KASPERSKY lab

В.А. Гинодман, Н.В. Обелец, А.А. Павлов

От первых вирусов до целевых атак

Москва 2014

Министерство образования и науки Российской Федерации

Национальный исследовательский ядерный университет «МИФИ»

В.А. Гинодман, Н.В. Обелец, А.А. Павлов

От первых вирусов до целевых атак

Учебное пособие

Москва 2014

УДК 004.056.53(075)+004.056.54(075)
ББК 32.973-018.2я7
П 12

Гинодман В.А., Обелец Н.В., Павлов А.А. **От первых вирусов до целевых атак**: Учебное пособие [Электронный ресурс]. М.: НИЯУ МИФИ, 2014. – 96 с.

Один из важнейших приоритетов в работе «Лаборатории Касперского» – просветительская деятельность в области информационной безопасности.

Предлагаемое учебное пособие открывает серию руководств Департамента образовательных инициатив ЗАО «Лаборатория Касперского» по программе «Информационная безопасность», цель которой – повышение общего уровня знаний пользователей в этой области.

В пособии повествуется об истории вредоносного программного обеспечения, приведен обзор его типологии. Описаны технологии детектирования вредоносных и потенциально нежелательных программ. Рассказывается также о наиболее опасных и совершенных современных компьютерных угрозах в контексте целевых атак и кибершпионажа.

Рецензенты: канд. техн. наук В.С. Горбатов, канд. техн. наук В.А. Петров

ISBN 978-5-7262-1968-4

Редактор *Е.Г. Станкевич*
Оригинал-макет изготовлен *С.В. Тялиной*

Подписано в печать 07.06.2014. Формат 60×84 1/8.
Уч.-изд.л. 12,0. Печ.л. 12,0. Изд. № 007-3.
Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское ш., 31.

Оглаление

Введение

Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер. В этом смысле XXI век нередко называют веком информации.

Вместе с тем можно отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека в частности. Именно поэтому в последнее время появились такие термины, как «информационная политика», «информационная безопасность», «информационная война» и целый ряд других новых понятий, в той или иной мере связанных с информацией.

Информационная безопасность – одна из главных проблем, с которой сталкивается современное общество. Причиной ее обострения является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

Примечательно, что еще в 1988 году известный программист Питер Нортон высказался резко против существования вирусов. Он официально объявил их несуществующим мифом и сравнил со сказками о крокодилах, живущих в канализации Нью-Йорка. В целом в 1980-х, да во многом и в 1990-х годах прошлого века угроза, которую может нести в себе вредоносное программное обеспечение (ПО), недооценивалась.

Одним из знаковых событий, которое помогло многим осознать масштабность угрозы, стало распространение сетевого червя Slammer в 2003 году. Этому вредоносному ПО удалось на 12 часов отключить от Интернета крупное и экономически развитое государство – Южную Корею.

О масштабах угрозы говорит также тот факт, что в середине 1990-х годов один новый вирус появлялся в среднем за один час, в середине 2000-х – уже каждую минуту, в настоящее время – каждую секунду. С таким потоком вредоносного ПО силами только лишь антивирусных аналитиков справиться уже невозможно, поэтому на современном этапе для борьбы с вирусами активно используют мощные компьютеры и специальное ПО, и только наиболее важные и сложные угрозы анализируются в «ручном» режиме.

Решение проблемы информационной безопасности связано с гарантированным обеспечением трех ее главных составляющих: доступности, целостности и конфиденциальности информации. В то же время исключительно важным, если не ключевым, аспектом информационной безопасности является компьютерная безопас-

ность, достижение которой невозможно без хорошего знания и понимания угроз, которые несет с собой вредоносное программное обеспечение.

Одно из важных направлений деятельности «Лаборатории Касперского» – просветительская деятельность в области информационной безопасности. В образовательной сфере наша компания сотрудничает с крупнейшими высшими учебными заведениями Российской Федерации (МГУ им. М.В. Ломоносова, НИЯУ МИФИ, МГТУ им. Н.Э. Баумана и др.).

Настоящее учебное пособие является первым в серии учебных пособий «Лаборатории Касперского» по учебной программе «Информационная безопасность». Цель данной программы – повышение общего уровня знаний пользователей по информационной безопасности.

При написании настоящего учебного пособия авторы ставили перед собой цель дать общее представление о предмете, рассказать об истории вредоносного ПО, представить обзор технологий детектирования вредоносных и потенциально нежелательных программ и рассказать о наиболее опасных и совершенных современных компьютерных угрозах в контексте целевых атак, кибершпионажа и использования кибероружия.

Пособие рассчитано на широкую аудиторию читателей и не предполагает для своего изучения специальной подготовки.

При составлении учебного пособия существенно использовались источники [LK09], [KL_Main], [KL_SecL], [KL_Blog].

Глава 1. Типы вредоносных программ

В данной главе будут разобраны основные типы и подтипы вредоносных программ, рассказано об их функционале и основных особенностях. При этом авторы не претендуют на исчерпывающее описание всех разновидностей встречающегося в информационном мире вредоносного ПО.

Будет также рассмотрен вопрос о классификации вредоносного ПО, о котором полезно иметь представление, в первую очередь, в историческом ракурсе. Дело в том, что с каждым годом вредоносное ПО становится всё более сложным и всё более многофункциональным. Согласно правилу «поглощения типов» при именовании вредоносного ПО более сложный функционал «поглощает» более простой. Таким образом, границы между различными типами вредоносного ПО в наше время все более стираются.

При написании главы существенно использованы материалы раздела [KL_SecL_7].

Вредоносные программы

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы, черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.).

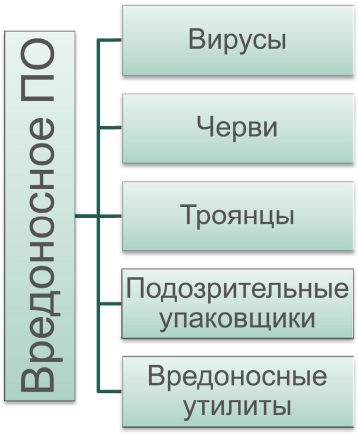


Рис. 1.1

Фундаментальное отличие вирусов и компьютерных червей от троянских программ в том, что вирусы и компьютерные черви обладают способностью к саморазмножению, а троянские программы – нет. В свою очередь вирусы отличаются от компьютерных червей по способу саморазмножения. Вирусы для этой цели используют локальные ресурсы компьютера, в то время как компьютерные черви саморазмножаются с помощью сетевых ресурсов.

Троянские программы

Этот тип вредоносного ПО, в отличие от компьютерных вирусов и червей, неспособен к самовоспроизведению.

