МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по дисциплине

«ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Часть 1. Основные понятия и определения

для студентов специальностей
1-40 03 01«Искусственный интеллект» и
1-53 01 02 «Автоматизированные системы обработки информации»

БРЕСТ 2012

УДК 681.3

Данные методические указания содержат общие сведения по лекционному курсу и лабораторному практикуму по дисциплине «Основы защиты информации». В методических указаниях представлены материалы по защите компьютерной информации. Приведены основные термины и определения. Представлено дерево классификации вредоносных программ, а также правило поглощения при классификации и правило именования вредоносных программ. Рассмотрены основные методы детектирования вредоносных объектов.

Данные методические указания ориентированы на применение студентами специальностей «Искусственный интеллект» и «Автоматизированные системы обработки информации» в учебном процессе в рамках дисциплины «Основы защиты информации».

Издается в 2-х частях. Часть 1.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ

1.1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В Законе Республики Беларусь №455-З «Об информации, информатизации и защите информации» применяются следующие основные термины и их определения:

база данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях;

банк данных – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;

владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь;

доступ к информации – возможность получения информации и пользования ею;

доступ к информационной системе и (или) информационной сети – возможность использования информационной системы и (или) информационной сети;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;

информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;

информационная услуга – деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации;

информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;

комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;

обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору;

оператор информационной системы – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги;

пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею;

пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими;

предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц;

распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц;

собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями.

1.2. ПРИНЦИПЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Правовое регулирование информационных отношений осуществляется на основе следующих принципов:

– свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией;

– установления ограничений распространения и (или) предоставления информации только законодательными актами Республики Беларусь;

– своевременности предоставления, объективности, полноты и достоверности информации;

– защиты информации о частной жизни физического лица и персональных данных;

– обеспечения безопасности личности, общества и государства при пользовании информацией и применении информационных технологий;

– обязательности применения определенных информационных технологий для создания и эксплуатации информационных систем и информационных сетей в случаях, установленных законодательством Республики Беларусь.

1.3. СУБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Субъектами информационных отношений могут являться:

– административно-территориальные единицы Республики Беларусь;

– государственные органы, другие государственные организации;

– иные юридические лица, организации, не являющиеся юридическими лицами;

– физические лица, в том числе индивидуальные предприниматели;

– иностранные государства, международные организации.

Субъекты информационных отношений в соответствии с Законом могут выступать в качестве:

– обладателей информации;

– пользователей информации, информационных систем и (или) информационных сетей;

– собственников и владельцев программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

– информационных посредников;

– операторов информационных систем.

1.4. ПРАВО НА ИНФОРМАЦИЮ

Государственные органы, физические и юридические лица вправе осуществлять поиск, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации, пользование информацией в соответствии с Законом и иными актами законодательства Республики Беларусь.

Государственные органы, общественные объединения, должностные лица обязаны предоставлять гражданам Республики Беларусь возможность ознакомления с информацией, затрагивающей их права и законные интересы, в порядке, установленном Законом и иными актами законодательства Республики Беларусь.

Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды в порядке, установленном Законом и иными актами законодательства Республики Беларусь.

Право на информацию не может быть использовано для пропаганды войны или экстремистской деятельности, а также для совершения иных противоправных деяний.

1.5. ВИДЫ ИНФОРМАЦИИ

В зависимости от категории доступа информация делится на:

– общедоступную информацию;

– информацию, распространение и (или) предоставление которой ограничено.

К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

– о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;

– о деятельности государственных органов, общественных объединений;

– о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

– о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

– о состоянии преступности, а также о фактах нарушения законности;

– о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

– о размерах золотого запаса;

– об обобщенных показателях по внешней задолженности;

– о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

– накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

К информации, распространение и (или) предоставление которой ограничено, относится:

– информация о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– информация, составляющая коммерческую и профессиональную тайну;

– информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

Никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь.

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь.

Порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления информации о частной жизни физического лица и персональных данных, а также пользования ими устанавливается законодательными актами Республики Беларусь.

Документирование информации осуществляется ее обладателем в соответствии с требованиями делопроизводства, установленными законодательством Республики Беларусь.

Порядок документирования информации, обработки, хранения, распространения и (или) предоставления документированной информации, а также пользования ею устанавливается актами законодательства Республики Беларусь, в том числе техническими нормативными правовыми актами.

1.6. РАСПРОСТРАНЕНИЕ И ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

Распространяемая и (или) предоставляемая информация должна содержать достоверные сведения о ее обладателе, а также о лице, распространяющем и (или) предоставляющем информацию, в форме и объеме, достаточных для идентификации таких лиц.

При использовании для предоставления информации технических средств, позволяющих ознакомить с информацией определенный круг лиц, обладатель информации и информационный посредник обязаны обеспечить пользователям информации возможность свободного отказа от получения предоставляемой таким способом информации.

Если обладателем информации либо информационным посредником или владельцем информационной сети получено уведомление о нежелании конкретного пользователя информации получать распространяемую и (или) предоставляемую информацию, они обязаны принять меры по предотвращению получения такой информации пользователем информации.

При распространении и (или) предоставлении информации по почте, сетям электросвязи лица, распространяющие и (или) предоставляющие информацию обязаны соблюдать требования законодательства Республики Беларусь о почтовой связи, об электросвязи и о рекламе.

Случаи и требования обязательного распространения и (или) предоставления информации, в том числе предоставления обязательных экземпляров документов, устанавливаются законодательными актами Республики Беларусь и постановлениями Совета Министров Республики Беларусь.

Предоставление общедоступной информации может осуществляться по запросу заинтересованного государственного органа, физического или юридического лица.

Запросы о получении общедоступной информации могут быть адресованы ее обладателям в форме:

– устного запроса;

– письменного запроса.

Предоставление заинтересованному государственному органу, физическому или юридическому лицу общедоступной информации по запросу может осуществляться посредством:

– устного изложения содержания запрашиваемой информации;

– ознакомления с документами, содержащими запрашиваемую информацию;

– предоставления копии документа, содержащего запрашиваемую информацию, или выписок из него;

– предоставления письменного ответа (справки), содержащего (содержащей) запрашиваемую информацию.

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов могут осуществляться посредством ее:

– распространения в средствах массовой информации;

– размещения в государственном органе в общедоступных местах;

– размещения в информационных сетях;

– предоставления на основании запросов заинтересованных государственных органов, физических и юридических лиц;

– распространения и (или) предоставления иными способами.

Государственные органы обязаны посредством размещения в государственном органе в общедоступных местах распространять, а также могут иными способами распространять и (или) предоставлять следующую информацию:

– официальное наименование государственного органа;

– адрес места нахождения государственного органа, контактный телефон (факс);

– организационную структуру государственного органа (руководство, отделы (управления), контактные телефоны), за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– режим работы государственного органа и время приема физических лиц;

– нормативные правовые акты, регламентирующие деятельность государственного органа, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

– официальное наименование, адрес места нахождения и режим работы вышестоящего государственного органа и время приема физических лиц в этом органе.

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов осуществляются на безвозмездной основе, если иное не установлено законодательными актами Республики Беларусь.

1.7. ЗАЩИТА ИНФОРМАЦИИ

1.7.1. ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

Целями защиты информации являются:

– обеспечение национальной безопасности, суверенитета Республики Беларусь;

– сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;

– обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

– недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

1.7.2. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Защите подлежит информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.

Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством Республики Беларусь.

Информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должны обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Советом Министров Республики Беларусь.

Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.

Обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, осуществляется путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям.

Для создания системы защиты информации используются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Советом Министров Республики Беларусь.

Физические и юридические лица, занимающиеся созданием средств защиты информации и реализацией мер по защите информации, осуществляют свою деятельность в этой области на основании специальных разрешений (лицензий), выдаваемых государственными органами, уполномоченными Президентом Республики Беларусь, в соответствии с законодательством Республики Беларусь о лицензировании.

1.7.3. МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

К **правовым мерам** по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К **организационным мерам** по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К **техническим (программно-техническим) мерам** по защите информации относятся меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

1.7.4. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации организуется:

– в отношении общедоступной информации – лицом, осуществляющим распространение и (или) предоставление такой информации;

– в отношении информации, распространение и (или) предоставление которой ограничено – собственником или оператором информационной системы, содержащей такую информацию, либо обладателем информации, если такая информация не содержится в информационных системах;

– иными лицами в случаях, определенных настоящим Законом и иными законодательными актами Республики Беларусь.

1.7.5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Обладатель информации, собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей или уполномоченные ими лица вправе:

– запрещать или приостанавливать обработку информации и (или) пользование ею в случае невыполнения требований по защите информации;

– обращаться в государственные органы, определенные Президентом Республики Беларусь и (или) Советом Министров Республики Беларусь, для оценки правильности выполнения требований по защите их информации в информационных системах, проведения экспертизы достаточности мер по защите их программно-технических средств, информационных ресурсов, информационных систем и информационных сетей, а также для получения консультаций.

