



Лекция

«Угрозы безопасности программного обеспечению»

1. Угрозы безопасности программного обеспечению ИС.
2. Общая характеристика и классификация вредоносных программ.



Угрозы безопасности программному обеспечению ИС

Программное обеспечение (ПО) информационных систем (ИС) в общем случае состоит из следующих основных компонент:

- операционной системы (ОС),
- сетевого программного обеспечения (СПО),
- системы управления базами данных (СУБД),
- прикладного программного обеспечения (ППО).

Определения (в соответствии с ISO/IEC 27000:2018):

Угроза (англ. **threat**) – потенциальная причина нежелательного инцидента, который может причинить вред системе или организации.

Уязвимость (англ. **vulnerability**) – слабое звено актива или средства управления, которое может быть источником угроз

Определения из других источников:

- *Загроза* – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС [НД ТЗІ 1.1-003-99].
- Под *угрозой* обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угрозы безопасности программному обеспечению ИС

Определения

Атака (attack) – спроба реалізації загрози [НД ТЗІ 1.1-003-99].

Атака – умышленное или непреднамеренное действие, которое может повредить или иным образом поставить под угрозу информацию и системы, которые ее поддерживают.

Атаки могут быть *активными* или *пассивными*, *преднамеренными* или *непреднамеренными*, а также *прямыми* или *косвенными*.

Тот, кто случайно читает конфиденциальную информацию, не предназначенную для его использования, совершает *пассивную* атаку.

Хакер, пытающийся взломать информационную систему, является *преднамеренной* атакой.

Удар молнии, вызывающий возгорание здания, является *непреднамеренной* атакой.

Прямая атака осуществляется хакером, использующим ПК для взлома системы.

Непрямая атака - это хакер, компрометирующий систему и использующий ее для атаки на другие системы - например, как часть ботнета (*botnet*) (группа скомпрометированных компьютеров, на которых запущено программное обеспечение по выбору злоумышленника, может работать автономно или под прямым контролем злоумышленника с атакуемыми системами и красть пользовательскую информацию или проводить распределенные атаки типа «отказ в обслуживании»).

Прямые атаки исходят от самой угрозы.

Косвенные атаки исходят от скомпрометированной системы или ресурса, который неисправен или работает под контролем угрозы.

Угрозы безопасности программному обеспечению ИС

Все угрозы защите компьютерных систем на уровнях рассматриваемых компонент можно разделить на следующие группы:

- ☐ на уровне операционной системы;
- ☐ на уровне систем управления базами данных;
- ☐ на уровне сетевого программного обеспечения;
- ☐ на уровне прикладного программного обеспечения.

Наиболее уязвимы критические компьютерные системы (КС).

Под критическими компьютерными системами будем понимать сложные компьютеризированные организационно-технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно-транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам.

Угрозы безопасности программному обеспечению ИС

Угрозы, характерные для операционной системы

1. Кража пароля.

Атака:

- ✓ подглядывание за пользователем (когда тот вводит пароль, дающий право на работу с операционной системой; даже если во время ввода пароль не высвечивается на экране дисплея, злоумышленник может достаточно легко «вычислить» пароль, просто следя за перемещением пальцев пользователя по клавиатуре);
- ✓ получение пароля из файла, в котором этот пароль был сохранен пользователем, не желающим затруднять себя вводом пароля при подключении к сети (как правило, такой пароль хранится в файле в незашифрованном виде);
- ✓ поиск пароля, который пользователи, чтобы не забыть, записывают на календарях, в записных книжках или на оборотной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять трудно запоминаемые пароли);
- ✓ кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);
- ✓ полный перебор всех возможных вариантов пароля;
- ✓ подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе – его имени, фамилии, номера телефона, даты рождения и т. д., с использованием сведений о существовании эквивалентных паролей, при этом из каждого класса опробуется всего один пароль, что может значительно сократить время перебора.

Угрозы безопасности программному обеспечению ИС

Угрозы, характерные для операционной системы

2. Сканирование жестких дисков компьютера.

Атака: злоумышленник последовательно пытается обратиться к каждому файлу, хранимому на жестких дисках компьютерной системы (если объем дискового пространства достаточно велик, можно быть вполне уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны злоумышленником; для сокрытия следов последний может организовать эту атаку под чужим именем: например, под именем пользователя, пароль которого известен злоумышленнику).

3. Сборка "мусора".

Атака: просмотр содержимое "мусорных" корзин (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, злоумышленник может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным другими пользователями).

Угрозы безопасности программному обеспечению ИС

Угрозы, характерные для операционной системы

4. Превышение полномочий.

Атака: используя ошибки в программном обеспечении или в администрировании операционной системы, злоумышленник получает полномочия, превышающие полномочия, предоставленные ему согласно действующей политике безопасности:

- ✓ запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);
- ✓ подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;
- ✓ модификация кода или данных подсистемы защиты самой операционной системы.

5. Отказ в обслуживании

Атака (целью этой атаки является частичный или полный вывод из строя операционной системы):

- ✓ захват ресурсов (вредоносная программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);
- ✓ бомбардировка запросами (вредоносная программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера).

Угрозы безопасности программному обеспечению ИС

Угрозы, характерные для систем управления базами данных

Угрозы, характерные для ОС (такие как кража паролей, превышение полномочий, отказ в обслуживании) актуальны и для систем управления базами данных. Кроме них, БД, функционирующие под управлением СУБД подвержены таким угрозам, как:

- ☐ нарушение (утрата) конфиденциальности данных;
- ☐ нарушение (утрата) целостности данных;
- ☐ потеря доступности данных.

Угрозой нарушения конфиденциальности данных является любое умышленное или случайное раскрытие информации, хранящейся в БД или передаваемой из одной системы в другую.

К нарушению конфиденциальности ведет как преднамеренное действие, направленное на реализацию несанкционированного доступа (НСД) к данным, так и случайная ошибка программного или неквалифицированного действия пользователя, которая привела к передаче незащищенной конфиденциальной информации по открытым каналам связи.

Угрозой нарушения целостности является любое преднамеренное или случайное изменение данных БД, приводящие к нарушению непротиворечивого набора правил (нарушению логических ограничений, накладываемых на данные).

К нарушению целостности данных может привести как умышленное деструктивное действие злоумышленника, изменяющего данные для достижения собственных целей, так и случайная ошибка программного или аппаратного обеспечения, приведшая к безвозвратному разрушению данных.