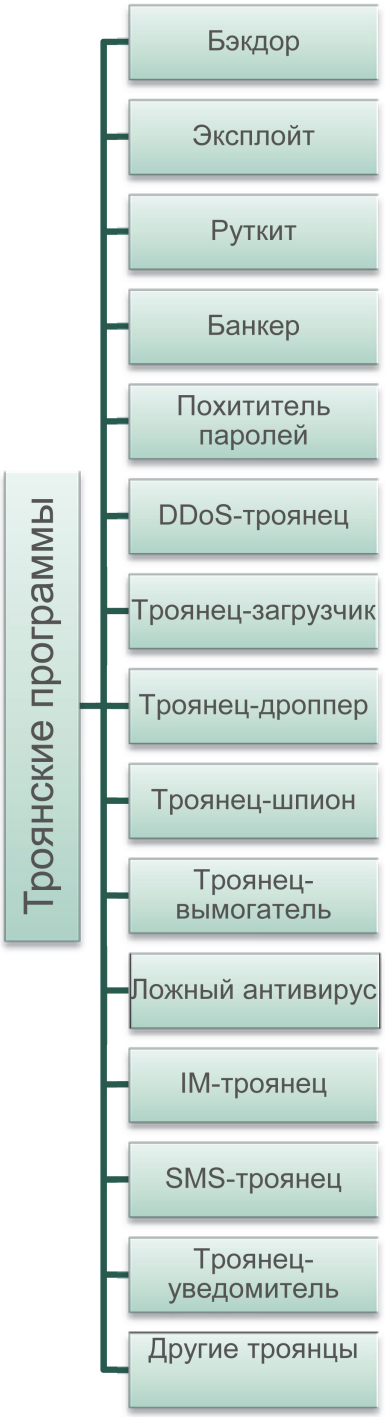


Рис. 1.2

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для DDoS-атак на удаленные ресурсы сети).

Основным признаком, по которому различают подтипы троянских программ, являются их несанкционированные пользователем действия – те, которые они производят на зараженном компьютере.

Бэкдор (Backdoor)

Вредоносная программа, предназначенная для скрытого удаленного управления злоумышленником пораженным компьютером. По своей функциональности бэкдоры во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов.

Эти вредоносные программы позволяют делать с компьютером всё, что в них заложил 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 ботнеты – сети зараженных вредоносным ПО компьютеров, централизованно управляемые злоумышленниками в злонамеренных целях.

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 компьютерные черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Эксплойт (Exploit)

Программа, в которой содержатся данные или исполняемый код, позволяющие использовать 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, заражение всех посетителей взломанного веб-сайта вредоносной программой). Также эксплойты интенсивно используются программами типа Net-Worm для проникновения на компьютер-жертву без участия пользователя.

Руткит (Rootkit)

Программа, предназначенная для сокрытия в системе определенных объектов либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти зараженного компьютера, вредоносная сетевая активность.

Сам по себе Руткит ничего вредоносного не делает, но данный тип программ в подавляющем большинстве случаев используется вредоносными программами для затруднения собственного обнаружения.

Банкер (Trojan-Banker)

Вредоносная программа, предназначенная для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт. Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы.

Похититель паролей (Trojan-PSW)

Вредоносная программа, предназначенная для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров. Название PSW произошло от Password-Stealing-Ware.

При запуске PSW-троянцы ищут необходимую им информацию в системных файлах, хранящих различную конфиденциальную информацию или в реестре. В случае успешного поиска программа отсылает найденные данные «хозяину». Для передачи данных могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы.

Некоторые троянцы данного типа воруют регистрационную информацию к различному программному обеспечению.

DDoS-троянец (Trojan-DDoS)

Вредоносная программа, предназначенная для проведения несанкционированной пользователем DoS-атаки с пораженного компьютера на компьютер-жертву по заранее определенному адресу.

Суть атаки сводится к посылке жертве многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого удаленного компьютера недостаточны для обработки всех поступающих запросов.

Часто для проведения распределенной DoS-атаки (DDoS-атаки) злоумышленники предварительно заражают троянцами данного типа множество компьютеров (например, в ходе массированной спам-рассылки), после чего каждый из зараженных компьютеров атакует заданную жертву.

Троянец-загрузчик (Trojan-Downloader)

Вредоносная программа, предназначенная для несанкционированной пользователем 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 регистрируются троянцем на автозагрузку в соответствии с возможностями операционной системы.

Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» интернет-ресурса (обычно, с веб-страницы).

Данный тип вредоносных программ часто используется для первоначального заражения посетителей веб-страниц, содержащих эксплойты.

Троянец-дроппер (Trojan-Dropper)

Вредоносная программа, предназначенная для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев.

Данный тип вредоносных программ обычно без каких-либо сообщений (либо 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.

В результате использования программ данного класса злоумышленники достигают двух целей:

- скрытной инсталляции троянских программ и вирусов;
- защиты от детектирования известных вредоносных программ антивирусами, поскольку не все из них в состоянии проверить все компоненты внутри подобных троянцев.

Троянец-шпион (Trojan-Spy)

Вредоносная программа, предназначенная для ведения электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т.д.). Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы.

Троянец-вымогатель (Trojan-Ransom)

Вредоносная программа, предназначенная для несанкционированной пользователем модификации данных на компьютере-жертве таким образом, чтобы сделать невозможным работу с ними либо блокировать нормальную работу компьютера. После того как данные «взяты в заложники» (блокированы), пользователю выдвигается требование выкупа.

Озвученную в требовании сумму жертва должна передать злоумышленнику, после чего злоумышленник обещает выслать программу для восстановления данных или нормальной работоспособности компьютера.

Ложный антивирус (Trojan-FakeAV)

Класс вредоносных программ, имитирующих работу антивирусного программного обеспечения или защитных компонентов операционной системы с целью получения от пользователя вознаграждения за обнаружение и удаление несуществующих угроз. Такие программы показывают множество нежелательных уведомлений, создают дискомфорт, стимулируя пользователя внести оплату. Иногда препятствуют нормальной работе компьютера, но, как правило, не блокируют систему полностью, чтобы не утратить доверие жертвы.

IM-троянец (Trojan-IM)

Вредоносная программа, предназначенная для кражи пользовательских аккаунтов (логин и пароль) от интернет-пейджеров (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.).

Найденная на зараженном компьютере информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, WWW (посредством указания данных в запросе) и другие способы.

SMS-троянец (Trojan-SMS)

Вредоносная программа, предназначенная для несанкционированной пользователем отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые записаны в теле вредоносной программы.

Троянец-уведомитель (Trojan-Notifier)

Вредоносная программа, предназначенная для несанкционированного пользователем сообщения своему «хозяину» 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 веб-странице злоумышленника, ICQ-сообщением.

Данные троянские программы используются в многокомпонентных троянских наборах для извещения злоумышленника об успешной инсталляции вредоносных программ в атакуемой системе.

Другие троянцы

Перечислим кратко, какие еще существуют типы троянцев.

Trojan-ArcBomb

Эти троянцы представляют собой архивы, специально сформированные 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 – в этом случае «архивная бомба» может остановить работу сервера.

Trojan-Clicker

Вредоносная программа, предназначенная для несанкционированного пользователем обращения к интернет-ресурсам (обычно, к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файл hosts в MS Windows).

Trojan-GameThief

Вредоносные программы, предназначенные для кражи пользовательской информации, относящейся к сетевым играм.

Trojan-Proxy

Вредоносные программы, предназначенные для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным интернет-ресурсам через компьютер-жертву.

Trojan-Mailfinder

Вредоносная программа, предназначенная для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими способами.

Trojan

Троянская программа, не принадлежащая ни к одному из перечисленных подтипов троянских программ, или многоцелевая троянская программа, способная совершать сразу несколько несанкционированных пользователем действий, присущих одновременно нескольким другим поведениям троянских программ, что не позволяет однозначно отнести ее к тому или иному подтипу.

Вирусы

Определение вируса по ГОСТ Р 51188-98 звучит так.

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Однако мы, как это принято при детектировании вредоносных объектов, будем различать способ самораспространения вредоносных программ и будем понимать термин «вирус» в более узком значении. Примем следующее определение.

Вирус – это вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компью–тера.

Вредоносные же программы, которые для своего саморазмножения используют сетевые ресурсы, будем относить к типу компьютерных червей.

Таким образом, 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.