Владелец информационных систем и информационных сетей обязан уведомить их собственника, а также обладателя информации о всех фактах нарушения требований по защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Республики Беларусь, обязаны:

– обеспечить защиту информации, а также постоянный контроль за соблюдением требований по защите информации;

– установить порядок предоставления информации пользователю информации и определить необходимые меры по обеспечению условий доступа к информации пользователя информации;

– не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– обеспечивать возможность незамедлительного восстановления информации, модифицированной (измененной) или уничтоженной вследствие неправомерного (несанкционированного) доступа к ней.

1.7.6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь.

Последующая передача персональных данных разрешается только с согласия физического лица, к которому они относятся, либо в соответствии с законодательными актами Республики Беларусь.

Субъекты информационных отношений, получившие персональные данные в нарушение требований Закона и иных законодательных актов Республики Беларусь, не вправе пользоваться ими.

2. КЛАССИФИКАЦИЯ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Целью данного раздела является отражение позиции некоторых антивирусных компаний, в том числе и «Лаборатории Касперского» в области классификации детектируемых антивирусными продуктами объектов, что позволяет избежать расхождения в позициях при классификации. Следует отметить, что предоставленная классификация детектируемых объектов не является универсальной и общепринятой. Различные антивирусные компании придерживаются собственной разработанной экспертами данной компании классификацией. В результате чего один и тот же детектируемый объект в разных антивирусных компаниях может иметь разные имена, что приводит к некоторому недопониманию со стороны пользователей.

2.1. ДЕРЕВО КЛАССИФИКАЦИИ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Все детектируемые объекты можно отобразить в виде дерева, приведенного на рисунке 2.1.

Класс Malware делится на следующие подклассы: Viruses and Worms, Trojan programs, Suspicious packers, Malicious tools. Класс PUPs делится на: Riskware, Pornware, AdWare. Каждый подкласс делится также на поведения объектов.

Рассмотрим основные детектируемые объекты.

2.2. ОПРЕДЕЛЕНИЯ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Malware – вредоносные программы, созданные специально для уничтожения, блокирования, модификации или копирования информации или нарушения работы компьютеров и компьютерных сетей. К данному классу относятся вирусы, черви, троянские программы и иные программы, созданные для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.).

2.2.1. ВИРУСЫ И СЕТЕВЫЕ ЧЕРВИ

Viruses and Worms – вредоносные программы, которые без ведома пользователя саморазмножаются на компьютерах или в компьютерных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

К вирусам и червям не относятся вредоносные программы, которые распространяют свои копии по сети и заражают удаленные машины по команде "хозяина" (например, Backdoor'ы), или такие, которые создают в системе свои многочисленные, но не умеющие размножаться далее копии.

Основным признаком, по которому программы выделяются в отдельное поведение в данном классе, является способ их распространения, т.е. как вредоносная программа передает свою копию по локальным или сетевым ресурсам.

К данному подклассу вредоносных программ относятся следующие поведения: NetWorm, Email-Worm, IM-Worm, IRC-Worm, P2P-Worm, Worm, Virus.

Большинство известных червей распространяется в виде файлов: во вложении в электронное письмо, при переходе по ссылке на каком-либо WEB- или FTP-ресурсе или по ссылке, присланной в ICQ- или IRC-сообщениях, а также через системы файлового обмена P2P и т. п.

Некоторые черви распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код. Для проникновения на удаленные компьютеры и запуска своей копии черви используют следующие методы:

– социальный инжиниринг (например, в электронном письме предлагается открыть вложенный файл);

– недочеты в конфигурации сети (например, копирование на диск, открытый для полного доступа);

– ошибки в службах безопасности операционных систем и приложений.

Часто такой червь ищет в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения таких компьютеров червь посылает специально сформированный сетевой пакет (эксплойт). В результате этого код (или часть кода) червя проникает на компьютер-жертву и активируется. Иногда сетевой пакет содержит только ту часть кода червя, которая загружает файл с основным функционалом и запускает его на исполнение. Встречаются и сетевые черви, которые используют сразу несколько эксплоитов для своего распространения, что увеличивает скорость нахождения жертвы.

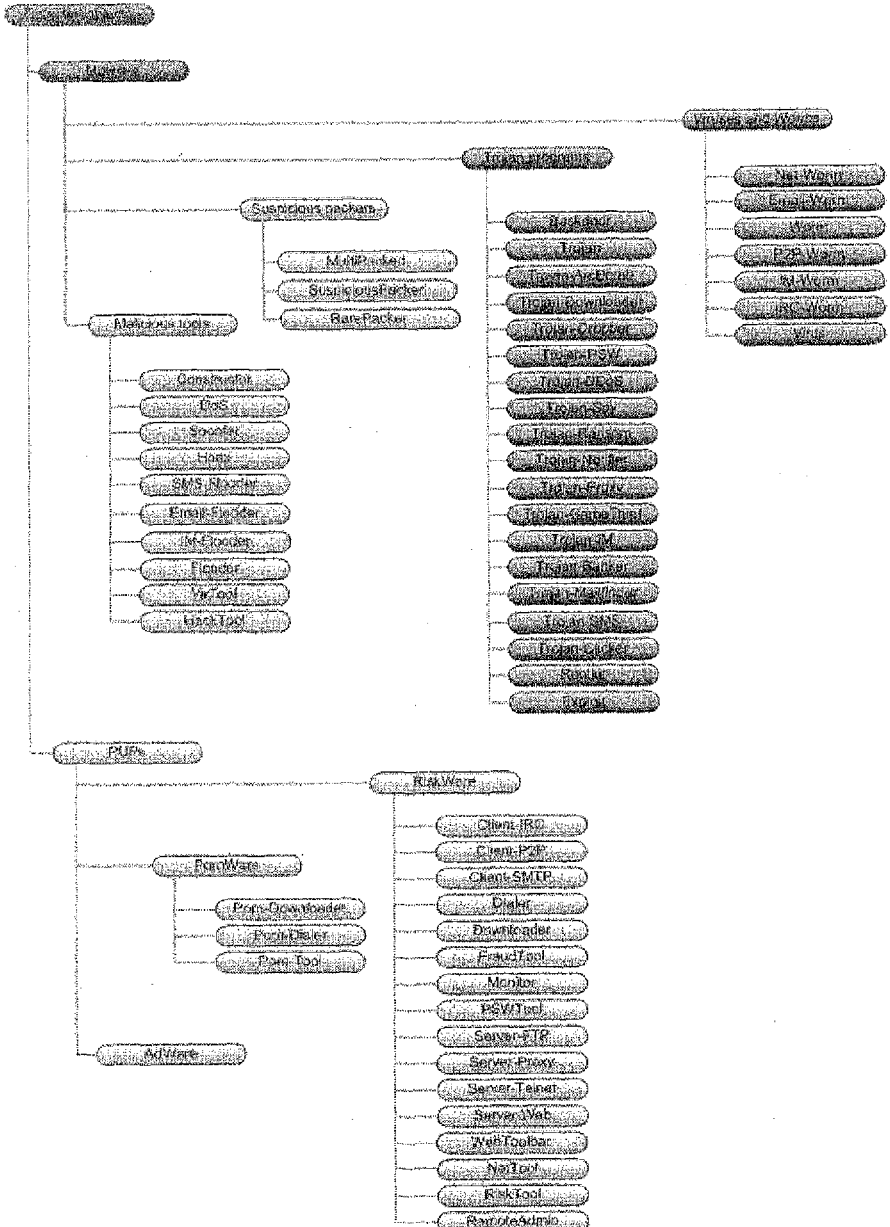

Рисунок 2.1 – Дерево детектируемых объектов

NetWorm – сетевые черви, размножаются в компьютерных сетях. Отличительной особенностью данного типа червей является то, что им не нужен пользователь в качестве звена в цепочке распространения (непосредственно для активации).

Email-Worm - размножаются по каналам электронной почты. При этом червь отсылает свою копию в виде вложения в электронное письмо или ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, ссылку (URL) на зараженный файл, расположенный на взломанном или хакерском веб-сайте). В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором – при открытии ссылки на зараженный файл. В обоих случаях результат одинаков – активизируется код червя. Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены следующие:

– прямое подключение к SMTP-серверу, с использованием встроенной в код червя почтовой библиотеки;

– использование сервисов MS Outlook;

– использование функций Windows MAPI.

Почтовые черви используют различные источники для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Например:

– адресная книга MS Outlook;

– адресная база WAB;

– файлы текстового формата на жестком диске: выделяют в них строки, являющиеся адресами электронной почты;

– письма, которые находятся в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие почтовые черви используют сразу несколько из перечисленных источников. Бывают и другие источники адресов электронной почты, например, адресные книги почтовых сервисов с web-интерфейсом.

IM-Worm – размножаются по каналам систем мгновенного обмена сообщениями (например, ICQ, MSNMessenger, AOLInstantMessenger, YahooPager, Skype и др.). Для этих целей черви, как правило, рассылают по списку контактов сообщения, содержащие ссылку (URL) на файл с телом червя, расположенного на каком-либо сетевом ресурсе. Этот прием практически полностью повторяет аналогичный способ рассылки, используемый почтовыми червями.