В настоящее время множество организаций функционирует в непрерывном режиме 24 часа в сутки, 7 дней в неделю. Потеря доступности данных будет означать, что, либо данные, либо система, либо и то и другое одновременно окажутся недоступными пользователям. Это может подвергнуть опасности, как финансовое положение организации, так и всевозможные системы управления, использующие базы данных для своих потребностей.

Угрозы безопасности программному обеспечению ИС

Угрозы конфиденциальности информации

1. *Инъекция SQL* (в общем случае *инъекция ввода*). Во многих приложениях используется динамический SQL – формирование SQL-предложений, использующих процедуру конкатенации строк и значений параметров. Зная структуру БД, злоумышленник может либо выполнить хранимую программу в запросе, либо закомментировать «легальные» фрагменты SQL-кода, внедрив, например, конструкцию UNION, запрос которой возвращает конфиденциальные данные.
2. *Логический вывод на основе функциональных зависимостей* (в общем случае угроза *inference*). Пример функциональной зависимости для схемы отношения (фамилия, имя, отчество, должность, зарплата): если должность=менеджер, то зарплата=1200. В реальных базах данных при наличии сведений о функциональных зависимостях злоумышленник может вывести конфиденциальную информацию при наличии доступа только к части отношений, составляющих декомпозированное отношение.
3. *Логический вывод на основе ограничения целостности* (в общем случае угроза *inference*). Для кортежей отношений в реляционной модели данных можно задать ограничения целостности. Выполняя многократные изменения данных и анализируя реакцию системы, злоумышленник может получить те сведения, к которым у него отсутствует непосредственный доступ.
4. *Использование оператора UPDATE для получения конфиденциальной информации* (в общем случае угроза *inference*). В некоторых стандартах SQL пользователь, не обладая привилегией на выполнение оператора SELECT, мог выполнить оператор UPDATE со сколь угодно сложным логическим условием. Так как после выполнения оператора UPDATE сообщается, сколько строк он обработал фактически пользователь мог узнать, существуют ли данные, удовлетворяющие этому условию.

Угрозы безопасности программному обеспечению ИС

Специфичными для систем управления базами данных угрозами доступности являются:

1. *Использование свойств первичных и внешних ключей.* В первую очередь сюда относится свойство уникальности первичных ключей и наличие ссылочной целостности. В том случае, если используются натуральные, а не генерируемые системой значения первичных ключей, можно создать такую ситуацию, когда в таблицу невозможно будет вставить новые записи, так как там уже будут записи с такими же значениями первичных ключей. Если в БД поддерживается ссылочная целостность, можно организовать невозможность удаления родительских записей, умышленно создав подчиненные записи. Важной особенностью реализации ссылочной целостности является вопрос об индексировании внешнего ключа. В том случае, если внешний ключ не проиндексирован, то при обновлении связанных записей, например, в СУБД Oracle возможна организация взаимной блокировки (dead-lock), что приведет к сбою в транзакции.

2. *Блокировка записей при изменении.* Заблокировав записи или всю таблицу, злоумышленник может на значительное время сделать ее недоступной для обновления.

3. *Загрузка системы бессмысленной работой,* простейший пример – выполнение запроса, содержащего декартово произведение двух больших отношений. Мощность декартового произведения двух отношений мощности N_1 и N_2 равна $N_1 * N_2$.

Возможны реализации и других классических угроз, например атаки типа «троянский конь» – запуска пользователями программ, содержащих выполняющий определенные действия код, внедренный туда злоумышленником.

Угрозы безопасности программному обеспечению ИС

Угрозы, характерные для сетевого программного обеспечения

СПО является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные.

На уровне СПО возможны следующие атаки злоумышленников:

- ✓ прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер злоумышленника подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);
- ✓ перехват сообщений на маршрутизаторе (если злоумышленник имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным для злоумышленника является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);
- ✓ создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида злоумышленник добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);
- ✓ навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер злоумышленника);
- ✓ отказ в обслуживании (злоумышленник отправляет в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Угрозы безопасности программному обеспечению ИС

Угрозы прикладному программному обеспечению

Для прикладного ПО характерны следующие угрозы безопасности:

- ✓ нелегальное копирование и распространение;
- ✓ нелегальное использование;
- ✓ нелегальное исследование и изменение;
- ✓ нелегальное снятие защиты от копирования и несанкционированного использования.

Общая система оценки уязвимостей CVSS (Common Vulnerability Scoring System, версии 2.0 и 3.X)

В настоящее время IT-персонал вынужден выявлять и обрабатывать уязвимости различных программных и аппаратных платформ.

Существует необходимость расставить приоритеты для этих уязвимостей, чтобы в первую очередь исправлять те из них, которые представляют наибольшую опасность.

Но так как уязвимостей, подлежащих исправлению много, и они могут быть оценены по разным шкалам, то свести эти данные воедино для общего анализа не представляется возможным.

Базы уязвимостей

Наименование	Адрес
Открытые базы уязвимостей	
Компания MITRE и её база «Общие уязвимости и воздействия» (Common Vulnerabilities and Exposures — CVE)	http://cve.mitre.org/data/downloads/allitems.html
Национальный институт стандартов и технологий (National Institute of Standards and Technology — NIST) и его Национальная база данных уязвимостей (National Vulnerabilities Database — NVD)	https://nvd.nist.gov/download.cfm
Открытая база данных уязвимостей (Open Source Vulnerability Database — OSVDB)	https://blog.osvdb.org/2014/03/
Группа чрезвычайного компьютерного реагирования США (United State Computer Emergency Readiness Team — US-CERT) с Базой данных записей уязвимостей (Vulnerability Notes Database — VND)	https://www.us-cert.gov/
Проект Security Focus и его база уязвимостей Bug Traq	http://www.securityfocus.com/bid
Компания IBM с базой уязвимостей X-Force	http://www-03.ibm.com/security/xforce/resources.html#all
ФСТЭК Российской Федерации База данных уязвимостей	http://www.bdu.fstec.ru/vul
Лаборатория Security Lab и его база уязвимостей	http://www.securitylab.ru/vulnerability/page1_1.php
Cisco Security Advisories and Responses	https://tools.cisco.com/security/center/publicationListing.x
Software Engineering Institute	https://www.kb.cert.org/vuls/bypublished/
WPScan Vulnerability Database	https://wpvulndb.com/
Коммерческие (закрытые) базы уязвимостей	
Компания Secunia	http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/vulnerability-intelligence-manager/
VUPEN Security	https://ssl0.ovh.net/en/

Общая система оценки уязвимостей CVSS (Common Vulnerability Scoring System, версии 2.0 и 3.X)

Поэтому группой экспертов по безопасности National Infrastructure Advisory Council (в эту группу вошли эксперты из различных организаций, таких как CERT/CC, Cisco, DHS/MITRE, eBay, IBM Internet Security Systems, Microsoft, Qualys, Symantec) был разработан стандарт Common Vulnerability Scoring System.