Компьютерные черви

К данной категории относятся программы, распространяющие свои копии по локальным и (или) глобальным сетям.

Большинство известных сетевых червей распространяются в виде файлов: вложений в электронные письма, ссылкой на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и пр.

Некоторые сетевые черви (так называемые бесфайловые или пакетные) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии компьютерные черви используют различные методы социальной инженерии (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

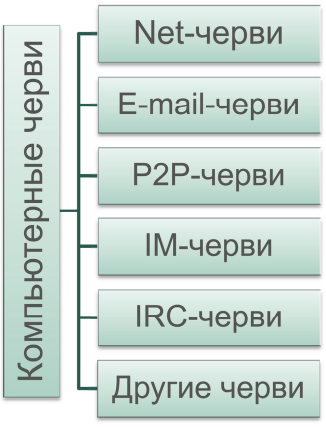


Рис. 1.3

Основной признак, по которому различают типы (поведения) компьютерных червей, – способ их распространения, т.е. то, как вредоносная программа передает свою копию по сетевым ресурсам.

Net-черви (Net-Worm)

Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения вредоносной программы по сети (т.е. непосредственно для активации вредоносной программы).

Зачастую при распространении такой червь ищет в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально сформированный сетевой пакет (эксплойт), в результате чего код (или часть кода) червя проникает на компьютер-жертву и активируется. Если сетевой пакет содержит только часть кода червя, то после проникновения в уязвимый компьютер он скачивает основной файл червя и запускает его на исполнение.

Email-черви (Email-Worm)

Вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению по каналам электронной почты. В процессе размножения 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 веб-сайте).

В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором – при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков – активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены:

- прямое подключение к SMTP-серверу с использованием встроенной в код червя почтовой библиотеки;
- использование сервисов MS Outlook;
- использование функций Windows MAPI[1].

[1] MAPI (Messaging Application Programming Interface) – программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви могут:

- рассылать себя по всем адресам, обнаруженным в адресной книге MS Outlook;
- считывать адреса из адресной базы WAB[2];
- сканировать «подходящие» файлы на диске и выделять в них строки, являющиеся адресами электронной почты;
- отсылать себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты.

P2P-черви (P2P-Worm)

Вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению по каналам файлообменных пиринговых[3] сетей.

Механизм работы большинства подобных червей достаточно прост – для внедрения в P2P-сеть компьютерному 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.

IM-черви (IM-Worm)

Вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению по каналам систем мгновенного обмена сообщениями (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.).

---

[2] WAB (Windows Address Book) – адресная книга Windows.

[3] Пиринговая сеть (от англ. peer-to-peer, P2P – равный к равному) – это компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и выполняет функции сервера [Wik].

Для этих целей компьютерные черви, как правило, рассылают на обнаруженные контакты (из контакт-листа) сообщения, содержащие URL на файл с телом червя, расположенный на каком-либо сетевом ресурсе. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

IRC-черви (IRC-Worm)

Вредоносные программы, обладающие способностью к несанкционированному пользователем саморазмножению через Internet Relay Chats (IRC).

У этого типа червей существует два способа распространения по IRC-каналам, напоминающие способы распространения почтовых червей. Первый способ 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).

Другие черви (Worm)

К данному подтипу относятся компьютерные черви, которые по тем или иным причинам не обладают ни одним из поведений других подтипов компьютерных червей.

Подозрительные упаковщики (SuspiciousPacker)

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.

Также при упаковке файлов может использоваться сразу несколько упаковщиков, или использоваться редко встречающийся упаковщик.

Вредоносные утилиты

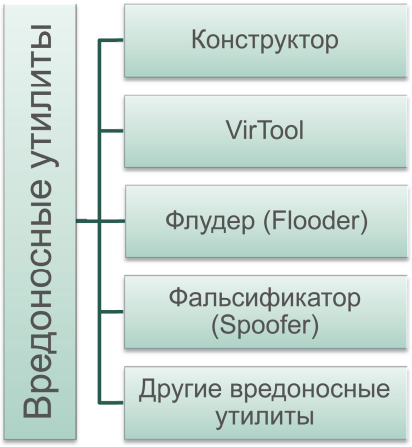


Рис. 1.4

Вредоносные программы, разработанные для автоматизации создания других 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 данной категории не представляют угрозы непосредственно компьютеру, на котором исполняются.

Основным признаком, по которому различают вредоносные утилиты, являются совершаемые ими действия.

К данной категории вредоносных программ относятся следующие поведения:

Конструктор (Constructor)

Программы, предназначенные для изготовления новых компьютерных вирусов, червей и троянских программ. Подобные программы позволяют генерировать исходные тексты вредоносных программ, объектные модули и непосредственно зараженные файлы.

Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вредоносной программы, наличие или отсутствие самошифрования, противодействие отладчику и т.п.

Первый конструктор вирусов VCL (Virus Creation Laboratory), представляющий собой графическую среду для разработки вирусов и различных троянских программ для MS DOS, появился в июле 1992 года.

VirTool

Программы, позволяющие злоумышленнику модифицировать другие вредоносные программы таким образом, чтобы они не детектировались антивирусным программным обеспечением.

Флудер (Flooder)

Программы, функцией которых является «забивание» информационным мусором (бесполезными сообщениями) сетевых каналов, интернет-пейджеров и SMS-каналов.

Данные программы могут использоваться спамерами.

Фальсификатор (Spoofer)

«Spoofer» в переводе с английского означает «злоумышленник, выдающий себя за законного пользователя». К этому подтипу относятся программы, позволяющие отправлять сообщения и сетевые запросы с поддельным адресом отправителя.

Утилиты данного типа могут быть использованы для того, чтобы затруднить обнаружение отправителя или выдать сообщение злоумышленника за сообщение, отправленное другим пользователем.

Другие вредоносные утилиты

Перечислим, какие еще существуют типы вредоносных утилит.

Ложная тревога (Hoax)

Программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен или будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. Программы этого типа могут, например, сообщать пользователю о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводить странные вирусоподобные сообщения и т.д.

DoS

Программа, предназначенная для проведения DoS-атаки с ведома пользователя на компьютер-жертву.

HackTool

Программы, используемые злоумышленниками при организации атак на локальный или удаленный компьютер. Они могут осуществлять несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы, очищать системные журналы с целью сокрытия следов присутствия в системе вредоносного ПО, анализировать сетевой трафик и т.д.

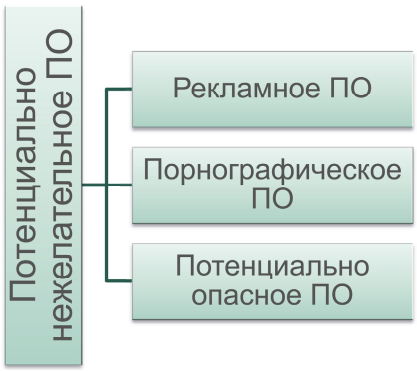


Рис. 1.5

Потенциально нежелательное ПО

Потенциально нежелательное ПО включает в себя программы, которые невозможно однозначно отнести ни к опасным, ни к безопасным. Дело в том, что некоторые программы обладают функциями, которые могут причинить вред пользователю, но только при выполнении ряда условий.

Например, если программа удаленного администрирования установлена на компьютер пользователя системным администратором, то ничего страшного в этом нет, так как программа всего лишь помогает администратору удаленно решать возникающие у пользователя проблемы. Но если та же программа установлена на компьютер пользователя злоумышленником, то он фактически получает полный контроль над компьютером-жертвой и в дальнейшем может использовать его по своему усмотрению. Таким образом, подобные программы могут быть использованы как во благо, так и во вред – в зависимости от того, в чьих руках они находятся.