IRC-Worm – размножаются через Internet Relay Chats. У данного типа червей, как и у почтовых червей, существуют два способа распространения по IRC-каналам. Первый заключается в отсылке URL на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю IRC-канала. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

P2P-Worm – размножаются по каналам файлообменных пиринговых сетей (например, Kazaa, Grokster, EDonkey, FastTrack, Gnutella и др.). Механизм работы большинства подобных червей достаточно прост: для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя: при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера. Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно – при этом червь предлагает для скачивания свою копию.

Worm – размножается в компьютерных сетях через сетевые ресурсы. В отличие от NetWorm, чтобы Worm активировался, пользователь должен запустить его. Черви этого типа ищут в сети удаленные компьютеры и копируют себя в каталоги, открытые на чтение и запись (если такие обнаружены). При этом такие черви или перебирают доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищут компьютеры в интернете, подключаются к ним и пытаются открыть их диски для полного доступа. Также к данному типу червей относятся черви, которые по тем или иным причинам нельзя отнести ни к одному из вышеописанных поведений (например, мобильные черви).

Virus – что касается вирусов, то их можно разделить по способу заражения компьютера на:

– файловые, заражают файлы;

– загрузочные, заражают загрузочные сектора жестких дисков и других носителей информации;

– макровирусы, написаны на внутреннем языке, так называемых макросах какого-либо приложения;

– скриптовые, написанные в виде скриптов для определенной командной оболочки - например, bat-файлы для DOS или VBS и JS - скрипты для Windows Scripting Host (WSH).

Размножается по локальным ресурсам компьютера. В отличие от червей, вирусы не используют сетевых сервисов для своего распространения и проникновения на другие компьютеры. Копия вируса попадает на удаленные компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

– при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;

– вирус скопировал себя на съемный носитель или заразил файлы на нем;

– пользователь отослал электронное письмо с зараженным вложением.

2.2.2. ТРОЯНСКИЕ ПРОГРАММЫ

Trojan programs – вредоносные программы, которые осуществляют несанкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители этого подкласса не умеют создавать свои копии, не способны к самовоспроизведению.

Основным признаком, который служит для дифференцирования троянских программ, является вид действия, которое они выполняют на зараженном компьютере. Внутри этого подкласса выделяют следующие поведения: Backdoor, TrojanRansom, TrojanArcBomb, TrojanClicker, TrojanDDoS, TrojanDownloader, TrojanDropper, TrojanIM, TrojanNotifier, TrojanProxy, TrojanSMS, TrojanSpy, TrojanMailfinder, TrojanGameThief, TrojanPSW, TrojanBanker, Trojan, Rootkit, Exploit.

Backdoor – предназначены для удаленного управления злоумышленником пораженным компьютером. По своим функциям Backdoor во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Подобные вредоносные программы позволяют делать с компьютером все, что в них заложит автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. Представители этого типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые бот-сети/зомби-сети, что позволяет злоумышленникам централизованно

управлять всей армией пораженных компьютеров для совершения злонамеренных действий. Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

TrojanRansom – модифицирует данные на компьютере-жертве, с тем чтобы пользователь не мог ими воспользоваться, или блокирует работу компьютера. После того, как данные «взяты в заложники» (блокированы или зашифрованы), у пользователя требуют выкуп за их расшифровку. Деньги жертва должна передать злоумышленнику, после чего тот обещает выслать программу для восстановления данных или нормальной работы компьютера.

TrojanArcBomb – архивы, сформированные таким образом, чтобы при попытке архиваторов разархивировать данные спровоцировать зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации – «архивная бомба» может просто остановить работу сервера. Встречаются три типа подобных «бомб»:

– некорректный заголовок архива;

– повторяющиеся данные;

– одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива. Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5ГБ данных упаковываются в 200КБ RAR или в 480КБ ZIP-архив). Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10100 одинаковых файлов в 30КБ RAR или 230КБ ZIP-архив).

TrojanClicker – предназначены для обращения к Интернет-ресурсам (обычно к веб-страницам). Достигается это либо передачей соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса Интернет-ресурсов (например, файл hosts в MSWindows). У злоумышленника могут быть следующие цели для таких действий:

– увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;

– организация DoS-атаки (Denial of Service) на какой-либо сервер;

– привлечение потенциальных жертв для заражения вирусами или троянскими программами.

TrojanDDoS – предназначены для проведения с пораженного компьютера DoS-атаки (Denial of Service attack) по заранее определенному адресу. Суть атаки сводится к отправке на компьютер-жертву многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого удаленного компьютера недостаточны для обработки всех поступающих запросов. Часто для проведения успешной DDoS-атаки злоумышленники предварительно заражают «троянцами» этого типа множество компьютеров (например, в ходе массированной спам-рассылки), после чего каждый из зараженных компьютеров атакует заданную жертву.

TrojanDownloader – предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки троянцев или рекламных систем. Загруженные из интернета программы затем либо запускаются на выполнение, либо включаются в список программ, запускаемых при старте операционной системы. Информация об именах и располо-

жении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с управляющего Интернет-ресурса (обычно с веб-страницы). Данный тип вредоносных программ в последнее время стал часто использоваться для первоначального заражения посетителей зараженных web-страниц, содержащих эксплойты.

TrojanDropper – предназначены для скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в их теле. Эти вредоносные программы обычно без каких-либо сообщений (или с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.) сохраняют на диск жертвы (часто в каталог windows, системный каталог windows, временный каталог и т.д.) другие файлы и запускают их на выполнение. Программы этого поведения хакеры используют для:

– скрытой инсталляции троянских программ и/или вирусов;

–защиты от детектирования известных вредоносных программ антивирусами, поскольку не все они в состоянии проверить все компоненты внутри подобных «троянцев».

TrojanNotifier – предназначены для передачи своему «хозяину» сообщения о том, что зараженный компьютер сейчас находится «на связи». При этом на адрес злоумышленника отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к web-странице злоумышленника, ICQ-сообщением. Такие троянские программы используются в многокомпонентных троянских наборах для извещения злоумышленника об успешной инсталляции вредоносных программ в атакуемой системе.

TrojanProxy – предназначены для осуществления злоумышленником доступа к различным Интернет-ресурсам через компьютер-жертву. Такие вредоносные программы обычно используется для рассылки спама.

TrojanSMS – предназначены для отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые жестко записаны в теле вредоносной программы.

TrojanSpy – предназначены для ведения электронного шпионажа за пользователем (вводимые с клавиатуры данные, изображения экрана, список активных приложений и т.д.). Найденная информация передается злоумышленнику. Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы.

TrojanMailfinder – предназначены для сбора адресов электронной почты на компьюте с последующей передачей их злоумышленнику через по электронной почте, через web, ftp *или другими способами. Украденные адреса используются злоумышленниками при проведении* последующих рассылок вредоносных программ и спама.

TrojanPSW - предназначены для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров.PSW – аббревиатура от Password Stealing Ware («ПО для кражи паролей»). При запуске PSW-троянцы ищут необходимую информацию в системных файлах, хранящих различную конфиденциальную информацию, или реестре. В случае успешного поиска программа отсылает найденные данные «хозяину». Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы. Некоторые троянцы данного типа воруют регистрационную информацию к различному программному обеспечению.

Программы, занимающиеся кражей учетных записей пользователей систем интернет-банкинга, интернет-пейджинга и онлайн-игр, в силу их многочисленности, выделены в отдельные поведения: TrojanBanker, TrojanIM и TrojanGameThief соответственно.

TrojanBanker – предназначены для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт. Найденная информация передается злоумышленнику. Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы.

TrojanGameThief – предназначены для кражи пользовательской информации, относящейся к сетевым играм. Найденная информация передается злоумышленнику. Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы.

TrojanIM – предназначены для кражи учетных записей пользователей (логин и пароль) интернет-пейджеров (например, ICQ, MSNMessenger, AOLInstantMessenger, YahooPager, Skype и др.). Найденная информация передается злоумышленнику. Для передачи данных могут быть использованы электронная почта, ftp, web (посредством указания данных в запросе) и другие способы.

Rootkit – предназначены для сокрытия в системе определенных объектов либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, папки, процессы в памяти зараженного компьютера, вредоносная сетевая активность. Сам по себе rootkit ничего вредоносного не делает, но данный тип программ в подавляющем большинстве случаев используется для того, чтобы препятствовать обнаружению вредоносных программ и продлить время их действия на пораженном компьютере.

Exploit – программы, в которых содержатся данные или исполняемый код и которые используют одну или несколько уязвимостей в программном обеспечении на локальном или удаленном компьютере с заведомо вредоносной целью. Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, для заражения всех посетителей взломанного web-сайта вредоносной программой). Помимо этого, эксплойты интенсивно используются Net-Worm'ами для проникновения на компьютер-жертву без помощи пользователя. Среди эксплоитов выделяются программы-Nuker'ы, которые отправляют на локальный или удаленный компьютер специальным образом сформированные запросы, в результате чего система прекращает свою работу.

