**2.2. Программно-технические угрозы информационной безопасности ПК**

К основным разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе). Англоязычное наименование этих феноменов — malware (буквально — «нехорошие изделия») или badware (от инициативы Stopbadware.org). Stopbadware.org определяет приложение как «badware» если оно:

• действует обманным путем или приводит к необратимым последствиям;

• приводит к потенциально нежелательным результатам без того, чтобы:

— вначале информировать пользователя об этом понятно и доходчиво;

— затем получить его согласие.

**Классификация программных закладок и их общие xарактеристики**

Классификация по следующей совокупности критериев:

-- характеру вредоносного воздействия на ПК;

• уничтожение или искажение программ и/или массивов данных;

• формирование каналов несанкционированного получения информации;

• вывод ПК из числа действующих, т. е. приведение его в такое состояние, при котором он не может осуществлять свои основные функции;

• вредоносное инициирование выполнения предусмотренных в ПК функций (например, ложная подача команды на остановку производства в автоматизированных системах управления технологическими процессами);

• создание препятствий в выполнении функций ПК (например, блокировка отображения информации на экране дисплея, выдачи на печать и др.).

-- способу реализации;

• аппаратный;

• программный;

• организационный.

-- способу проникновения в ПК;

• злоумышленно создаваемые в процессе производства аппаратуры ЭВТ и компонентов ее программного обеспечения;

• неосознанно вносимые персоналом или пользователями ПК в процессе ее функционирования;

• злоумышленно вносимые в процессе функционирования ПК;

• злоумышленно создаваемые в процессе ремонта аппаратуры или обновления ПК.

-- способности к саморазмножению.

• саморазмножающиеся;

• несаморазмножающиеся.

**Средства вторжения в частную жизнь**

Это программы (privacy-invasive software), игнорирующие право пользователя на частную жизнь (или конфиденциальность) и часто преследующие негативные или коммерческие цели.

**Компьютерные наблюдения.** Этот термин (computer surveillance) имеет двоякое толкование: во-первых, сюда относятся средства отслеживания (слежения, «трекинга», от англ. tracking) компьютерной активности, во-вторых — это средства «зомбирования» компьютера, превращения его в устройство наблюдения за пользователем.

**Мониторинговый программный продукт** (tracking software — следящая программа) предназначен для обеспечения наблюдаемости вычислительных систем, а также позволяет фиксировать деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов.

**Компьютерные вирусы**

Вирус — это специально написанная, небольшая по размерам программа (т. е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д.

**Классификация вирусов.** Один из известных «вирусологов» страны Е. Касперский предлагает условно классифицировать вирусы по следующим признакам:

|  |  |  |
| --- | --- | --- |
| Признак | Тип вируса | Пояснения |
| Среда обитания | Сетевые | Распространяются по компьютерной сети |
| Файловые | Внедряются в выполняемые файлы |
| Загрузочные | Внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record) |
| Комбинированные | Например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы и часто применяют оригинальные методы проникновения в систему |
| Способы заражения | Резидентные | При инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера |
| Нерезидентные | Не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными. |
| Деструктивные возможности | Безвредные | Не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения) |
| Неопасные | Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами |
| Опасные | Могут привести к серьезным сбоям в работе |
| Очень опасные | Могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти |
| Особенности алгоритма | Компаньон-вирусы (companion) | Вирусы не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для exe-файлов файлы-спутники, имеющие то же самое имя, но другое расширение. |
| «Черви» (worm) | Распространяются в компьютерной сети и, так же, как и компаньон-вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии |
| «Паразитические» | Вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются «червями» или «компаньонами» |
| «Студенческие» | Примитивные вирусы, часто нерезидентные и содержащие большое число ошибок |
| «Стелс»-вирусы (вирусы-невидимки, stealth) | Представляют собой весьма совершенные программы, которые перехватывают обращения ОС к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы |
| Полиморфические вирусы | Самошифрующиеся или вирусы-призраки (polymorphic) – труднообнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика |
| Макровирусы | Используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Наиболее распространены макровирусы, заражающие текстовые документы редактора Microsoft Word |

**Вирусы без точки входа.** Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (ЕРО-вирусы — Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке ехе-файлов. Такие вирусы записывают команду перехода на

свой код в какое-либо место файла и получают управление не при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке).

