмы по созданию антивирусных программ. Конечно же, создателям вирусов не следует рассчитывать на материальное поощрение: как демонстрирует опыт, их деятельность была и остается безвозмездной. К тому же в настоящий момент предложение (новейшие вирусы) абсолютно удовлетворяет потребность (возможности антивирусных компаний по обработке новейших вирусов).

Во-вторых, мне несколько жалко создателей вирусов, в особенности «профессионалов». Ведь для того, чтобы составить такой вирус, следует: а) затратить достаточно большое количество сил и времени, при этом гораздо больше, нежели потребуется для того, чтобы понять в вирусе внести его в

основу данных или даже написать особый антивирус; и б) не обладать иного, наиболее заманчивого, занятия. Таким Образом, писатели вирусов - «профессионалы» довольно работоспособны и в то же время с этим мучаются от безделья - ситуация, как мне кажется, крайне грустная. И в-третьих, к моему отношению к создателям вирусов изрядно глубоко подмешаны чувства нелюбви и презрения равно как к людям, заведомо и напрасно расходующим себя в ущерб абсолютно всем другим.

Антивирусные программы, как метод защиты от компьютерных вирусов.

Итак, что же такое антивирус? Сразу же развеем одну зачастую возникающую иллюзию. По какой-то причине многие полагают, что антивирус способен выявить каждый вирус, то есть, запустив противовирусную программу или монитор, можно быть совершенно убежденным в их надежности. Такая точка зрения не полностью точна. Проблема в том, что антивирус- это в свою очередь программа, разумеется, написанная специалистом. Однако эти программы способны различать и истреблять только лишь популярные вирусы. В Таком Случае, имеется антивирус против конкретного вируса способный быть написанным только лишь в том случае, если у разработчика программного обеспечения имеется в наличии хотя бы один образец данного вируса. Вот и проходит данная нескончаемая борьба среди создателей вирусов и антивирусов, разумеется, первых в нашем государстве по какой-то причине преимущественно больше, нежели вторых. Однако и у разработчиков антивирусов имеется превосходство! Проблема в том, что существует огромное число вирусов, алгоритм которых почти скопирован с алгоритма иных вирусов. Как правило, подобные разновидности формируют непрофессиональные программисты, которые по каким-то обстоятельствам приняли решение составить вирус. Для борьбы с подобными "копиями" изобретено новейшее орудие - эвристические анализаторы. С их поддержкой антивирус способен обнаруживать похожие аналоги популярных вирусов, извещая юзеру, что у него, очевидно, завелся вирус. Безусловно, безопасность эвристического анализатора не 100%, но все же его показатель полезного воздействия более 0,5. Подобным способом, в данной информационной борьбе, как, впрочем, и в любой иной, остаются сильнейшие. Вирусы, которые не распознаются противовирусными детекторами, способны составить только лишь наиболее опытнейшие и грамотные программисты.[1]

Таким образом, на 100% защититься от вирусов почти нереально (предполагается, что пользователь изменяется дискетами с друзьями и

играет в игры, а также приобретает сведение с иных источников, к примеру с сетей). В случае если же не вводить сведение в пк снаружи, заразиться вирусом нереально - непосредственно он никак не появится. Ни один вид антивирусных программ по отдельности не предоставляет абсолютной защиты от вирусов. Наилучшей стратегией защиты от вирусов считается многоуровневая, "эшелонированная" защита. Средствам поиска в "обороне" от вирусов отвечают программы-детекторы, разрешающие обследовать вновь приобретенное программное обеспечение на наличие вирусов. На первом плане защиты находятся программы-фильтры. Данные программы имеют все шансы первыми проинформировать о работе вируса и избежать заражение программ и дисков. Второй эшелон защиты оформляют программы-ревизоры, программы-доктора и доктора-ревизоры. Наиболее полный состав защиты- это средства разделения доступа. Они не дают возможность вирусам и неверно работающим программам, в том числе и в случае, если они пробрались в компьютер, испортить важные данные.

.....

Литература.

1. *Денисов Т.В*. "Антивирусная защита" // Мой Компьютер, №4, 1999. - 36 с.
2. *Касперский Е.В*. Компьютерные вирусы: что это такое и как с ними бороться. - М.: СК Пресс, 1998г. - 288 с.
3. *Мостовой Д.Ю.* "Современные технологии борьбы с вирусами" // Мир ПК - №8, 1993. - 98 с.
4. *Файтс Ф., Джонстон П., Кратц М.* "Компьютерный вирус: проблемы и прогноз". Москва, "Мир", 1993. - 112 с.