Антивирусные продукты «Лаборатории Касперского» предоставляют пользователям решение вопроса о том, что делать с подобными программами. Этот тип программ детектируется антивирусом Касперского опционально, в случае осознанного выбора со стороны пользователя.

Если обнаруженные на своём компьютере потенциально нежелательные программы вам знакомы, и вы абсолютно уверены в том, что они не причинят вреда вашим данным, то можно либо отключить детектирование потенциально нежелательных программ, либо добавить конкретные программы в список «исключений» антивируса.

В настоящее время к потенциально нежелательным программам «Лаборатория Касперского» относит программы классов Рекламное ПО (Adware), Порнографическое ПО (Pornware) и Потенциально опасное ПО (Riskware).

Рекламное ПО (Adware)

Это программное обеспечение, предназначенное для показа рекламных сообщений (чаще всего в виде графических баннеров); перенаправления поисковых запросов на рекламные веб-страницы, а также для сбора данных маркетингового характера об активности пользователя, позволяющих сделать рекламу более таргетированной.

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. Часто у Adware-программ нет процедур деинсталляции, используются пограничные с вирусными технологии, позволяющие скрытно внедряться на компьютер пользователя и незаметно осуществлять на нем свою деятельность.

Проникновение

На компьютеры пользователей Рекламное ПО чаще всего попадает двумя способами:

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

- путем несанкционированной пользователем установки рекламных компонентов при посещении пользователем «зараженных» веб-страниц.

Большинство программ freeware и shareware прекращает показ рекламы после их покупки или регистрации. Подобные программы часто используют встроенные Adware-утилиты сторонних производителей. В некоторых случаях эти Adware-утилиты остаются установленными на компьютере пользователя и после регистрации программ, с которыми они изначально попали в операционную систему. При этом удаление Adware-компонента, всё еще используемого какой-либо программой для показа рекламы, может привести к сбоям в функционировании этой программы.

В случае установки рекламных компонентов при посещении пользователем «зараженных» веб-страниц в большинстве случаев применяют хакерские технологии: проникновение в компьютер через уязвимости системы безопасности интернет-браузера, а также использование троянских программ, предназначенных для скрытной установки программного обеспечения (Trojan-Downloader или Trojan-Dropper). Рекламное ПО, действующее подобным образом, часто называют Browser Hijackers[4].

Доставка рекламы

Известны два основных способа доставки рекламной информации:

- скачивание рекламных текстов и изображений с веб- или FTP-серверов, принадлежащих рекламодателю;
- перенаправление поисковых запросов интернет-браузера на рекламный веб-сайт.

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

Сбор данных

Многие рекламные системы, помимо доставки рекламы, 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.

[4] «Hijacker» в переводе с английского – «бандит», «налетчик».

Примечание: не стоит путать Рекламное ПО, занимающееся сбором информации, с троянскими шпионскими программами. Его отличие состоит в том, что оно осуществляет подобный сбор с согласия пользователя.

Если Рекламное ПО никак не уведомляет пользователя об осуществляемом им сборе информации, то оно подпадает под поведение «Троянец-шпион» (Trojan-Spy) и относится к категории вредоносных программ.

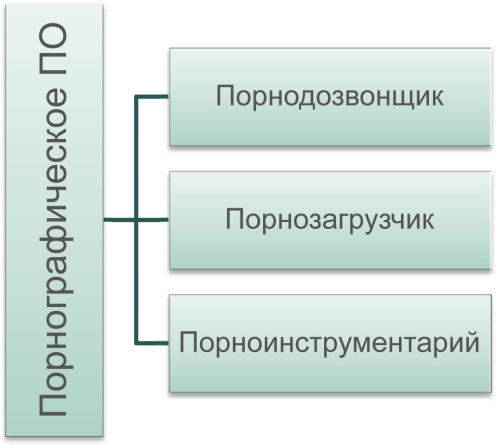


Рис. 1.6

Порнографическое ПО (Pornware)

К «Порнографическому ПО» относятся программы, которые так или иначе связаны с показом пользователю информации порнографического характера.

Программы категории «Порнографическое ПО» могут быть установлены пользователем на свой компьютер сознательно, с целью поиска и получения порнографической информации. В этом случае они не являются вредоносными.

С другой стороны, те же самые программы могут быть установлены на пользовательский компьютер злоумышленниками – через использование уязвимостей операционной системы и интернет-браузера или при помощи вредоносных троянских программ классов «Троянец-загрузчик» (Trojan-Downloader) или «Троянец-дроппер» (Trojan-Dropper). Делается это обычно с целью рекламы платных порнографических сайтов и сервисов.

К категории программ «Порнографическое ПО» (Pornware) относят:

порнодозвонщик (Porn-Dialer)

Программы, дозванивающиеся до порнографических телефонных служб, параметры которых сохранены в теле этих программ.

Отличие от вредоносных скрытых программ дозвона состоит в том, что пользователь уведомляется программой о совершаемых ею действиях.

порнозагрузчик (Porn-Downloader)

Программы, выполняющие загрузку из сети на компьютер пользователя данных порнографического характера.

Отличие от вредоносных программ загрузки состоит в том, что пользователь уведомляется программой о совершаемых ею действиях.

порноинструментарий (Porn-Tool)

Программы, так или иначе связанные с поиском и показом порнографических материалов (например, специальные панели инструментов для интернет-браузера и особые видеоплееры).

Потенциально опасное ПО (Riskware)

К этой категории относят обычные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые, тем не менее, в руках злоумышленника способны причинить вред пользователю (вызвать уничтожение, блокирование, модификацию или копирование информации, нарушить работу компьютеров или компьютерных сетей).