Общая система оценки уязвимостей (CVSS) – это открытая схема, которая предназначена для решения этой проблемы. Использование CVSS предоставляет следующие выгоды:

- ❑ *Стандартизованная оценка уязвимостей.* После нормализации оценок уязвимостей для всех программных и аппаратных платформ компании может использоваться единая политика управления уязвимостями. Эта политика сходна с договором о предоставлении услуг (SLA, Service Level Agreement), который определяет, как быстро конкретная проблема должна быть решена.
- ❑ *Открытость системы.* Пользователи часто не понимают, каким образом была получена оценка уязвимости. Часто задаются такие вопросы: «Из-за каких свойств уязвимость получила именно эту оценку? Чем она отличается от той, о которой стало известно вчера?» Использование CVSS позволяет каждому увидеть индивидуальные особенности уязвимости, которые привели к указанной оценке.
- ❑ *Приоритезация рисков:* Как только для уязвимости вычислена контекстная метрика, оценка этой уязвимости становится зависимой от среды. Это означает, что полученная оценка отражает реальный риск от наличия этой уязвимости, который существует в данной организации с учетом других уязвимостей.

Общая система оценки уязвимостей CVSS (Common Vulnerability Scoring System, версии 2.0 и 3.X)

В 2014 году рекомендации по использованию CVSSv2 выпускают такие авторитетные организации, как NIST и ITU, занимающиеся разработкой руководств и стандартов в области телекоммуникации и информационных систем. Использование метрик CVSS для оценки уязвимостей закреплено в стандартах PCI DSS.

В CVSS (*общей системе оценки уязвимостей*) используются группы метрик, а также дается описание базовых метрик [base metrics], вектора уязвимости [vector] и оценок уязвимости.

Метод оценки CVSS состоит из трех основных метрик:

- базовой;
- временной;
- контекстной (окружения).

Каждая из них, в свою очередь, состоит из набора метрик.

Группы метрик CVSS



- Группа базовых метрик представляет основные существенные характеристики уязвимости, которые не изменяются со временем и не зависят от среды.
- Группа временных метрик представляет такие характеристики уязвимости, которые могут измениться со временем, но не зависят от среды.
- Группа контекстных метрик представляет такие характеристики уязвимости, которые зависят от среды

Базовые CVSS-метрики составляются для того, чтобы определить и отобразить основные характеристики уязвимости.

Эта попытка объективно охарактеризовать уязвимость дает пользователям ясное и интуитивно понятное представление об уязвимости.

Затем пользователи могут использовать временные и контекстные группы метрик, чтобы получить более подробную информацию об уязвимости с учетом своей среды. Это позволяет принимать обоснованные решения при выборе способа минимизации риска от наличия уязвимости.

Группы метрик CVSS

Базовые метрики

Существуют метрики возможности эксплуатации [*exploitability*] и воздействия [*impact*]:

Возможность эксплуатации

а) Вектор доступа [**access vector, AV**] описывает возможный способ эксплуатации уязвимости:

- локальный [**local, L**] — уязвимость эксплуатируется только локально;
- локально-сетевой [*adjacent network, A*] — уязвимость может эксплуатироваться только из смежных сетей;
- сетевой [**network, N**] — уязвимость может эксплуатироваться удаленно.

Чем дальше может находиться источник атаки, тем опаснее уязвимость.

б) Сложность доступа [**access complexity, AC**] описывает уровень сложности атаки:

- Высокий уровень [**high, H**] — для эксплуатации уязвимости требуется выполнить определенную последовательность действий;
- Средний уровень [**medium, M**] — уязвимость нельзя отнести ни к сложной, ни к легко эксплуатируемой;
- Низкий уровень [**low, L**] — уязвимость эксплуатируется просто.

Чем ниже оценка сложности доступа, тем опаснее уязвимость.

в) Метрика «аутентификация» [**authentication, Au**] описывает способ аутентификации для эксплуатации уязвимости:

- Многократная [**multiple, M**] — атакующий должен пройти аутентификацию два и более раз;
- Однократная [**single, S**] — атакующий должен пройти аутентификацию один раз;
- Нулевая [**none, N**] — аутентификация не требуется.

Чем меньше раз требуется проходить аутентификацию, тем опаснее уязвимость.

Группы метрик CVSS

Базовые метрики

Воздействие

- а) Метрика «воздействие на конфиденциальность» **[confidentiality, C]** описывает воздействие уязвимости на конфиденциальность данных системы:
- нулевое **[none, N]** — воздействие отсутствует;
 - частичное **[partial, P]** — можно считать часть данных;
 - полное **[complete, C]** — можно считать любые данные.

Чем сильнее воздействие на конфиденциальность данных в системе, тем опаснее уязвимость.

- б) Метрика «воздействие на целостность» **[integrity, I]** описывает воздействие уязвимости на целостность данных системы:
- нулевое **[none, N]** — воздействие отсутствует;
 - частичное **[partial, P]** — можно изменить часть данных;
 - полное **[complete, C]** — можно изменить любые данные.

Чем сильнее воздействие на целостность данных в системе, тем опаснее уязвимость.

- в) Метрика «воздействие на доступность» **[availability, A]** описывает воздействие уязвимости на доступность системы:
- нулевое **[none, N]** — воздействие отсутствует;
 - частичное **[partial, P]** — уязвимость может вызвать в системе временные отказы в обслуживании или снижение производительности;
 - полное **[complete, C]** — уязвимость может вызвать полный отказ системы в обслуживании.

Чем сильнее воздействие на доступность системы, тем опаснее уязвимость.

Обратите внимание на сокращенные названия метрик и их значения в скобках. Эти сокращения используются в описании базового вектора уязвимости.

Группы метрик CVSS

Базовый вектор [base vector]

Он записывается в следующем формате:

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

Это сокращенная запись уязвимости, в которой информация о метриках приводится вместе со значениями метрик.

В скобках указываются возможные значения для указанных базовых метрик.