Trojan – вредоносная программа, занимающаяся уничтожением, блокированием, модификацией или копированием информации, нарушением работы компьютеров или компьютерных сетей, и при этом не попавшая ни в одно из вышеприведенных троянских поведений. Также к Trojan относятся «многоцелевые» троянские программы, т.е. те, которые в состоянии совершать сразу несколько действий, присущих одновременно нескольким поведениям троянских программ, что не позволяет ОДНОЗНАЧНО отнести их к тому или иному поведению.

2.2.3. ПОДОЗРИТЕЛЬНЫЕ УПАКОВЩИКИ

Вредоносные программы часто сжимаются различными способами упаковки, совмещенными с шифрованием содержимого файла для того, чтобы исключить обратную разработку программы и усложнить анализ поведения проактивными и эвристическими методами. Антивирусом детектируются результаты работы подозрительных упаковщиков – упакованные объекты. Существуют приемы борьбы с распаковкой: например, упаковщик может расшифровывать код не полностью, а лишь по мере исполнения, или, расшифровывать и запускать

вредоносный объект целиком только в определенный день недели. Основными признаками, по которым дифференцируют поведения объектов подкласса Suspicious packers, являются вид и количество упаковщиков, использованных при сжатии файла. К данному подклассу вредоносных программ относятся следующие поведения: MultiPacked, SuspiciousPacker, RarePacker.

MultiPacked – многократно упакованные различными программами упаковки файловые объекты. Антивирусный продукт выдает рассматриваемый вердикт при обнаружении исполняемых файлов, упакованных одновременно тремя и более упаковщиками.

SuspiciousPacker – файловые объекты, сжатые упаковщиками, созданными специально для защиты вредоносного кода от детектирования антивирусными продуктами.

RarePacker – файловые объекты, сжатые различными редко встречающимися упаковщиками, например, реализовывающими какую-либо концептуальную идею.

2.2.4. ХАКЕРСКИЕ УТИЛИТЫ

Вредоносные программы, разработанные для автоматизированного создания вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. В отличие от вирусов, червей и троянских программ, представители данного подкласса не представляют опасности непосредственно для компьютера, на котором исполняются, все вредоносные действия программа совершает по прямому указанию пользователя. Основным признаком, по которому различают Malicious tools, являются совершаемые ими действия. К данному подклассу вредоносных программ относятся следующие поведения: Constructor, DoS, Email-Flooder, IM-Flooder, SMS-Flooder, Flooder, Spoofer, VirTool, Hoax, HackTool.

Constructor – предназначены для изготовления новых компьютерных вирусов, червей и троянских программ. Известны конструкторы вредоносных программ для DOS, Windows и макроплатформ. Эти программы генерируют исходные тексты вредоносных программ, объектные модули, и/или непосредственно вредоносные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вредоносной программы, наличие или отсутствие самошифровки, противодействие отладчику и т. п.

DoS – предназначены для проведения DoS-атаки (Denial of Service attack) на компьютер-жертву. Суть атаки сводится к отправке на удаленный компьютер многочисленных запросов, и если ресурсы этого компьютера недостаточны для обработки всех поступающих запросов, это приводит к отказу в обслуживании.

Email-Flooder – переполняют бесполезными сообщениями каналы электронной почты. Могут использоваться спамерами.

IM-Flooder – переполняют бесполезными сообщениями каналы интернет-пейджеров (например, ICQ, MSNMessenger, AOLInstantMessenger, YahooPager, Skype и др.). Могут использоваться спамерами.

SMS-Flooder – переполняют бесполезными сообщениями каналы передачи SMS-сообщений. Могут использоваться спамерами.

Flooder – переполняют бесполезными сообщениями сетевые каналы, отличные от почтовых, интернет-пейджеров и SMS (например, IRC). Могут использоваться спамерами.

Spoofer – подменяют адрес отправителя в сообщений или в сетевых запросах Эти программы могут быть использованы с различными целями (например, не дать получателю обнаружить настоящего отправителя или выдать сообщение за сообщение, отправленное другим лицом).

VirTool – модифицируют другие вредоносные программы таким образом, чтобы они не детектировались антивирусным ПО.

Hoax – не причиняют компьютеру прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен, либо предупреждают пользователя об опасности, которой на самом деле не существует. К «злым шуткам» относятся, например, программы, которые пугают пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят сообщения, характерные для вирусов, и т. д. — в зависимости от «чувства юмора» автора такой программы.

HackTool – вносит в список разрешенных посетителей системы новых пользователей; чистит системные журналы для сокрытия следов присутствия злоумышленника в системе, анализирует и собирает сетевые пакеты для совершения злонамеренных действий и т.д. Используется злоумышленниками при организации атак на локальный или удаленный компьютер.

2.2.5. ПОТЕНЦИАЛЬНО НЕЖЕЛАТЕЛЬНЫЕ ПРОГРАММЫ

Потенциально нежелательные программы (PUPs, Potentially Unwanted Programs) - это программы, которые разрабатываются и распространяются легальными компаниями, могут использоваться в повседневной работе, например, в работе системных администраторов. Однако некоторые программы обладают набором функций, которые при определенных условиях могут причинить вред пользователю. Например, если программа удаленного администрирования установлена на компьютер пользователя системным администратором, то это обычная практика, и администратор получает всего лишь возможность решать возникающие на удаленном компьютере проблемы. Но если такая же программа нелегально установлена на компьютер пользователя злоумышленником, то он в состоянии получить полный контроль над удаленным компьютером и использовать его по своему усмотрению. Антивирусная программа в целом ряде случаев не может без помощи пользователя определить, опасна или нет та или иная программа. Если обнаруженные программы данного класса знакомы пользователю, и он на 100% уверен в том, что они не причинят вреда его данным (например, он сам купил эти программы, ему известны их функции), то он может либо совсем отказаться от дальнейшего их детектирования, либо добавить подобные программы в список «исключений» — после этого антивирус не будет реагировать на их действия. Если же пользователь по какой-либо причине заподозрил обнаруженную антивирусными базами программу во вредоносных действиях (например, он не устанавливал эту программу на свой компьютер и не знает, откуда она появилась, или начал сомневаться в том, что программа безопасна, ознакомившись с ее описанием на нашем сайте), то антивирус поможет пользователю избавиться от этой программы. В любом случае, пользователь принимает самостоятельное решение. В настоящее время к условно нежелательным программам (PUPs) относят программы подклассов Adware, Pornware и Riskware.

Adware – рекламное программное обеспечение, предназначенное для показа рекламных сообщений (чаще всего в виде графических баннеров), перенаправления поисковых запросов на рекламные web-страницы, а также для сбора данных маркетингового характера о пользователе (например, какие тематические сайты он посещает), что позволяет более четко задать аудиторию для рекламной кампании. За исключением показа рекламы или сбора данных, подобные программы, как правило, никак не проявляют своего присутствия в системе: отсутствует значок в системном трее, нет упоминаний об установленных файлах в меню программ. Часто у Adware-программ нет процедуры де-

инсталляции, используются пограничные с вирусными технологии, позволяющие программам скрытно внедряться на компьютер пользователя и работать на нем.

На компьютеры пользователей Adware чаще всего попадает двумя способами:

– путем встраивания в бесплатное и условно-бесплатное программное обеспечение (freeware, shareware);

–путем несанкционированной пользователем установки на его компьютер при посещении им зараженных web-страниц.

Большинство программ freeware и shareware прекращает показ рекламы после их покупки и/или регистрации. Но такие программы часто используют встроенные Adware-утилиты сторонних производителей, и в некоторых случаях эти Adware-утилиты остаются установленными на компьютере пользователя и после регистрации программ, с которыми они попали в операционную систему. При этом удаление Adware-компонента, все еще используемого какой-либо программой для показа рекламы, может привести к сбоям в функционировании этой программы. Базовое назначение Adware, распространяемых первым способом, первого – неявная форма оплаты программного обеспечения, осуществляемая за счет показа пользователю рекламной информации (рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство – разработчику Adware). Adware помогает сократить расходы и разработчикам программного обеспечения (доход от Adware стимулирует их к написанию новых и совершенствованию существующих программ), и самим пользователям. В случае установки рекламных компонентов при посещении пользователем зараженных веб-страниц часто используются хакерские технологии: проникновение в компьютер через уязвимости в системе безопасности Интернет-браузера, а также использование троянских программ, предназначенных для скрытой установки программного обеспечения (TrojanDownloader или TrojanDropper). Adware-программы, действующие подобным образом, часто называют BrowserHijackers.

Известны два основных способа доставки рекламной информации:

– загрузка на компьютер рекламных текстов и изображений с веб- или FTP-серверов, принадлежащих рекламодателю;

– перенаправление поисковых запросов интернет-браузера на рекламный web-сайт.

Перенаправление запросов в некоторых случаях происходит только при отсутствии запрашиваемой пользователем web-страницы, т.е. при ошибке в наборе адреса страницы.