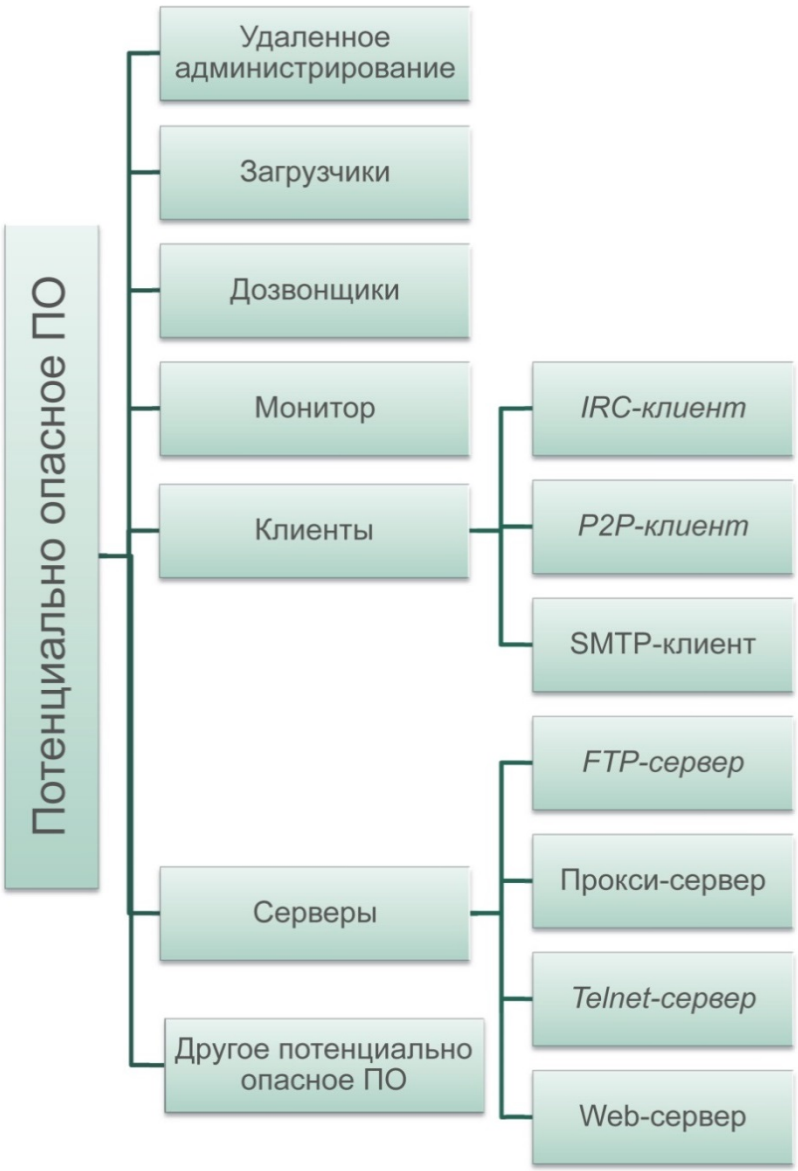


Рис. 1.7

В списке программ категории «Потенциально опасное ПО» можно обнаружить коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки («скачивания») 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, которым могут воспользоваться злоумышленники для причинения вреда пользователям.

У вас нет повода для беспокойства, если подобная программа установлена на компьютер вами или вашим сетевым администратором.

К этой категории детектируемых объектов относят:

Удаленное администрирование (RemoteAdmin)

Программы, используемые для удаленного управления компьютером. Вредоносными не являются. Будучи установленными злоумышленником, дают ему возможность полного контроля над компьютером-жертвой.

Загрузчики (Downloader)

Программы, позволяющие осуществлять в скрытом режиме загрузку различного контента с сетевых ресурсов. Вредоносными не являются. Подобные программы могут использоваться злоумышленниками для загрузки вредоносного контента на компьютер-жертву.

Дозвонщики (Dialer)

Программы, позволяющие устанавливать в скрытом режиме телефонные соединения через модем. Вредоносными не являются.

Монитор (Monitor)

Программы, содержащие функции наблюдения за активностью на компьютере пользователя (активные процессы, сетевая активность и т.д.).

Клиенты

- *IRC-клиент (Client-IRC)*
  Программы, используемые для общения в Internet Relay Chats (IRC). Вредоносными не являются. Детектирование добавлено по причине частого использования злоумышленниками расширенного функционала этих программ – с завидной периодичностью обнаруживаются вредоносные программы, устанавливающие Client-IRC на пользовательские компьютеры со злонамеренными целями.

- *P2P-клиент (Client-P2P)*
  Программы, используемые для работы в peer-to-peer сетях. Вредоносными не являются. Детектирование добавлено по просьбам пользователей, поскольку ряд программ подобного рода стал причиной утечки конфиденциальной информации.

- *SMTP-клиент (Client-SMTP)*
  Программы, используемые для отправки электронной почты и имеющие скрытый режим работы. Вредоносными не являются. Эти программы могут включаться злоумышленниками в состав пакета вредоносных программ для рассылки спама или иного вредоносного контента с компьютеров пользователей.

Серверы

- *FTP-сервер (Server-FTP)*
  Программы, содержащие функциональность 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.

- *Прокси-сервер (Server-Proxy)*
  Программы, содержащие функциональность 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.

- *Telnet-сервер (Server-Telnet)*
  Программы, содержащие функциональность 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.

- *Web-сервер (Server-Web)*
  Программы, содержащие функциональность веб-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.

Другое потенциально опасное ПО

Существует много других разновидностей потенциально опасного ПО. Упомянем некоторые из них:

PSWTool

Программы, позволяющие просматривать или восстанавливать забытые (часто – скрытые) пароли.

FraudTool

Программы, которые выдают себя за другие программы, хотя таковыми не являются. Часто предлагают пользователю перечислить финансовые средства на определенные счета для оплаты «услуг».

NetTool

Программы, обладающие различной сетевой функциональностью (например, удаленная перезагрузка компьютера, сканирование открытых сетевых портов, удаленный запуск произвольных приложений и т.д.). Вредоносными не являются.

WebToolbar

Панели инструментов расширяют возможности пользовательского программного обеспечения и устанавливаются с разрешения пользователя. Вредоносными не являются.

Правила «поглощения типов»

В предыдущих разделах были описаны основные типы и подтипы вредоносных программ. Однако с каждым годом вредоносное ПО становится всё более сложным и многофункциональным и всё чаще встречается ситуация, когда вредоносной программе присущи черты сразу нескольких типов как вредоносных функций, так и способов распространения программы.

В таких случаях для классификации вредоносных программ используют так называемые правила «поглощения типов», которые позволяют однозначно отнести вредоносную программу к тому или иному типу (поведению) вне зависимости от реализованной в ней функциональности.

Правила поглощения относятся только к вредоносным программам и не затрагивают потенциально нежелательное ПО.

Как работают правила поглощения? Каждому поведению вредоносной программы присваивается определенный уровень опасности, и менее опасные поведения поглощаются более опасными.

Правила поглощения для всех имеющихся типов вредоносных программ основываются на иерархической таблице, представленной на рис. 1.8.