Специалист по оценке выбирает одно значение для каждой базовой метрики.

Оценка

Формулы расчета базовой оценки **[base score]**, возможности эксплуатации и элементов оценки воздействия приведены в руководстве *A complete Guide to the Common Vulnerability Scoring System Version 2.0* или Common Vulnerability Scoring System version 3.1, Specification Document, Revision 1.

Однако, считать все вручную необходимости нет, так как существует калькулятор оценки уязвимостей – [Common Vulnerability Scoring System Calculator Version 2](#) или [Common Vulnerability Scoring System Calculator Version 3.0\(3.1\)](#).

Все, что нужно сделать специалисту по оценке — это внести значения для соответствующих метрик.

Уровень опасности

Базовая оценка зависит от оценки возможности эксплуатации и элементов оценок воздействия на систему и выставляется от 0 до 10, где 10 соответствует высочайшему уровню опасности уязвимости.

Группы метрик CVSS

Рейтинги серьезности уязвимости национальной базы данных уязвимостей
(NVD (national vulnerability database) Vulnerability Severity Ratings)

Качественная оценка	Количественная оценка	
	CVSS v2.0	CVSS v3.0 (v3.1)
None		0.0
Low	0.0-3.9	0.1-3.9
Medium	4.0-6.9	4.0-6.9
High	7.0-10.0	7.0-8.9
Critical		9.0-10.0

Общая характеристика и классификация вредоносных программ

Вредоносная программа (англ. *"malicious software"* – злонамеренное программное обеспечение) – злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.

Вредоносные программы можно классифицировать:

➤ *по наличию материальной выгоды:*

- ✓ *не приносящие* прямую материальную выгоду тому, кто разработал (установил) вредоносную программу (хулиганство; вандализм, в том числе на религиозной, националистической, политической почве; самоутверждение; стремление доказать свою квалификацию);
- ✓ *приносящие* прямую материальную выгоду злоумышленнику за счет:
 - хищения конфиденциальной информации;
 - получения контроля над удаленными компьютерными системами (с целью распространения спама с многочисленных компьютеров-зомби, с целью организации распределенных атак на отказ в обслуживании, с целью получения доступа к конфиденциальной информации и т. д.);

➤ *по цели разработки:*

- ✓ программное обеспечение, которое изначально разрабатывалось специально для обеспечения получения несанкционированного доступа к информации, хранимой на компьютере с целью причинения вреда (ущерба);
- ✓ программное обеспечение, которое изначально не разрабатывалось специально для обеспечения получения несанкционированного доступа к информации, хранимой на компьютере и изначально не предназначалась для причинения вреда (ущерба).

Общая характеристика и классификация вредоносных программ

Вредоносное ПО способно:

- создавать помехи работе пользователя (в шутку или для достижения других целей):
 - ✓ уничтожать или искажать данные, осуществлять труднозамечаемые повреждения файлов;
 - ✓ шифровать данные и т. д.;
- шпионить за пользователем:
 - ✓ регистрировать нажатие клавиш с целью кражи информации паролей, номеров кредитных карточек и т. д.;
 - ✓ "добывать" криптографическую информацию (такую как открытые и закрытые ключи, используемые при шифровании и цифровой подписи);
- использовать ресурсы компьютера, как правило, заражённого в преступных целях:
 - ✓ получать несанкционированный доступ к ресурсам самого компьютера или третьим ресурсам, доступным через него;
 - ✓ выводить из строя или приводить к отказу обслуживания компьютерные системы, сети;
 - ✓ осуществлять сбор адресов электронной почты и распространять спам и т. д.;
- осуществлять прочие виды незаконной деятельности:
 - ✓ распространять вредоносные программы;
 - ✓ деактивизировать антивирусное программное обеспечение и межсетевые экраны и т. д.

Общая характеристика и классификация вредоносных программ

Симптомы воздействия вредоносных программ:

- ✓ прекращение или сильное замедление работы во всемирной информационной компьютерной сети;
- ✓ усиление шума, исходящего от компьютера (создается усиленной работой жёстких дисков);
- ✓ изменение домашней страницы в браузере, автоматическое открытие окон с незнакомыми вам страницами;
- ✓ изменение обоев на рабочем столе;
- ✓ появление новых неизвестных процессов в окне «Процессы» диспетчера задач;
- ✓ появление в реестре автозапуска новых приложений;
- ✓ запрет на изменение настроек компьютера в учётной записи администратора;
- ✓ невозможность запустить исполняемый файл (выдается сообщение об ошибке);
- ✓ всплывание окон системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса и названия;
- ✓ мониторы интернета показывают фальшивую загрузку видеопрограмм, игр, порнороликов и порносайтов, которые вы не закативали и не посещали;
- ✓ открывание и закрывание консоли CD-ROM;
- ✓ проигрывание звуков и/или изображений, демонстрация фотоснимков;
- ✓ перезапуск компьютера во время старта какой-либо программы;
- ✓ случайное и/или беспорядочное отключение компьютера и т. д.

Общая характеристика и классификация вредоносных программ

Вредоносные программы и вредоносные действия, осуществляемые с помощью программного обеспечения, можно классифицировать следующим образом :

- ✓ вредоносные программы, осуществляющие атаки методом подбора пароля (*Brute force attacks*);
- ✓ бомбы с часовыми механизмами (*Time bombs*);
- ✓ вишинг (*Vishing*);
- ✓ дифейсмент (*Defacement*);
- ✓ вредоносные программы, осуществляющие DoS-атаки (*DoS-attacks*);
- ✓ зомби (*Zombies*);
- ✓ клавиатурные перехватчики (*Keyloggers*);
- ✓ логические бомбы (*Logic bombs*);
- ✓ люки (*Backdoors*);
- ✓ почтовые бомбы (*Mail bombs*);
- ✓ руткит (*Rootkit*);
- ✓ скамминг (*Scamming*);
- ✓ sniffинг (*Sniffing*);
- ✓ спуфинг (*Spoofing*);
- ✓ троянские кони (Троянцы) (*Trojan Horses*);
- ✓ фишинг (*Phishing*);
- ✓ фарминг (*Pharming*).

Общая характеристика и классификация вредоносных программ

Бомбы с часовыми механизмами (time bombs) – одна из разновидностей логических бомб, в которых срабатывание скрытого модуля определяется временем.

Вишинг (vishing) – технология интернет мошенничества, разновидность фишинга, заключающаяся в использовании в злонамеренных целях автонабирателей ("war dialers") и возможностей Интернет-телефонии (VoIP) для кражи личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д.