Многие рекламные системы помимо доставки рекламы также собирают информацию о компьютере и пользователе:

– IP-адрес компьютера;

– версию установленной операционной системы и Интернет-браузера;

– список часто посещаемых пользователем Интернет-ресурсов;

– поисковые запросы;

– прочие данные, которые можно использовать при проведении последующих рекламных кампаний.

Не стоит путать Adware, занимающиеся сбором информации, с троянскими шпионскими программами. Отличие Adware состоит в том, что они осуществляют его с согласия пользователя. Если Adware никак не уведомляет пользователя об осуществляемом сборе информации, то она однозначно попадает под поведение TrojanSpy и относится к категории вредоносных программ (Malware).

Pornware – программы, которые связаны с показом пользователю материалов порнографического характера. К этому подклассу относятся Porn-Dialer, Porn-Downloader и Porn-Tool.

Porn-Dialer – дозваниваются до порнографических телефонных служб, номер телефона и/или специальный код которых сохранены в теле этих программ. Отличие от вредоносных программ дозвона состоит в том, что пользователь уведомляется программой о совершаемых ею действиях.

Porn-Downloader – загружают из Сети на компьютер пользователя медиафайлы порнографического содержания. Отличие от вредоносных скрытых программ дозвона состоит в том, что пользователь уведомляется программой о совершаемых ею действиях.

Porn-Tool – занимаются поиском и показом порнографических материалов (например, специальные панели инструментов для интернет-браузера и особые видеоплееры).

Программы подкласса Pornware могут быть установлены пользователем на свой компьютер сознательно, с целью поиска и получения материалов порнографического характера. В этом случае они не являются нежелательными. С другой стороны, те же самые программы могут быть установлены на пользовательский компьютер злоумышленниками: с использованием уязвимостей операционной системы и Интернет-браузера или при помощи вредоносных троянских программ TrojanDownloader или TrojanDropper. Делается это обычно с целью «принудительной» рекламы платных порнографических сайтов и сервисов, которые не привлекли бы внимание обычного пользователя.

Riskware – это легальные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые в руках злоумышленника способны причинить вред пользователю (вызвать уничтожение, блокирование, модификацию или копирование данных, нарушить работу компьютеров или компьютерных сетей). В списке программ подкласса Riskware можно обнаружить утилиты удаленного администрирования, программы-клиенты IRC, Dialers, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, а также многочисленные интернет-серверы служб FTP, Web, Proxy и Telnet. Все эти программы не являются вредоносными сами по себе, однако обладают функционалом, который злоумышленники могут использовать в неблаговидных целях.

К этому подклассу относятся Client-IRC, Client-P2P, Client-SMTP, Dialer, Downloader, FraudTool, Monitor, PSWTool, Server-Telnet, Server-FTP, Server-Proxy, Server-Web, NetTool, RiskTool, RemoteAdmin и WebToolbar.

Client-IRC – используются для общения в Internet Relay Chats. Вредоносными не являются. Детектируются по причине частого использования злоумышленниками расширенного функционала этих программ - вредоносные программы устанавливают Client-IRC на пользовательские компьютеры со злонамеренными целями. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Client-P2P – используются для работы в peer-to-peer сетях. Вредоносными не являются. Детектирование добавлено по настоянию пользователей, т.к. ряд программ подобного рода стал причиной утечки конфиденциальной информации. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Client-SMTP – используются для отправки электронной почты и имеют скрытый режим работы. Вредоносными не являются. Такие программы могут включаться злоумышленниками в состав пакета вредоносных программ с целью использования для рассылки спама с компьютеров пользователей. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Dialer – устанавливают в скрытом режиме телефонные соединения через модем. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Downloader – осуществляют в скрытом режиме загрузку различного контента с сетевых ресурсов. Вредоносными не являются. Такие программы могут использоваться злоумышленниками для загрузки вредоносного контента на компьютер-жертву. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

FraudTool – выдают себя за другие программы, хотя таковыми не являются. Часто предлагают пользователю перечислить финансовые средства на указанный счет для оплаты «услуг». Примером таких программ могут служить псевдоантивирусы, которые выводят сообщения об «обнаружении» вредоносных программ, но на самом деле ничего не находят и не лечат.

Monitor – содержат функции наблюдения за активностью на компьютере пользователя (активные процессы, сетевая активность и т.д.). Вредоносными не являются. В этих же целях могут быть использованы злоумышленниками. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

PSWTool – позволяют просматривать или восстанавливать забытые (часто скрытые) пароли. С таким же успехом в подобных целях данный тип программ может быть использован злоумышленниками. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Server-Telnet – содержат функции telnet-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Server-FTP – содержат функции FTP-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Server-Proxy – содержат функции proxy-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например для рассылки спама или иного вредоносного контента от имени компьютера-жертвы. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

Server-Web – содержат функции web-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

NetTool – обладают функциями для работы с сетью (например, удаленная перезагрузка компьютера, сканирование открытых сетевых портов, удаленный запуск произвольных приложений и т.д.), которые позволяют киберпреступникам использовать их со злонамеренной целью. Вредоносными не являются.

Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

RiskTool – обладают различными функциями (например, сокрытие файлов в системе, сокрытие окон запущенных приложений, уничтожение активных процессов и т.д.), позволяющей использование их киберпреступниками со злонамеренными целями. Вредоносными не являются. В отличие от NetTool эти программы предназначены для локальной работы. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

RemoteAdmin – используются для удаленного управления компьютером. Вредоносными не являются. Будучи установленными злоумышленником, дают ему возможность полного контроля компьютером-жертвой. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

WebToolbar – с разрешения пользователя устанавливают панели инструментов, позволяющие использовать одну или несколько поисковых систем при работе в интернете, расширяя таким образом возможности пользовательского программного обеспечения. Вредоносными не являются. Детектируются по причине их распространения с помощью вредоносных программ в виде вложенных файлов, т.е. инсталляция WebToolbar'ов на компьютер пользователя производится вредоносными программами. Если такая программа установлена на вашем компьютере вами или вашим сетевым администратором, никакой опасности она не представляет.

2.3. ПРАВИЛА ПОГЛОЩЕНИЯ РАЗЛИЧНЫХ ТИПОВ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Правила поглощения относятся только к вредоносным программам (Malware), детектируемым сигнатурным анализатором. Они не затрагивают потенциально-нежелательные программы (PUPs), а также вердикты проактивной защиты (префикс PDM:) и эвристики (префикс HEUR:).

Согласно классификации каждый детектируемый объект имеет четкое описание и однозначное расположение в дереве классификации. В реальной же жизни часто встречаются вредоносные программы, которые обладают целым набором вредоносных функций и способов распространения. Возьмем для примера некую вредоносную программу, распространяемую по электронной почте в виде вложений и через P2P-сети в виде файлов. В дополнение к этому она содержит функцию несанкционированного пользователем сбора адресов электронной почты с пораженных компьютеров. Таким образом, вредоносная программа (согласно классификации) может быть с равным успехом отнесена к Email-Worm, к P2P-Worm и к TrojanMailfinder. В конечном итоге различные модификации одной и той же вредоносной программы могут получить различные названия в зависимости от того, какому поведению отдает предпочтение антивирусный эксперт, анализировавший код – и результат не вызовет ничего кроме путаницы. Во избежание подобных проблем используется так называемые правила поглощения, которые позволяют однозначно отнести вредоносную программу к тому или иному поведению вне зависимости от реализованной в ней функциональности.

Как работают правила поглощения? Каждому поведению присваивается определенный уровень опасности, и менее опасные поведения поглощаются более опасными. Например, в приведенном примере самым опасным является поведение Email-Worm, и рассматриваемая вредоносная программа должна быть отнесена именно к этому типу. Правила поглощения для всех имеющихся типов вредоносных программ могут быть представлены в виде дерева, приведенном на рисунке 2.2.

Наименее опасные поведения расположены внизу рисунка, наиболее опасные - вверху. В том случае, если программу можно отнести к нескольким поведениям, ее следует отнести к наиболее опасному. В том случае, если вредоносную программу можно отнести к нескольким равнозначным поведениям (например, TrojanDownloader и TrojanDropper), то для такой программы выбирается вышестоящее (объединяющее) поведение.

Правило объединения равнозначных поведений под именем вышестоящего действует только для троянских программ, вирусов и червей. И не действует для Malicioustools.

Если вредоносная программа содержит два или более функционала с равнозначным уровнем опасности, которые могут быть отнесены к TrojanRansom, TrojanArcBomb, TrojanClicker, TrojanDDoS, TrojanDownloader, TrojanDropper, TrojanIM, TrojanNotifier, TrojanProxy, TrojanSMS, TrojanSpy, TrojanMailfinder, TrojanGameThief, TrojanPSW или TrojanBanker, то такая вредоносная программа относится к типу Trojan. Если вредоносная программа содержит два или более функционала с равнозначным уровнем опасности, которые могут быть отнесены к IM-Worm, P2P-Worm или IRC-Worm, то такая вредоносная программа относится к типу Worm.