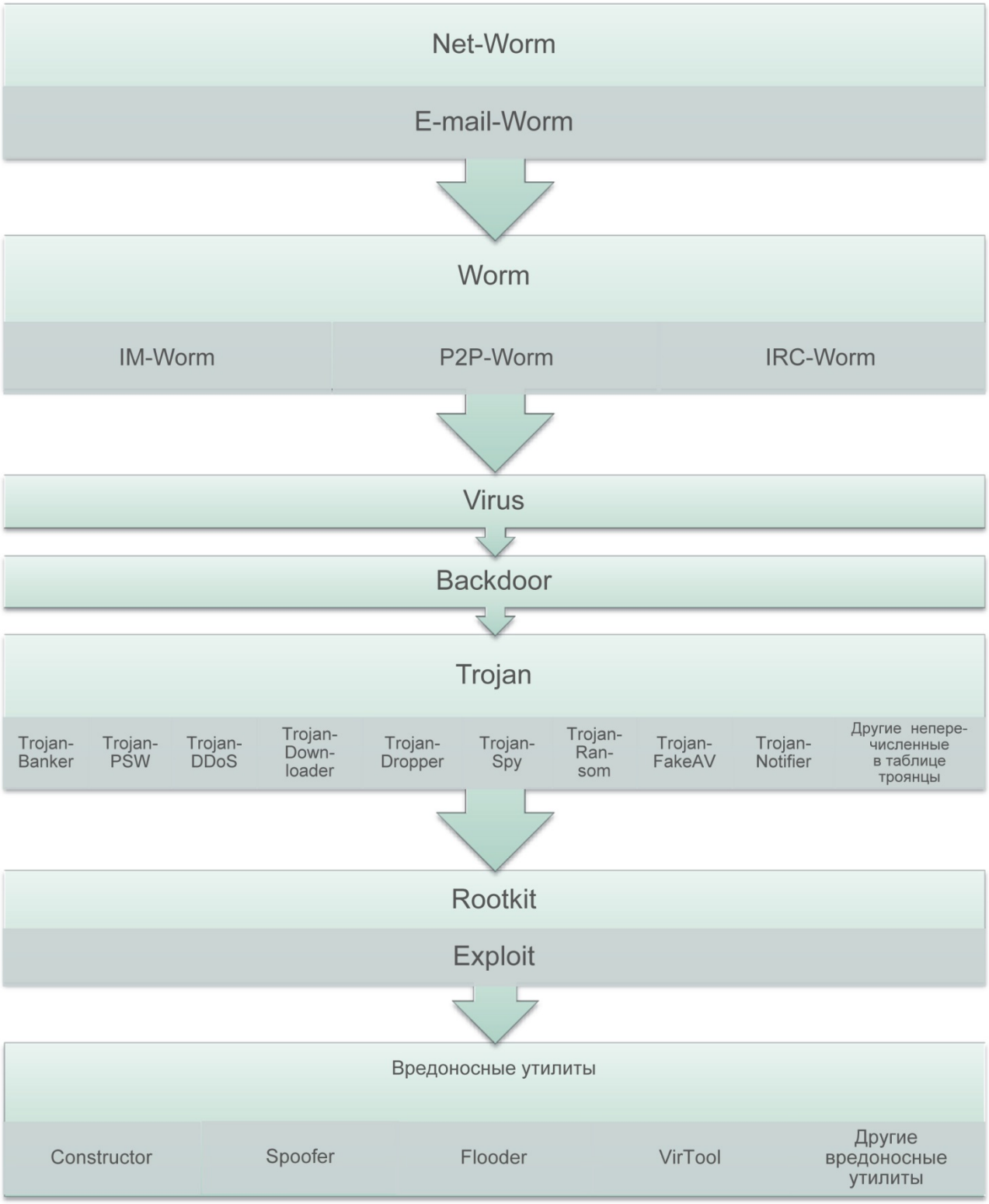


Рис. 1.8. Правила поглощения

Наименее опасные поведения расположены внизу, наиболее опасные – вверху.

В случае обнаружения у вредоносной программы нескольких поведений, ей присваивается наиболее опасное из них. Если вредоносная программа обладает несколькими равнозначными поведениями (например, Trojan-Downloader и Trojan-Dropper), то для такой программы выбирается вышестоящее (объединяющее) поведение.

Так, если вредоносная программа содержит два или более функционалов с равнозначным уровнем опасности, которые могут быть отнесены к Trojan-Ransom, Trojan-ArcBomb, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-IM, Trojan-Notifier, Trojan-Proxy, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-GameThief, Trojan-PSW или Trojan-Banker, то данная вредоносная программа относится к типу Trojan.

Если вредоносная программа содержит два или более функционалов с равнозначным уровнем опасности, которые могут быть отнесены к IM-Worm, P2P-Worm или IRC-Worm, то такая вредоносная программа относится к типу Worm.

Для того чтобы проиллюстрировать работу правил «поглощения типов», рассмотрим некую вредоносную программу, распространяющуюся по электронной почте в виде вложений и через P2P-сети в виде файлов. В дополнение к этому «зловред» содержит функцию несанкционированного пользователем сбора адресов электронной почты с пораженных компьютеров. Таким образом, вредоносная программа имеет черты Email-Worm, P2P-Worm и Trojan Mailfinder. Однако самым опасным из этих поведений является поведение Email-Worm, поэтому, согласно правилам «поглощения типов», рассматриваемая вредоносная программа будет отнесена именно к этому типу.

Правила именования детектируемых объектов

Необходимость создания классификации детектируемых объектов возникла одновременно с появлением первой антивирусной программы. Несмотря на то, что вирусов в то время было мало, их всё равно необходимо было как-то отличать друг от друга по названиям.

Пионеры антивирусной индустрии, как правило, использовали самую простую классификацию, состоящую из уникального имени вируса и размера детектируемого файла. Однако из-за того, что один и тот же вирус в разных антивирусных программах мог именоваться по-разному, началась путаница.

Первые попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века, в рамках альянса антивирусных специалистов CARO (Computer AntiVirus Researcher's Organization). Альянсом был создан документ «CARO malware naming scheme», который на какой-то период стал стандартом для индустрии.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема перестала быть эффективной. Еще более важной причиной отказа от нее стали существенные отличия в технологиях детектирования каждой антивирусной компании и, как следствие, невозможность унификации результатов проверки разными антивирусными программами.

Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов, однако они, по большей части, остаются безуспешными. Последним значительным проектом подобного рода было создание организации CME (Common Malware Enumeration), которая присваивает одинаковым детектируемым объектам единый уникальный идентификатор.

Используемая в «Лаборатории Касперского» система классификации детектируемых объектов, являющихся одной из наиболее широко распространенных в индустрии, послужила основой для классификаций некоторых других антивирусных компаний. В настоящее время классификация «Лаборатории Касперского» включает в себя весь объем детектируемых антивирусом Касперского вредоносных или потенциально нежелательных объектов и основана на разделении объектов по типу совершаемых ими на компьютере пользователей действий.

Для всех детектируемых антивирусными продуктами объектов используется следующая система именования:

Behavior.Platform.Name[.Variant]

Behavior определяет поведение детектируемого объекта. Для вирусов и червей поведение определяется по способу распространения; для троянских программ и вредоносных утилит – по совершаемым ими действиям; для потенциально нежелательного ПО – по функциональному назначению детектируемого объекта.

Platform – среда, в которой выполняется вредоносный или потенциально нежелательный программный код. Может быть как программной, так и аппаратной.

Для мультиплатформенных детектируемых объектов используется платформа с названием Multi. В качестве примера мультиплатформенной вредоносной программы можно привести Virus.Multi.Etapux, который заражает исполняемые файлы на операционных системах Windows и Linux.

Name – имя детектируемого объекта, позволяет выделять семейства детектируемых объектов.

Variant – модификация детектируемого объекта. Может содержать как цифровое обозначение версии программы, так и буквенное, начиная с «a»: «a» – «z», «aa» – «zz», ...

Variant не является обязательным в имени и может отсутствовать.

Приведем несколько примеров именования вредоносного ПО.

Пример 1. Trojan-PSW.Win32.Zbot

Zbot (или Zeus) – один из самых известных и самых опасных банковских троянцев. Trojan-PSW.Win32.Zbot – одна из разновидностей данного вредоносного ПО, которая специализируется на краже конфиденциальной информации и нацелена на компьютеры под управлением 32-разрядной ОС Windows.

Пример 2. Net-Worm.Linux.Ramen

Сетевой червь, заражающий системы под управлением ОС Linux. Имя детектируемого объекта – Ramen.

Это вредоносное ПО было обнаружено в начале 2001 года и представляло собой первого сетевого червя для некогда популярного дистрибутива системы Linux компании Red Hat.

Пример 3. Trojan-Spy.HTML.Fraud.gen

Эта троянская программа представляет собой поддельную HTML-страницу и предназначена для ведения электронного шпионажа за пользователем. Имя детектируемого объекта – Fraud, модификация – «gen».

Данный зловред рассылается по электронной почте под видом важного сообщения от крупных коммерческих банков, интернет-магазинов, софтверных компаний и т.д. Попадая по ссылке из письма на сайт, пользователь вводит свои учетные данные, после чего они пересылаются злоумышленникам, которые могут получить полный доступ к управлению конфиденциальной информацией пользователя.

Данная троянская программа на февраль 2014 года занимает первое место среди всех вредоносных программ, распространяющихся по почте [KL_SecL_12].

Пример 4. AdWare.Win32.IBryte.heur

Потенциально нежелательное рекламное ПО, которое работает под 32-раз–рядной ОС Windows. Имя детектируемого объекта – IBryte, спецификация – «heur».