Диффейсмент (defacement) – искажение веб-страниц. Вид компьютерного вандализма, иногда являющийся для хакера забавой, а иногда средством выражения политических пристрастий. Искращения могут производиться в какой-то части сайта или выражаться в полной замене существующих на сайте страниц (чаще всего, стартовой).

DoS (denial of service – отказ в обслуживании) – атака, имеющая своей целью заставить сервер не отвечать на запросы. Такой вид атаки не подразумевает получение некоторой секретной информации, но иногда бывает подспорьем в инициализации других атак.

Причины, по которым может возникнуть DoS-условие:

- ✓ *ошибка* в программном коде, приводящая к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение серверного приложения;
- ✓ *некорректная проверка данных пользователя*, приводящая к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов (исчерпанию процессорных ресурсов) либо выделению большого объема оперативной памяти (исчерпанию памяти);
- ✓ *флуд (flood)* – атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания ресурсов системы – процессора, памяти либо каналов связи;
- ✓ *атака второго рода* – атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

Общая характеристика и классификация вредоносных программ

DDoS (Distributed Denial of Service – распределенная *DoS*) – подтип *DoS* атаки, имеющий ту же цель что и *DoS*, но производимой не с одного компьютера, а с нескольких компьютеров в сети.

Зомби (zombies) – маленькие компьютерные программы, разносимые по сети интернет компьютерными червями. Программы-зомби устанавливаются в пораженной системе и ждут дальнейших команд к действию.

Клавиатурные перехватчики (keyloggers) – вид троянских программ, чьей основной функцией является перехват данных, вводимых пользователем через клавиатуру. Объектами похищения являются персональные и сетевые пароли доступа, логины, данные кредитных карт и другая персональная информация.

Логические бомбы (logic bombs) – вид троянского коня – скрытые модули, встроенные в ранее разработанную и широко используемую программу. Являются средством компьютерного саботажа.

Backdoors (задние ворота), или trapdoor (люк) – программная закладка, обеспечивающая вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода существующей системы безопасности.

Люк может присутствовать в программном продукте вследствие умышленных или неумышленных действий со стороны программиста для обеспечения:

- ✓ тестирования и отладки программного продукта;
- ✓ окончательной сборки конечной программы;
- ✓ скрытого средства доступа к программному продукту и данным.

Общая характеристика и классификация вредоносных программ

Почтовые бомбы (*mail bombs*) – один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение, или множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя. Такого рода вредительское воздействие в известной литературе относят к классу "компьютерного хулиганства", которое получило название "пинание" (*pinging*).

Руткит – вредоносная программа, предназначенная для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, *rootkit* может маскировать процессы других программ, различные ключи реестра, папки, файлы. *Rootkit* распространяются как самостоятельные программы, так и как дополнительные компоненты в составе иных вредоносных программ - программ-люков, почтовых червей и т. д. По принципу своей работы *rootkit* условно разделяют на две группы: *User Mode Rootkits (UMR)* – так называемый *rootkit*, работающие в режиме пользователя, и *Kernel Mode Rootkit (KMR)* – так называемый *rootkit*, работающие в режиме ядра.

Скамминг – от английского "*scamming*", что означает "жульничество", вид интернет мошенничества. Заключается в привлечении клиентов, якобы брачными агентствами (на самом деле скам-агентствами), с целью выуживания у них денег брачными аферами.

Сниффинг (*Sniffing* – *нюхание*) – вид сетевой атаки, также называется "пассивное прослушивание сети". Несанкционированное прослушивание сети и наблюдение за данными производятся при помощи специальной не вредоносной программой – пакетным сниффером, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение. Перехваченные таким сниффером данные могут быть использованы злоумышленниками для легального проникновения в сеть на правах фальшивого пользователя.

Общая характеристика и классификация вредоносных программ

Спуфинг (Spoofing) – вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения. Используется для обхода систем управления доступом на основе IP адресов, а также для набирающей сейчас обороты маскировки ложных сайтов под их легальных двойников или просто под законные бизнесы.

Троянские кони (троянцы) (Trojan Horses) – вредоносные программы, содержащие скрытый модуль, осуществляющий несанкционированные пользователем действия в компьютере. Эти действия не обязательно будут разрушительными, но они всегда направлены во вред пользователю.

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – технология интернет мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т. д.

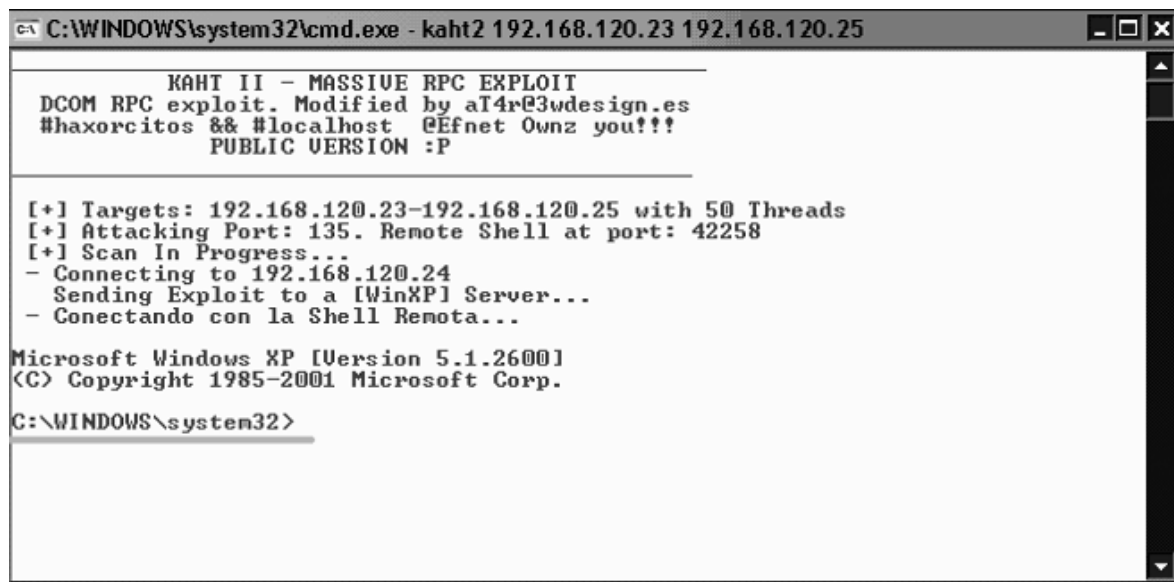
Фарминг (pharming) – сравнительно новый вид интернет мошенничества. Фарминг технологии позволяют изменять *DNS (Domain Name System)* записи либо записи в файле *HOSTS*. При посещении пользователем легитимной, с его точки зрения, страницы производится перенаправление на поддельную страницу, созданную для сбора конфиденциальной информации. Чаще всего такие страницы подменяют страницы банков – как оффлайновых, так и онлайн-овых.