**Прочие способы заражения.** Существуют вирусы, которые не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в расчете на то, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на их запуск — например, install.exe или winstart.bat. Некоторые вирусы записывают свои копии в архивные файлы (jar, zip, гаг), а другие записывают команду запуска зараженного файла в bat-файлы. Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла принуждают ОС выполнить вирусный код. Этой цели они достигают модификацией необходимых полей файловой системы.

**Автономные** (вирусы-программы). Со временем вирусы, внедряющие свой код в тело других программ, сдали свои позиции, во многом по той причине, что размеры вирусов выросли, а укрыть код размером в сотни килобайт довольно сложно. В итоге «исполняемые» вирусы перестали маскироваться и превратились

в независимые программы, не нуждающиеся в «хозяине-переносчике». Сразу же перед авторами вирусов возникла проблема — как заставить пользователей загрузить этот вирус и запустить у себя на машине?

Программные вирусы, написанные для операционной системы Windows, обычно маскируются под разные утилиты, например, под ключи к условно-бесплатных программам, мультимедийные презентации, обновления для операционной системы или даже антивирусные программы. Большинство вирусов пользователи запускают на своем компьютере самостоятельно.

**Скрипт-вирусы.** Макровирусы являются одной из разновидностей большого семейства вредоносных программ — скрипт-вирусов. Следует отметить также, что скрипт-вирусы являются подгруппой файловых вирусов и написаны на различных скрипт-языках (VBS, JS, ВАТ, РНР и т. д.). Общая черта скрипт-вирусов — это привязка к одному из «встроенных» языков программирования. Каждый вирус привязан к конкретным изъянам в защите одной из программ Windows и представляет собой не самостоятельную программу, а набор инструкций, которые заставляют в общем-то безобидный «движок» программы совершать не свойственные ему разрушительные действия.

**PolyEngine** — полиморфные генераторы. Полиморфные генераторы не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

**Constructor** — конструкторы вирусов и троянских программ, или VirTools — это утилиты предназначенные для изготовления новых компьютерных вирусов и «троянцев» и/или их изучения в хакерских целях. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули и/или непосредственно зараженные файлы.

**FileCryptor, PolyCryptor** — скрытие от антивирусных программ, хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки.

**VirTool** — утилиты, предназначенные для облегчения написания компьютерных вирусов и для их изучения в хакерских целях.

**Компьютерные черви**

**Email-Worm** — почтовые черви. К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе

(например, URL на зараженный файл, расположенный на взломанном или хакерском Web-сайте). В первом случае код червя запускается при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

**IM-Worm** — черви, использующие Internet-пейджеры. Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты (из списка контактов) сообщений, содержащих URL на файлы, расположенные на каком-либо Web-сервере.

**IRC-Worm** — черви в IRC-каналах. У данного типа червей, как и у почтовых червей, существуют два способа распространения по IRC-каналам, повторяющие способы, описанные выше. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

**Net-Worm** — прочие сетевые черви. Существуют прочие способы заражения удаленных компьютеров, например:

• копирование червя на сетевые ресурсы;

• проникновение червя на компьютер через уязвимости в операционных системах и приложениях;

• проникновение в сетевые ресурсы публичного использования;

• паразитирование на других вредоносных программах.

**P2P-Worm** — черви для файлообменных сетей. Механизм работы большинства подобных червей достаточно прост — для внедрения в Р2Р-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению

Р2Р-червя 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 Р2Р-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно; при этом червь предлагает для скачивания свою копию.

**Троянские программы**

«Троянские кони» (Trojan horse) или просто «троянцы» (Trojans) представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями (обычно это — уничтожение информации, перехват и передача информации, целенаправленная модификация кода программы, интересующей нарушителя).

**Backdoor** — троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети.

**Trojan-PSW** (Password Stealing Ware) — воровство паролей. Данное семейство объединяет «троянские» программы, «ворующие» различную информацию с зараженного компьютера, обычно — системные пароли. При запуске РSW-«троянцы» ищут системные файлы, хранящие различную конфиденциальную информацию (обычно номера телефонов и пароли доступа к Internet) и отсылают ее по указанному в коде «троянца» электронному адресу или адресам.

**Trojan-Clicker** — Internet-кликеры. Семейство «троянских» программ, основная функция которых — организация несанкционированных обращений к Internet-pecypcaм (обычно к Web-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса Internet-pecypcoв (например, файл hosts в MS Windows).