Альтернативные классификации детектируемых объектов

Киберкриминал пребывает в непрекращающемся развитии, регулярно появляются новые угрозы, быстро развиваются наиболее прибыльные мошеннические схемы получения доходов.

По этой причине часто возникает необходимость выделить из всего многообразия детектируемых объектов одно или другое подмножество, характеризующее наиболее яркие и опасные тенденции развития вредоносных программ.

В классификации, описанной выше, черви и вирусы разделяются по способу распространения, остальные вредоносные программы – по совершаемым ими действиям. Но часто для того, чтобы выделить тот или иной тренд развития вредоносных программ, этих признаков бывает недостаточно, и тогда используются другие признаки классификации, позволяющие выделить необходимые поведения из многообразия детектируемых объектов.

Для удобства обозначения наиболее ярких, устоявшихся, опасных трендов последнего времени многие участники антивирусного рынка используют следующие категории:

- Crimeware
- Spyware
- Ransomware
- Bot-clients

Поговорим подробнее о каждой из этих категорий.

Crimeware

Crimeware – категория вредоносных программ, разработанных специально для автоматизации совершения финансовых преступлений.

Подобная автоматизация весьма многогранна. Это могут быть программы, отслеживающие появление на экране окна подключения к банковской системе с целью последующего перехвата вводимой в это окно секретной информации, а также 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, куда пароль был сохранен заранее.

Фантазия злоумышленников безгранична, и новые подходы получения доступа к счетам пользователей становятся всё более изощренными.

В качестве примеров семейств вредоносных программ категории Crimeware можно привести Trojan-Spy.Win32.Goldun, Trojan-Spy.Win32.Webmoner, всех представителей поведения Trojan-Banker и многие другие.

Наибольшее число представителей категории Crimeware относятся к Trojan-Banker и Trojan-Spy, но согласно правилам поглощения, функциональностью для автоматизации совершения финансовых преступлений могут обладать представители вышестоящих поведений, а именно: Trojan, Backdoor, Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, Net-Worm, хотя и значительно реже, чем представители Trojan-Banker и Trojan-Spy.

Spyware

Spyware – категория вредоносных программ, применяемых для несанкционированного пользователем слежения за его действиями и несанкционированного им сбора данных.

Это могут быть программы, записывающие все нажатые пользователем клавиши в лог-файл для последующей передачи сохраненной информации злоумышленнику, а также 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 Trojan-Spy и Trojan-PSW, а также все представители Trojan-GameThief, Trojan-IM, Trojan-Mailfinder, Trojan-Banker, Trojan-Notifier.

Trojan-Banker, относящийся к Crimeware, также относится и к Spyware в силу того, что представители этого поведения собирают данные о пользователе. В данном случае имеем пересечение подмножеств Crimeware и Spyware.

Trojan-Notifier также относится к Spyware, поскольку, согласно определениям, под эту категорию подпадают «...программы, применяемые для несанкционированного пользователем слежения за его действиями...», а Trojan-Notifier скрытно сообщают «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, Net-Worm.

Любые вредоносные программы, занимающиеся шпионской деятельностью, однозначно классифицируются как вредоносные, Adware же относятся к потенциально нежелательному ПО.

Ransomware

Ransomware – категория вредоносных программ, блокирующих данные или работоспособность компьютера-жертвы. Подобное поведение не санкционировано пользователем компьютера и используется вредоносной программой с целью дальнейшего требования выкупа у пользователя.

В качестве примеров семейств программ, относящихся к Ransomware, можно привести Trojan-Ransom.Win32.Gpcode и Trojan-Ransom.Win32.Krotten. Gpcode использует шифрование файлов, выбирая в качестве мишеней наиболее «ценные» данные – документы, базы данных и др., после чего показывает пострадавшим файл с указанием координат, где «помогут» восстановить данные. Krotten использует несколько иной подход, заключающийся в изменении системного реестра таким образом, чтобы с компьютером было невозможно работать. Восстановление работоспособности возможно после уплаты «выкупа».

К данной категории вредоносных программ в первую очередь относятся представители поведения Trojan-Ransom, но, согласно правилам поглощения, к категории Ransomware могут относиться представители вышестоящих поведений, а именно: Trojan, Backdoor, Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm, Net-Worm.

Bot-clients

Bot-clients – категория вредоносных программ, предназначенных для объединения пораженных компьютеров в бот-сети и позволяющих осуществлять удаленное централизованное управление всем множеством пораженных компьютеров для совершения злонамеренных действий без ведома пользователя. В качестве примера такого рода злонамеренных действий можно привести DDoS-атаки, осуществляемые против выбранной владельцем такой сети жертвы.

К категории Bot-clients в первую очередь относятся представители поведения Backdoor, но, согласно правилам поглощения, могут относиться и представители вышестоящих поведений, а именно: Virus, IM-Worm, P2P-Worm, IRC-Worm, Worm, Email-Worm и Net-Worm. Причем компьютерные черви достаточно часто имеют в своем составе функционал, позволяющий объединять зараженные компьютеры в бот-сети.

Контрольные вопросы

1. Дайте определения вируса, компьютерного червя, троянской программы.
2. В чем особенность троянской программы типа «бэкдор»?
3. В чем отличие между Net-, P2P- и IM-червями?
4. Приведите примеры потенциально опасного ПО.
5. Расскажите о правилах поглощения типов.
6. Поясните следующие примеры именования вредоносного ПО:
   - Trojan-Downloader.Java.Agent.lc,
   - Net-Worm.Win32.Kido.ih,
   - Trojan-Spy.HTML.Fraud.gen.

Глава 2. История развития вредоносного ПО

История появления и эволюции компьютерных вирусов, сетевых червей, троянских программ насчитывает более трех десятилетий. Зародившись в 1970-х годах как явление весьма необычное, как компьютерный феномен, примитивные вирусы постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети. Идея вируса, заражающего другие программы и компьютеры, за двадцать лет трансформировалась в криминальный бизнес. Будучи изначально творчеством вирусописателей-исследователей, компьютерные вирусы стали оружием в руках интернет-преступников.

Помимо интереса теоретического, история развития вирусов может принести и практическую пользу – по ней можно предсказывать будущее развитие вредоносных программ (например, дальнейшую эволюцию вирусов для мобильных устройств, угрозы для онлайн-банкинга и т.п.).

Сам термин «компьютерный вирус» был введен в 1983 году американским ученым Фредом Коэном (Fred Cohen) в его диссертационной работе, посвященной исследованию самовоспроизводящихся компьютерных программ [Coh83]. Известна даже точная дата – 3 ноября 1983 года, когда на еженедельном семинаре по компьютерной безопасности в Университете Южной Калифорнии (США) был предложен проект по созданию самораспространяющейся программы, которую тут же окрестили вирусом. Для ее отладки потребовалось 8 часов компьютерного времени на машине VAX 11/750 под управлением операционной системы Unix и ровно через неделю, 10 ноября, состоялась первая демонстрация. Через несколько лет Фредом Коэном по результатам этих исследований была опубликована работа «Computer Viruses: theory and experiments» [Coh87] с подробным описанием вопроса.

Строго говоря, вирусом называется вредоносное ПО, которое обладает способностью самораспространения посредством ресурсов локального компьютера. Но в более широком смысле слово «вирус» может использоваться как синоним термина «вредоносное ПО». В каком смысле мы используем в данной главе термин «вирус», будет ясно либо из контекста, либо мы будем явно уточнять этот момент.