Общая характеристика и классификация вредоносных программ

Другие виды вредоносных программ

Эксплойт, эксплоит (*exploit* – эксплуатировать) – это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (*DoS*-атака).

Действие всех эксплойтов сводится либо к получению удаленного доступа к атакуемой системе в виде командной оболочки, так называемого, *шелла* (*shell* или *rootshell*), либо в удаленном выполнении какой-либо системной команды, либо к вынужденной перезагрузке удаленной системы.



```
C:\WINDOWS\system32\cmd.exe - kaht2 192.168.120.23 192.168.120.25

KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
PUBLIC VERSION :P

[+] Targets: 192.168.120.23-192.168.120.25 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 42258
[+] Scan In Progress...
- Connecting to 192.168.120.24
- Sending Exploit to a [WinXP] Server...
- Conectando con la Shell Remota...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Рис. 1 – Возможности воздействия эксплойта kaHt2

Последствия применения эксплойтов могут быть непредсказуемыми. В случае получения злоумышленником удаленного доступа к системе, он имеет практически полный (системный) доступ к компьютеру.

Общая характеристика и классификация вредоносных программ

Репликаторы – могут создавать одну, или более своих копий в компьютерной системе. Это приводит к быстрому переполнению памяти компьютера.

"Раздеватель" – комплекс специально разработанных программных средств, ориентированных на исследование защитного механизма программного продукта от несанкционированного копирования (НСК) и его преодоление.

Под *нелегальным распространением* понимается продажа, обмен или бесплатное распространение программного продукта, авторские права на который принадлежат третьему лицу, без его согласия.

Нелегальное использование – это использование программного продукта без согласия владельца авторских прав.

Нелегальное изменение – это внесение в код программы или внешний вид (интерфейс) изменений, не оговоренных с владельцем авторских прав, с тем, чтобы измененный продукт не попадал под действие авторских прав.

Под *компьютерным вирусом* (или просто вирусом) понимается автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в сетях и отдельных компьютерах.

Принципиальное отличие вируса от троянской программы состоит в том, что вирус после его активизации существует самостоятельно (автономно) и в процессе своего функционирования заражает (инфицирует) программы путем включения (имплантации) в них своего текста. Компьютерный вирус можно рассматривать как своеобразный "генератор троянских программ". Программы, зараженные вирусом, называются *вирусоносителями*.

Червями называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ИС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

Общая характеристика и классификация вредоносных программ

Вирусы, использующие для размножения сетевые средства, принято называть *сетевыми*.

Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликации (саморазмножения) и проявления. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации в компьютере или на магнитных носителях.

Физическая структура компьютерного вируса достаточно проста. Он состоит из головы и, возможно, хвоста. *Под головой вируса* понимается его компонента, получающая управление первой. *Хвост* – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют *несегментированными*, вирусы, содержащие голову и хвост – *сегментированными*.

Компьютерные вирусы классифицируют:

❑ *по режиму функционирования:*

- ✓ *резидентные вирусы* – вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера (до выключения компьютера или перезагрузки операционной системы) и контролируют доступ к его ресурсам. Такие вирусы активны не только в момент работы зараженной программы, но и после завершения работы;
- ✓ *транзитные вирусы* – выполняются только в момент запуска зараженной программы;

❑ *по объекту внедрения (среде обитания):*

- ✓ *файловые вирусы* – вирусы, заражающие файлы с программами;
- ✓ *загрузочные вирусы* – вирусы, заражающие программы, хранящиеся в системных областях дисков;
- ✓ *макровирусы*;
- ✓ *сетевые*.

Общая характеристика и классификация вредоносных программ

Файловые вирусы подразделяются на вирусы, заражающие:

- ✓ исполняемые файлы;
- ✓ командные файлы и файлы конфигурации;
- ✓ файлы с драйверами устройств;
- ✓ файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки и т.п.

Существуют резидентные и нерезидентные файловые вирусы.