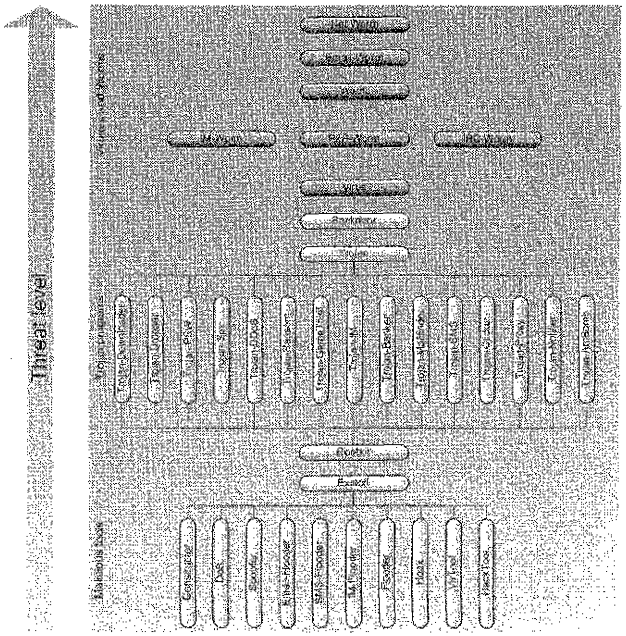

Рисунок 2.2 – Правила поглощения различных типов вредоносных программ

2.4. ПРАВИЛА ИМЕНОВАНИЯ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Вердикт – это полное имя вредоносной программы. Для всех детектируемых антивирусными продуктами объектов используется следующая система именования:

[Prefix:]Behaviour.Platform.Name[.Variant]

Prefix определят подсистему, задетектировавшую объект. Для вердиктов эвристического анализатора используется префикс «HEUR:», для вердиктов модуля проактивной защиты - «PDM:».

Prefix не является обязательным в вердикте и может отсутствовать.

Behaviour определяет поведение детектируемого объекта. Для вирусов и червей поведение определяется по способу распространения, для троянских программ и Malicioustools – по совершаемым ими действиям. Для Suspiciou spackers – по поведению распаковщика, а для PUPs - по функциональному назначению детектируемого объекта. Поведение детектируемого объекта может быть одним из следующих: NetWorm, Email-Worm, IM-Worm, IRC-Worm, P2P-Worm, Worm, Virus, Backdoor, TrojanRansom, TrojanArc-Bomb, TrojanClicker, TrojanDDoS, TrojanDownloader, TrojanDropper, TrojanIM, TrojanNotifier, TrojanProxy, TrojanSMS, TrojanSpy, TrojanMailfinder, TrojanGameThief, TrojanPSW, TrojanBanker, Trojan, Rootkit, MultiPacked, SuspiciousPacker, RarePacker, Constructor, DoS, Exploit, Email-Flooder, IM-Flooder, SMS-Flooder, Flooder, Spoofer, VirTool, Hoax, HackTool, Adware, Porn-Dialer, Porn-Downloader, Porn-Tool, Client-IRC, Client-P2P, Client-SMTP, Dialer, Downloader, FraudTool, Monitor, PSWTool, Server-Telnet, Server-FTP, Server-Proxy, Server-Web, NetTool, RiskTool, RemoteAdmin и WebToolbar.

Platform - среда, в которой выполняется вредоносный или потенциально-нежелательный программный код. Может быть как программной, так и аппаратной. Для мультиплатформенных детектируемых объектов используется платформа обозначается как Multi. В качестве примера мультиплатформенной вредоносной программы можно привести Virus.Multi.Etapux, который заражает исполняемые файлы на операционных системах Windows и Linux. Для эвристичского анализатора на момент написания данной версии документа существует две платформы: «Win32» и «Script» (обобщенная платформа для различных видов скриптов), для PDM - одна платформа - «Win32».

Name – имя детектируемого объекта, позволяет выделять семейства детектируемых объектов. Под семейством подразумевается детектируемые объекты, имеющие общее происхождение (авторство, исходные коды), принцип работы или направление выполняемых действий. Например, вредоносные программы семейства Trojan.Win32.StartPage изменяют стартовые страницы браузеров.

Variant – модификация детектируемого объекта. Может содержать как цифровое обозначение версии программы, так и буквенное обозначение, начиная с 'a': 'a' 'z', 'aa' 'zz', ... Variant не является обязательным в вердикте и может отсутствовать.

Пример именования детектируемых объектов представлен на рисунке 2.3.

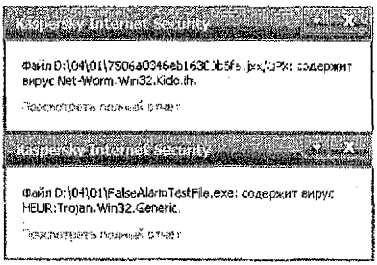

Рисунок 2.3 – Пример именования детектируемых объектов

2.5. АЛЬТЕРНАТИВНЫЙ ПОДХОД К КЛАССИФИКАЦИИ ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ

Для выделения тенденций развития вредоносных программ используется также альтернативная классификация. Новые угрозы появляются вновь и вновь; быстро развиваются наиболее удачные мошеннические схемы. По этой причине часто возникает необходимость выделить из всего многообразия детектируемых объектов то или иное подмножество, характеризующее наиболее яркие и опасные тенденции развития вредоносных программ. В изложенном выше подходе к классификации черви и вирусы определяются по способу распространения, остальные вредоносные программы - по совершаемым ими действиям. Но часто аналитикам, чтобы выделить ту или иную тенденцию развития вредоносных программ, этих признаков бывает недостаточно. По этой причине используются другие признаки для классификации объектов, позволяющие выделить необходимые поведения из многообразия детектируемых объектов и объединить их в категории. Для обозначения наиболее ярких, устоявшихся и опасных трендов последнего времени используются следующие категории:

Crimeware;
Spyware;
Ransomware;
Bot-clients.

Поясним, что входит в каждую из этих категорий.

Crimeware – категория вредоносных программ, разработанных специально для совершения финансовых преступлений. Злоумышленниками написаны сотни различных программ подобного рода. Это могут быть программы, отслеживающие появление на экране окна подключения к банковской системе с целью перехвата вводимых в этом окне конфиденциальных данных, или программы, копирующие содержимое буфера обмена в момент подключения к системам электронного платежа. В последнем случае расчет злоумышленника весьма прост - пользователь чаще всего не вводит свой пароль вручную в окно подключения к системе, а копирует его через буфер обмена из другого места, где пароль был сохранен ранее. Фантазия злоумышленников безгранична и новые подходы получения доступа к счетам пользователей становятся все более изощренными. В качестве примеров семейств вредоносных программ категории Crimeware можно привести Trojan-Spy.Win32.Goldun, Trojan-Spy.Win32.Webmoner и многие другие. А также всех представителей TrojanBanker. Наибольшее число представителей категории Crimeware, безусловно, относится к TrojanBanker и TrojanSpy, но согласно рисунку 2.2 и правилам поглощения, функциональностью для совершения финансовых преступлений могут обладать представители вышестоящих поведений, а именно Trojan, Backdoor, Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, NetWorm, хотя и значительно реже, чем представители TrojanBanker и TrojanSpy. Crimeware является подмножеством Malware и может пересекаться с другими подмножествами/категориями вредоносных программ.

Spyware – категория вредоносных программ, применяемых для несанкционированного пользователем слежения за его действиями и/или несанкционированного им сбора данных. Это могут быть программы, записывающие все нажатые пользователем клавиши в лог-файл для последующей передачи сохраненной информации злоумышленнику, или программы, собирающие без ведома пользователя адреса электронной почты на его компьютере для последующей передачи их спамерам и т.д. В качестве примеров семейств вредоносных программ категории Spyware можно привести Trojan-Spy.Win32.Keylogger, Trojan-PSW.Win32.PdPinch и многие другие. Также к Spyware относятся другие представители TrojanSpy и TrojanPSW, а также все представители TrojanGameThief, TrojanIM, TrojanMailfinder, TrojanBanker, TrojanNotifier, TrojanBanker, несмотря на то что он относится к

Crimeware, можно отнести и к Spyware в силу того, что представители этого поведения собирают данные о пользователе. В данном случае мы имеем типичное пересечение подмножеств Crimeware и Spyware. TrojanNotifier относится к Spyware, так как позволяет скрытно сообщать своему «хозяину» о подключении компьютера-жертвы к сети. Согласно правилам поглощения, к Spyware могут относиться представители вышестоящих над упомянутыми поведений, а именно Trojan, Backdoor, Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, NetWorm.

Ransomware – категория вредоносных программ, блокирующих данные или работоспособность компьютера. Их действия не санкционированы пользователем компьютера; программа используется злоумышленниками с целью дальнейшего требования выкупа. В качестве примеров семейств, относящихся к Ransomware, можно привести Trojan-Ransom.Win32.Gpcode и Trojan-Ransom.Win32.Krotten. Gpcode занимается шифрованием файлов, выбирая в качестве мишеней наиболее ценные данные - документы, базы данных и др., после чего появляется сообщение с указанием координат, где «помогут» восстановить данные. Krotten изменяет системный реестр таким образом, чтобы на компьютере было невозможно работать. Восстановление работоспособности возможно после уплаты «выкупа». К данной категории вредоносных программ в первую очередь относятся представители поведения Trojan-Ransom, но правилам поглощения, к категории Ransomware могут относиться представители более опасных поведений, а именно Trojan, Backdoor, Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, NetWorm.