**Trojan-Downloader** — транспортировка других вредоносных программ. «Троянские» программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем. Загруженные из Internet программы затем либо запускаются на выполнение, либо регистрируются «троянцем» на автозагрузку в соответствии с возможностями операционной системы. Данные действия при этом происходят без ведома пользователя.

**Trojan-Dropper** — инсталляторы прочих вредоносных программ. «Троянские» программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для «подсовывания» на компьютер-жертву вирусов или других «троянских» программ.

**Trojan-Spy** — шпионские программы. Данные «троянцы» осуществляют электронный шпионаж за пользователем зараженного компьютера — вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику. «Троянские» программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

**АгсВоmb** — «бомбы» в архивах. Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — 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 полностью заблокировать работу сервера.

Встречаются три типа подобных «бомб»: некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве.

**Другие виды угроз**

**DoS, DDoS — сетевые атаки.** **Программы-рекламы (Adware)**. **Потенциально опасные приложения (Riskware).** К потенциально опасным относятся приложения, которые не имеют вредоносных функций, но могут являться частью среды разработки вредоносного программного обеспечения или использоваться злоумышленниками в качестве вспомогательных компонентов вредоносных программ. К категории таких программ относятся программы, имеющие бреши и ошибки, а также некоторые утилиты удаленного администрирования, программы автоматического переключения раскладки клавиатуры, всевозможные утилиты для остановки процессов или скрытия их работы.

**Программы-шутки (Jokes)**. Данные программы изменяют или прерывают работу компьютера способом, который их создатель счел смешным или, наоборот, пугающим. Они часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т. д.

**Мистификации.** Мистификацией называется сообщение, распространяющееся среди пользователей Internet. Обычно оно отправляется по электронной почте и иногда с помощью средств коммуникации, таких как ICQ или Skype.

**Фишинг.** Термин «фишинг» обозначает преступную деятельность, использующую методы социальной инженерии (манипулирования пользователем, направленное на получение конфиденциальных данных). Целью фишинга является доступ к таким данным, как номера банковских счетов, PIN-коды и т. п.

Попытка получения информации обычно замаскирована в виде сообщения от доверенного лица или бизнес-структуры, например финансовой или страховой компании. Сообщение выглядит вполне благонадежным и содержит графику и текст, который может быть получен от оригинального источника.

**Факторы уязвимости систем для вредоносных программ**

Атакуемой «системой» могут быть различные объекты — отдельное приложение, ОС в целом, отдельный компьютер или сеть. Могут быть выделены следующие факторы уязвимости:

**Гомогенность (монокультурность)** — например, когда все компьютеры в сети используют одну и ту же ОС или одни и те же наборы приложений. В частности, ОС MS Windows занимает такую большую долю рынка, что, ориентируясь на нее, злоумышленник может подорвать большое количество систем.

**Дефекты** — многие системы содержат ошибки, которыми могут воспользоваться вредоносные программы. Типичным примером является буферная недостаточность, когда небольшой объем буфера в ОП приводит к необходимости многократного перезаписывания данных, чем и может воспользоваться ЗПС, чтобы заставить систему выполнить свой код.

**Запуск без подтверждения** — код с дискеты, CD-ROM или USB-устройства может быть запущен без подтверждения пользователем. Первоначально ПК всегда загружались с дискет и до недавнего времени НГМД был первичным загрузочным устройством по умолчанию, поэтому зараженная дискета, оставленная в НГМД, имеет все шансы быть запущенной, и то же самое можно сказать о CD, поскольку BIOS довольно редко запрашивает подтверждение пользователем загрузки со сменных носителей.

**Сверхпривилегии пользователей**. В некоторых системах обычные пользователи имеют привилегии администратора в том смысле, что они могут изменять внутреннюю структуру этой системы. Это, конечно, определяется конфигурацией, однако в системах MS Windows конфигурация по умолчанию отличается тем, что здесь пользователь имеет сверхпривилегии.

**Сверхпривилегированный код.** Вредоносная программа, запущенная как привилегированный код, может воспользоваться этим для подрыва системы.

**Инъекция SQL** {англ. — SQL injection) — в зависимости от типа используемой СУБД и условий инъекции, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.

**Эксплойт** (англ. exploit — использовать) — фрагмент программного кода, который, используя возможности, предоставляемые ошибкой, отказом или уязвимостью, ведет к повышению привилегий или отказу в обслуживании компьютерной системы.