Файловый резидентный вирус отличается от нерезидентного тем, что заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память компьютера. Резидентный вирус состоит из, так называемого, инсталлятора и программ обработки прерываний. Инсталлятор получает управление при активизации вирусоносителя и инфицирует оперативную память путем размещения в ней управляющей части вируса и замены адресов в элементах вектора прерываний на адреса своих программ, обрабатывающих эти прерывания. На так называемой фазе слежения, следующей за описанной фазой инсталляции, при возникновении какого-либо прерывания управление получает соответствующая программа вируса. По сравнению с нерезидентными вирусами, резидентные вирусы могут реализовать самые разные способы инфицирования. Наиболее распространенными способами являются инфицирование запускаемых программ, а так же файлов при их открытии или чтении.

Файловый нерезидентный вирус целиком размещается в исполняемом файле, в связи, с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.

Общая характеристика и классификация вредоносных программ

По способу заражения файлов вирусы делятся на:

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

Overwriting-вирусы. Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как ОС и приложения довольно быстро перестают работать.

Parasitic-вирусы. К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (*prepending*), в конец файлов (*appending*) и в середину файлов (*inserting*). В свою очередь, внедрение вирусов в середину файлов происходит различными методами – путем переноса части файла в его конец или внедрения в заведомо неиспользуемые данные файла (*cavity-вирусы*).

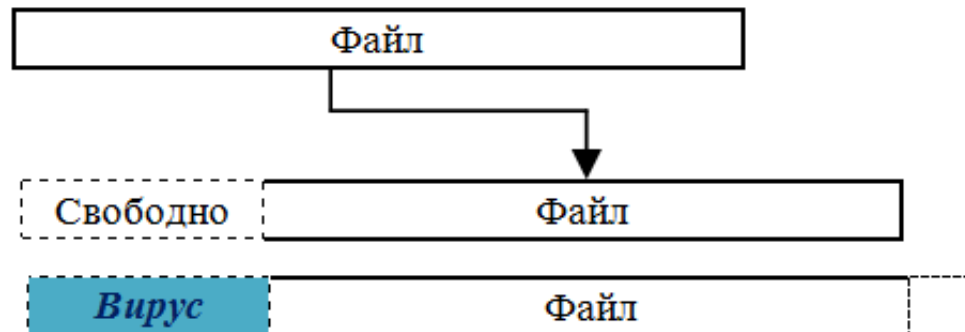
Общая характеристика и классификация вредоносных программ

Внедрение вируса в начало файла

Известны два способа внедрения паразитического файлового вируса в начало файла. *Первый способ* заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется на освободившееся место:

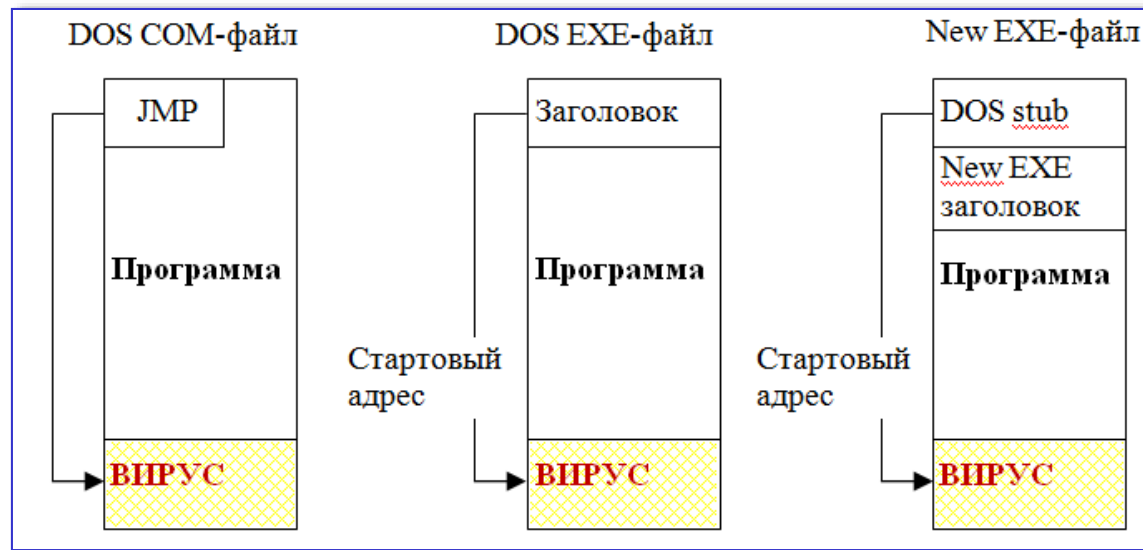


Второй способ заключается в том, что вирус создает в оперативной памяти свою копию, дописывает к ней заражаемый файл и сохраняет полученную конкатенацию на диск.



Общая характеристика и классификация вредоносных программ

Внедрение вируса в конец файла



Внедрение вируса в середину файла

Существует несколько возможностей внедрения вируса в середину файла.

В наиболее простом из них вирус *переносит часть файла в его конец* или *раздвигает файл* и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше.

Отдельные вирусы при этом сжимают переносимый блок файла так, что длина файла при заражении не изменяется.

Второй метод – *cavity*, при котором вирус записывается в заведомо неиспользуемые области файла.

Общая характеристика и классификация вредоносных программ

Вирусы без точки входа (ЕРО-вирусы – Entry Point Obscuring viruses)

Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко.

Перед тем как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать "правильный" адрес в файле – иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов.

Первый способ – поиск в файле последовательности стандартного кода Си/Паскаль. Эти вирусы ищут в заражаемых файлах стандартные заголовки процедур Си/Паскаль и записывают вместо них свой код.

Второй способ – трассировка или дизассемблирование кода файла. Такие вирусы загружают файл в память, затем трассируют или дизассемблируют его и в зависимости от различных условий выбирают команду (или команды), вместо которой записывается код перехода на тело вируса.

Третий способ применяется только резидентными вирусами – при запуске файла они контролируют какое-либо прерывание (чаще – INT 21h – сервисные функции DOS). Как только заражаемый файл вызывает это прерывание, вирус записывает свой код вместо команды вызова прерывания.

Общая характеристика и классификация вредоносных программ

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

Наиболее распространены компаньон-вирусы, использующие особенность DOS первым выполнять .com-файл, если в одном каталоге присутствуют два файла с одним и тем же именем, но различными расширениями имени – .com и .exe.

Некоторые вирусы используют не только вариант com-exe, но также и bat-com-exe.

Вторую группу составляют вирусы, которые при заражении переименовывают файл, давая ему какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла.

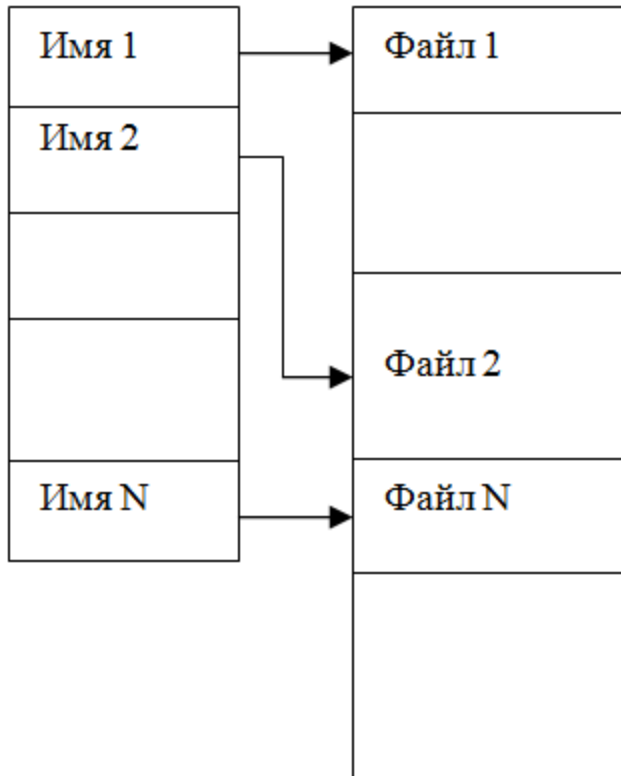
В третью группу входят так называемые Path-companion-вирусы, которые "играют" на особенностях PATH. Они либо записывают свой код под именем заражаемого файла, но "выше" на один уровень PATH (ОС, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву выше на один подкаталог и т. д.

Общая характеристика и классификация вредоносных программ

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

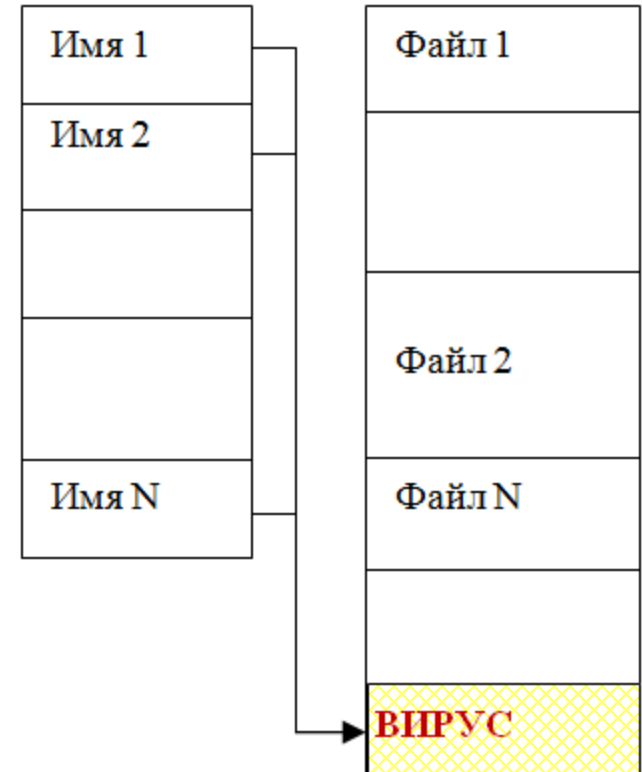
Сектор каталога

Диск



Сектор каталога

Диск



Общая характеристика и классификация вредоносных программ

Файловые черви (*worms*) являются в некотором смысле разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям "специальные" имена, чтобы подтолкнуть пользователя на запуск своей копии, например INSTALL.EXE или WINSTART.BAT.

Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

OBJ-, LIB-вирусы и вирусы в исходных текстах. Вирусы, заражающие obj- и lib-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл при этом не является выполняемым и не способен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится com- или exe-файл, получаемый в процессе компоновки зараженного obj/lib-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются obj/lib-файлы, на втором (компоновка) получается работоспособный вирус.

Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения.

Общая характеристика и классификация вредоносных программ

Загрузочные вирусы подразделяются на вирусы, заражающие:

- ✓ системный загрузчик, расположенный в загрузочном секторе дискет и логических дисков;
- ✓ внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

По степени и способу маскировки бывают:

- ✓ вирусы, не использующие средств маскировки;
- ✓ *stealth-вирусы* – вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных (они изменяют информацию таким образом, что файл появляется перед пользователем в незараженном виде, например, временно печат зараженные файлы);
- ✓ *вирусы-мутанты (MtE-вирусы)* – вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса. *MtE-вирусы делятся на:*
 - *обычные вирусы-мутанты*, в разных копиях которых различаются только зашифрованные тела, а расшифровщики совпадают;
 - *полиморфные вирусы*, в разных копиях которых различаются не только зашифрованные тела, но их дешифровщики.

Макровирусы. Макровирусы являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Для существования вирусов в конкретной системе необходимо наличие встроенного в систему макроязыка с возможностями:

- привязки программы на макроязыке к конкретному файлу;
- копирования макропрограмм из одного файла в другой;
- получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Общая характеристика и классификация вредоносных программ

Сетевые вирусы. К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

По деструктивным возможностям вирусы можно разделить на:

- ✓ безвредные, то есть никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- ✓ неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;
- ✓ опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- ✓ очень опасные – в алгоритм их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

Общая характеристика и классификация вредоносных программ

Сравнительная характеристика вредоносных программ для различных ОС

<i>Операционные системы</i>	<i>Всего</i>	<i>Backdoors, Hacktools, Exploits, Rootkits</i>	<i>Вирусы и черви</i>	<i>Трояны</i>	<i>Прочие</i>
Linux	1898	942 (50%)	136 (7%)	88 (5%)	732 (38%)
FreeBSD	43	33 (77%)	10 (23%)	0 (0%)	0 (0%)
Sun Solaris	119	99 (83%)	17 (15%)	3 (2%)	0 (0%)
Unix	212	76 (36%)	118 (56%)	3 (1%)	15 (7%)
OS X	48	14 (29%)	9 (19%)	11 (23%)	14 (29%)
Windows	2247659	501515 (22%)	40188 (2%)	1232798 (55%)	473158 (21%)

Общая характеристика и классификация вредоносных программ

Условно опасные программы

В настоящее время к условно опасным программам относят программы классов Riskware, Adware и Pornware.

Riskware

К классу программ Riskware относятся легальные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые, тем не менее, в руках злоумышленника способны причинить вред пользователю и его данным.

В списке программ класса Riskware можно обнаружить:

- ✓ легальные утилиты удаленного администрирования: программы-клиенты *IRC* (*Internet Relay Chat* – служба, позволяющая множеству людей беседовать в реальном масштабе времени путем набора сообщений на клавиатуре),
- ✓ *ISQ* (*Intelligent Call Query* – частная служба, принадлежащая компании AOL Time Warner - США),
- ✓ мониторы любой активности, утилиты для работы с паролями,
- ✓ многочисленные интернет-серверы служб FTP, Web, Proxy, Telnet и т.д.

Общая характеристика и классификация вредоносных программ

Adware

Рекламное программное обеспечение (*Adware, Spyware, Browser Hijackers*) предназначено для показа рекламных сообщений. Чаще всего они представляются в виде графических баннеров, рекламных веб-страниц, на которые осуществляется перенаправление поисковых запросов. За исключением показов рекламы, подобные программы, как правило, никак не проявляют своего присутствия в системе (отсутствует значок в системном трее, нет упоминаний об установленных файлах в меню программ). Зачастую у *Adware*-программ нет процедуры деинсталляции.

На компьютеры пользователей Adware попадает двумя способами:

- ✓ путем встраивания рекламных компонентов в бесплатное и условно-бесплатное программное обеспечение (*freeware, shareware*);
- ✓ путем несанкционированной установки рекламных компонентов при посещении пользователем "зараженных" веб-страниц.

Определенное количество рекламных систем помимо доставки рекламы также собирают конфиденциальную 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.