Bot-clients – категория вредоносных программ, занимающихся объединением пораженных компьютеров в бот-сети (или зомби-сети), что позволяет осуществлять удаленное централизованное управление всеми пораженными компьютерами без ведома пользователей. Например, для рассылки спама и проведения DDoS-атак. К данной категории вредоносных программ в первую очередь относятся представители поведения Backdoor, но правилам поглощения, к категории Bot-clients могут относиться представители более опасных поведений, а именно Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, NetWorm. Причем черви достаточно часто имеют в своем составе функционал, позволяющий объединять зараженные компьютеры в бот-сети.

3. МЕТОДЫ ДЕТЕКТИРОВАНИЯ ОБЪЕКТОВ

3.1. СИГНАТУРНЫЙ АНАЛИЗ

Сигнатурный анализ (dictionary-based examination) – сравнение байтовой последовательности в проверяемом объекте с имеющейся в базах сигнатурой. Характерная особенность этого способа состоит в том, что антивирус работает только с исходным байтовым кодом программы, не изучая ее поведение в системе. Антивирусные базы представляют собой файлы с записями, которые позволяют идентифицировать наличие в проверяемых объектах сотен тысяч известных вредоносных программ. Эти записи содержат информацию о контрольных участках кода вредоносных программ и алгоритмы лечения объектов, в которых эти программы содержатся.

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждой вредоносной программы и поиска ее путем сравнения файлов с выявленными чертами. Сигнатурой вредоносной программы будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вредоносного кода в файле (включая случаи, когда файл целиком является телом вредоносной программы). Все вместе сигнатуры известных детектируемых объектов составляют антивирусную базу. Пример выделения сигнатуры вредоносной программы представлен на рисунке 3.1.

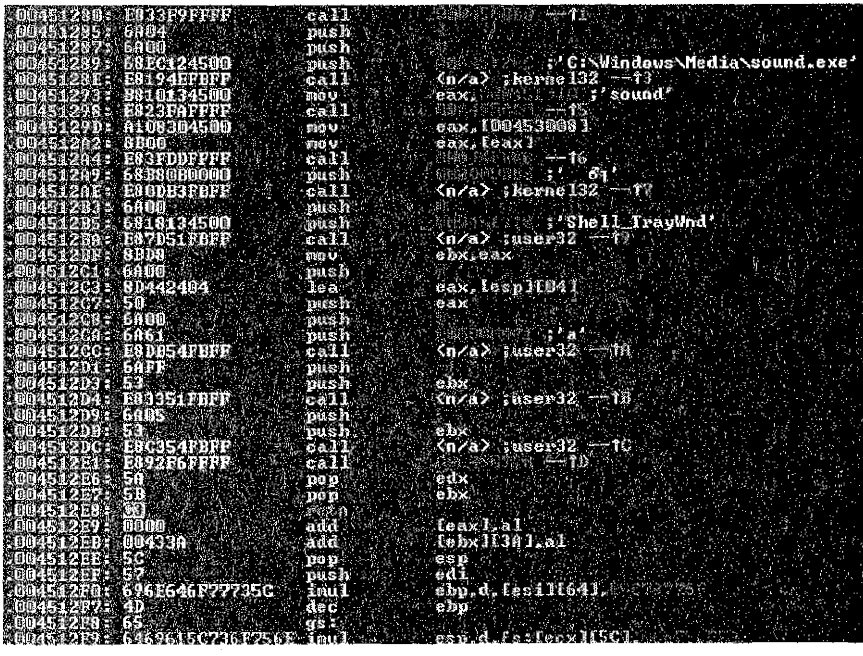

Рисунок 3.1 – Пример сигнатуры вредоносной программы

Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вредоносных объектов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются.

Одно из распространенных заблуждений насчет сигнатур заключается в том, что каждая сигнатура соответствует ровно одной вредоносной программе. И как следствие, антивирусная база с большим количеством сигнатур позволяет обнаруживать больше вредоносных объектов. На самом деле это не так. Очень часто для обнаружения семейства похожих вредоносных программ используется одна сигнатура, и поэтому считать, что количество сигнатур равно количеству обнаруживаемых объектов, уже нельзя. Соотношение количества сигнатур и количества известных вредоносных объектов для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве объектов.

Важное дополнительное свойство сигнатур - точное и гарантированное определение типа вредоносной программы. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения.

Другое важное, но уже отрицательное свойство - для получения сигнатуры необходимо иметь образец вредоносной программы. Следовательно, сигнатурный метод непригоден для защиты от новых вредоносных объектов, т. к. до тех пор, пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются новыми вредоносными программами. С момента появления вредоносного объекта в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вредонос способен заражать компьютеры почти беспрепятственно.

Недостатки и достоинства сигнатурного анализа:

позволяет определять конкретную вредоносную программу с высокой точностью и малой долей ложных срабатываний;

неспособен обнаруживать какие-либо новые, неизвестные вредоносные программы;

беззащитен перед полиморфными вредоносными программами и изменёнными версиями одной и той же вредоносной программы;

требует регулярного и крайне оперативного обновления;

требует кропотливого ручного анализа вредоносных объектов.

3.2. ВЕРОЯТНОСТНЫЙ АНАЛИЗ

Вероятностный анализ применяется для обнаружения неизвестных вредоносных программ, и, как следствие, не предполагает лечения. Данная технология не способна на 100% определить вредоносный объект перед ней или нет и характеризуется ложными срабатываниями.

Существуют несколько алгоритмов вероятностного анализа, наиболее популярные из которых:

– эвристический анализ;

– поведенческий анализ;

– анализ контрольных сумм.

Эвристический анализ (heuristic analysis) - это анализ кода проверяемого объекта с помощью эмуляции его исполнения и определение по косвенным признакам, таким как загрузка и запись файлов, обращение к системному реестру, изменение настроек файервола или антивируса, является ли объект вредоносным. По результатам эмуляции создаются так называемые эвристические сигнатуры, которые содержат в себе набор действий, характерных для тех или иных вредоносных объектов. Причем в отличие от сигнатурного метода эвристический анализ позволяет детектировать как известные, так и неизвестные вредоносные объекты, однако лечение в таких случаях практически всегда оказывается невозможным. Пример работы эмулятора представлен на рисунке 3.2. А на рисунке 3.3 изображен пример эвристической сигнатуры.

Несмотря на заявления и рекламные проспекты разработчиков антивирусных средств относительно совершенствования эвристических механизмов, эффективность эвристического сканирования на данный момент далека от ожидаемой. Независимые тесты компонентов эвристического анализа показывают, что уровень обнаружения новых вредоносных программ составляет не более чем 40-50 % от их числа.

Положительным эффектом от использования этого метода является возможность обнаружить новые вредоносные программы еще до того, как для них будут выделены сигнатуры. Отрицательные стороны весьма существенны:

– вероятность ошибочно определить наличие в проверяемом объекте вредоносный код, когда на самом деле объект чист - ложные срабатывания;

– невозможность лечения зараженных объектов;

– низкая эффективность против действительно новаторских технологий вирусописательства, вызывающих наиболее масштабные эпидемии.

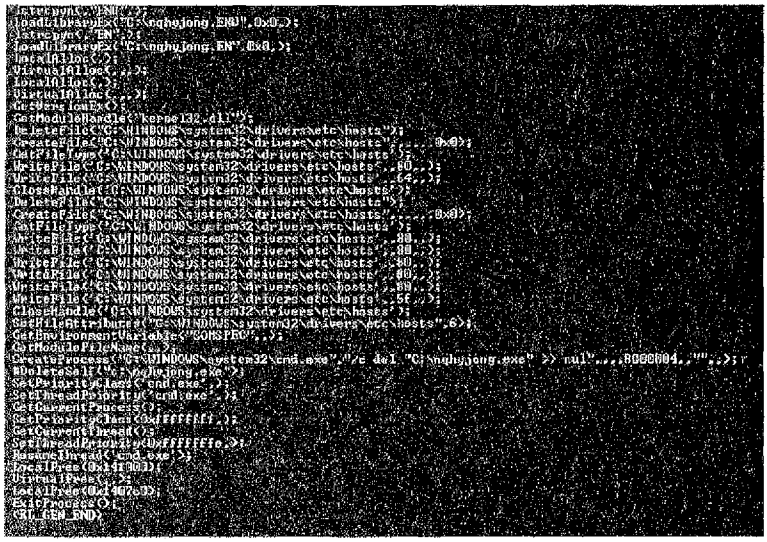

Рисунок 3.2 – Пример работы эмулятора

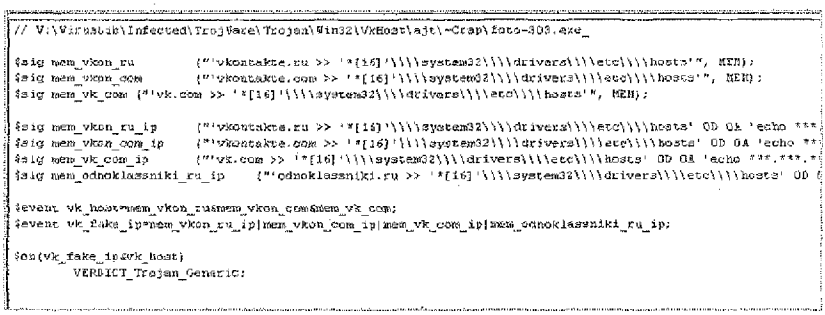

Рисунок 3.3 – Пример эвристической сигнатуры

Поведенческий анализ - технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций. Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вредоносных объектов, могут выполняться и обычными приложениями. Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вредоносные программы практически всегда выполняют ряд однотипных действий. Например, для внедрения в систему, почти каждый макровирус использует один и тот же алгоритм: в какой-нибудь стандартный макрос, автоматически запускаемый средой Microsoft

Office при выполнении стандартных команд (например, "Save", "Save As", "Open", и т.д.), записывается код, заражающий основной файл шаблонов normal.dot и каждый вновь открываемый документ.

Средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR компьютера, анализатор блокирует действие и выводит соответствующее уведомление пользователю.

Помимо этого поведенческие анализаторы могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись дискет, форматирование жестких дисков и т. д.

Поведенческие анализаторы не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вредоносные объекты - все подозрительные программы априори считаются неизвестными вредоносными программами. Средства, реализующие технологии поведенческого анализа, не предполагают лечения. Пример сигнатуры поведенческого модуля представлен на рисунке 3.4.

```
$sig url1       {'i'gethostbyname("fuckingpicshunter'', PDM);
$sig url2       {'i'gethostbyname("adserving.cpxinteractive'', PDM);
$sig inject     {'i'ZwQueueApcThread("' *[30] i'.exe'', PDM);
$sig srv1       {'i'PDMFileAccessed("?:\\documents and settings\\' *[30] i'\\local settings\\temporary internet files\\
$sig srv2       {'i'PDMFileAccessed("?:\\documents and settings\\' *[30] i'\\local settings\\temporary internet files\\'


$on {url1 & url2 & inject & {srv1 & srv2}}
        $verdict {"PDM:Trojan.Win32.Generic.Number.silent", SILENT_DETECT};
```

Рисунок 3.4 – Пример сигнатуры поведенческого модуля

Анализ контрольных сумм - это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы.

Анализаторы контрольных сумм, как и поведенческие анализаторы, не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. На сегодняшний день подобная технология применяется в сканерах при первой проверке файла. У объекта вычисляется контрольная сумма и помещается в специальный кэш. Перед следующей проверкой того же объекта контрольная сумма вычисляется еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

4. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. НЕКОТОРЫЕ ПРАВИЛА РАБОТЫ ЗА КОМПЬЮТЕРОМ

Самым простым примером организационных методов защиты от вирусов является выработка и соблюдение определенных правил обработки информации. Правила можно условно разделить на две категории:

– правила обработки информации;

– правила использования программ.

К первой группе правил могут относиться, например, такие как:
– не открывать вложения в почтовых сообщениях от незнакомых и подозрительных отправителей;
– регулярно проверять используемые сменные накопители на наличие вредоносных объектов перед их использованием;
– проверять на предмет вредоносности файлы, загружаемые из сети Интернет;
– работая в Интернет, не принимать подозрительные предложения загрузить файл или установить программу.

Общим местом всех таких правил являются два принципа:
– использовать только те программы и файлы, которым доверяешь и происхождение которых известно;
– все данные, поступающие из внешних источников, тщательно проверять на предмет вредоносности.

Вторая группа правил, обычно включает такие характерные пункты:
– следить за тем, чтобы программные средства, обеспечивающие защиту, были постоянно активны;
– регулярно обновлять антивирусные базы и модули защиты;
– регулярно устанавливать исправления операционной системы и часто используемых программ;
– не менять настройки по умолчанию программ, обеспечивающих защиту, без необходимости и полного понимания сути изменений.

Здесь также можно проследить два общих принципа:
– использовать наиболее актуальные версии защитных программ - поскольку способы проникновения и активации вредоносных программ постоянно совершенствуются, разработчики защитных программ постоянно добавляют новые технологии защиты и пополняют базы известных вредоносных программ и атак;
– не препятствовать функциям программ антивирусной защиты – очень часто пользователи считают, что защитные программы неоправданно замедляют работу компьютера, и стремятся за счет безопасности повысить производительность. В результате значительно увеличиваются шансы на заражение компьютера вредоносным объектом.

4.2. ПОЛИТИКА БЕЗОПАСНОСТИ

Политика безопасности – это набор законов, правил, процедур и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Причем, политика безопасности относится к активным методам защиты, поскольку учитывает анализ возможных угроз и выбор адекватных мер противодействия.

На домашнем компьютере пользователь сам устанавливает себе правила, которым он считает нужным следовать. По мере накопления знаний о работе компьютера и о вредоносных программах, он может сознательно менять настройки защиты или принимать решение об опасности тех или иных файлов и программ.

В большой организации все сложнее. Когда коллектив объединяет большое количество сотрудников, выполняющих разные функции и имеющих разную специализацию, сложно ожидать от всех разумного поведения с точки зрения безопасности. Поэтому в каждой организации правила работы с компьютером должны быть общими для всех сотрудников и утверждены официально. Обычно документ, содержащий эти правила, называется инструк-

цией пользователя. Кроме основных правил, перечисленных выше, он должен обязательно включать информацию о том, куда должен обращаться пользователь при возникновении ситуации, требующей вмешательства специалиста.

При этом инструкция пользователя в большинстве случаев содержит только правила, ограничивающие его действия. Правила использования программ в инструкцию могут входить только в самом ограниченном виде. Поскольку большинство пользователей недостаточно компетентны в вопросах безопасности, они не должны, а часто и не могут менять настройки средств защиты и как-то влиять на их работу.

Сотрудникам, ответственным за безопасность, приходится устанавливать и настраивать защитные программы на большом количестве компьютеров. Если на каждом компьютере заново решать, какие настройки безопасности должны быть установлены, несложно предположить, что разные сотрудники в разное время и на разных компьютерах установят пусть и похожие, но несколько разные настройки. В такой ситуации будет очень сложно оценить, насколько защищена организация в целом, т. к. никто не знает всех установленных параметров защиты.

Чтобы избежать описанной ситуации, в организациях выбор параметров защиты осуществляется не на усмотрение ответственных сотрудников, а в соответствии со специальным документом - политикой безопасности. В этом документе написано, какую опасность несут вредоносные программы и как от них нужно защищаться. В частности, политика безопасности должна давать ответы на такие вопросы:

– какие компьютеры должны быть защищены средствами антивирусной защиты и с какими настройками;

– какие объекты должны проверяться антивирусом - заархивированные файлы, сетевые диски, входящие и исходящие почтовые сообщения и т. д.;

– какие действия должен выполнять антивирус при обнаружении зараженного объекта – помещать в карантин, удалять и т.д.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Виды информации.
2. Цели защиты информации.
3. Основные требования по защите информации.
4. Меры по защите информации.
5. Дерево классификации детектируемых объектов.
6. Вирусы и сетевые черви.
7. Троянские программы.
8. Подозрительные упаковщики.
9. Хакерские утилиты.
10. Потенциально нежелательные программы.
11. Правило поглощения различных типов детектируемых объектов.
12. Правило именования детектируемых объектов.
13. Альтернативная классификация детектируемых объектов.
14. Сигнатурный анализ.
15. Эвристический анализ.
16. Поведенческий анализ.
17. Метод контрольных сумм.
18. Правовые меры защиты информации.
19. Организационные меры защиты информации.
20. Политики безопасности.

ЛИТЕРАТУРА

1. Об информации, информатизации и защите информации: Закон Республики Беларусь № 455-З.
2. Материалы «Лаборатории Касперского».
3. Национальный открытый университет, http://www.intuit.ru/.

УЧЕБНОЕ ИЗДАНИЕ

Составитель: Безобразов Сергей Валерьевич

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по дисциплине

«ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Часть 1. Основные понятия и определения

для студентов специальностей
1-40 03 01 «Искусственный интеллект» и
1-53 01 02 «Автоматизированные системы обработки информации»

Ответственный за выпуск: Безобразов С.В.
Редактор: Боровикова Е.А.
Компьютерная верстка: Горун Л.Н.
Корректор: Никитчик Е.В.

Подписано к печати 10.07.2012 г. Бумага «Снегурочка». Формат 60x84 1/16.
Гарнитура Arial Narrow. Усл. печ. л. 2,1. Уч. изд. л. 2,25. Заказ № 717. Тираж 50 экз.
Отпечатано на ризографе Учреждения образования «Брестский государственный технический университет» 224017, г. Брест, ул. Московская, 267.