Теоретические основы самораспространяющихся программ были заложены в 40-х годах прошлого столетия в трудах по изучению самовоспроизводящихся математических автоматов американского ученого Джона фон Неймана (John von Neumann), который также известен как автор базовых принципов работы современного компьютера. В 1951 году фон Нейманом был разработан метод, который демонстрировал возможность создания таких автоматов (см. [Neu66]).

В 1959 журнал «Scientific American» опубликовал статью Л.С. Пенроуза (L.S. Penrose) «Self-Reproducing Machines» [Pen59], посвященную самовоспроизво-

дящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый Ф.Ж. Шталь (F.G. Stahl) реализовал модель на практике с помощью машинного кода на IBM 650.

Далее мы даем краткий обзор истории вредоносного ПО, в которой предпринята попытка ее периодизации.

Первые вирусы (конец 1960-х – 1970-е)

Программы, о которых пойдет речь ниже, могут быть причислены к вредоносному ПО лишь с оговорками. Правильнее говорить о том, что в этих программах угадываются некоторые характерные черты, присущие вредоносам.

Creeper. В начале 1970-х годов в прототипе современного интернета – военной компьютерной сети ARPANET (от англ. Advanced Research Projects Agency Network) – была обнаружена программа Creeper (англ.: «тот, кто ползает»), которая перемещалась по серверам. Creeper был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. На зараженных системах программа обнаруживала себя сообщением: «I'M THE CREEPER: CATCH ME IF YOU CAN», которое выводилось на дисплей или принтер. Для удаления Creeper'а была написана программа Reeper, которая аналогичным образом распространялась по сети, удаляла обнаруженные копии Creeper и затем самоликвидировалась.

Pervading Animal (середина 1970-х) – так называлась первая известная вирус-игра для машины Univac 1108. С помощью наводящих вопросов программа пыталась определить имя животного, задуманного играющим. Благодаря наличию функции добавления новых вопросов, когда модифицированная игра записывалась поверх старой версии плюс копировалась в другие директории, через некоторое время диск становился переполненным.

Первые вирусные эпидемии (1981–1989)

Возможности первых вирусов были сильно ограничены малой функциональностью существующих на тот момент вычислительных машин. Только в конце семидесятых, вслед за выпуском очень успешного и массового поколения персональных компьютеров того времени – Apple II, и впоследствии IBM Personal Computer (1981 год), стали возможны вирусные эпидемии. Появление BBS (Bulletin Board System) – серверов общего доступа через коммутируемые телефонные сети – обеспечило быстрый обмен информацией между даже самыми отдаленными точками планеты. Сеть серверов BBS становится популярной и привлекает внимание программистов-вирусописателей. Появляется большое количество разнообразных

«троянцев» – программ, не имеющих способности к размножению, но при запуске наносящих системе вред.

Elk Cloner (1981) – первый документально зафиксированный компьютерный вирус, созданный неким Ричардом Скрента (Richard Skrenta) для ПК Apple II.

Вирус записывался в загрузочные секторы дискет, к которым обращалась ОС компьютера. Проявлял себя вирус весьма многосторонне: переворачивал изображение на экране, заставлял мигать текст, выводил сообщение:

ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!

Brain (1986). Зарегистрирована первая глобальная эпидемия вируса – он известен под именем «Brain» – для IBM-совместимых персональных компьютеров. Вирус был написан двумя братьями-программистами Баситом и Амжадом Фарук Алви (Basit и Amjad Farooq Alvi) из Пакистана. Согласно их собственному утверждению они написали Brain, прежде всего, с целью выявления уязвимостей в операционной системе DOS, а также для того, чтобы проследить географию перемещения программ, дискет и т.п. [YTb1]. Вирус заражал загрузочные сектора, менял метку диска на «(c) Brain» и оставлял сообщение с именами, адресом и телефоном авторов. В течение нескольких месяцев программа вышла за пределы Пакистана. Ничего деструктивного вирус не делал.

Virdem (1986). Немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к выполняемым MS-DOS-файлам формата COM. Опытный образец программы, получившей название Virdem, был продемонстрирован на форуме компьютерного андеграунда – Chaos Computer Club (декабрь 1986 года, Гамбург, ФРГ). По результатам исследований Бюргер выпустил книгу «Computer Viruses. The Disease of High Technologies» [Bur89], послужившую толчком к написанию тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи.

Lehigh (1987) – вредоносное ПО, вызвавшее эпидемию в Лехайском университете (США), где в то время работал Фред Коэн. Вредонос заражал только системные файлы COMMAND.COM и был запрограммирован на удаление всей информации на текущем диске. В течение нескольких дней было уничтожено содержимое со-

тен дискет из библиотеки университета и личных дискет студентов. Всего за время эпидемии было заражено около четырех тысяч компьютеров. Однако за пределы университета Lehigh не вышел.

Cristmas Tree (1987). Этот сетевой вирус распространял себя в операционной среде VM/CMS. 9-го декабря программа была запущена в сеть Bitnet в одном из университетов Западной Германии, проникла через шлюз в European Academic Research Network (EARN) и затем – в сеть IBM VNet. Через четыре дня (13 декабря) вредоносное ПО парализовало сеть – она была забита его копиями. При запуске программа выводила на экран изображение рождественской елочки и рассылала свои копии всем пользователям сети, чьи адреса присутствовали в соответствующих системных файлах NAMES и NETLOG.

Suriv (1987–1988). Действие резидентных файловых вирусов Suriv сводилось к загрузке кода в память компьютера, перехватывании файловых операций и заражении запускаемых пользователем COM- и (или) EXE-файлов.

Suriv-2 стал первым в истории вредоносным ПО, которое заражало EXE-файлы. Однако самой известной модификацией вредоноса стала версия Suriv-3, больше известная под именем «Jerusalem». Она была в состоянии заражать как EXE-, так и COM-файлы.

«Jerusalem» стал причиной глобальной вирусной эпидемии, первой настоящей пандемией, вызванной MS-DOS-вирусом. «Jerusalem» отличался от своих предшественников дополнительной деструктивной функцией – уничтожением всех запускаемых программ в пятницу, 13. Такой черной датой стало 13 мая 1988 года, когда в одночасье перестали работать компьютеры многих коммерческих фирм, государственных организаций и учебных заведений, в первую очередь Америки, Европы и Ближнего Востока. Название, кстати, вирус получил по месту одного из инцидентов – университета в Иерусалиме.

Первая известная вирусная мистификация. Псевдоним ее автора – Mike RoChenle. В октябре 1988 года он разослал на станции BBS большое количество сообщений о вирусе, который передается от модема к модему со скоростью 2400 бит/с. В качестве панацеи предлагалось перейти на использование модемов со скоростью 1200 бит/с. Как это ни смешно, многие пользователи действительно последовали этому совету.

Червь Морриса (1988). С ним связана первая эпидемия, вызванная сетевым червем. Программа, написанная аспирантом факультета Вычислительной техники Корнелльского университета (США) Робертом Т. Моррисом, использовала ошибки в системе безопасности операционной системы Unix для платформ VAX и Sun Microsystems. С целью незаметного проникновения в вычислительные системы использовался подбор паролей (из списка, содержащего 481 вариант). Это позволяло

маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы.

Червь Морриса заразил более 6000 компьютеров в США – по тем временам огромное число (около 10 % всех серверов в сети) – и практически парализовал их работу на срок до пяти суток. Среди жертв вируса был, например, Исследовательский центр NASA. Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается примерно в 100 млн дол.

Первый в истории суд над автором вредоносного ПО. Роберт Т. Моррис добровольно явился с повинной. Учитывая этот факт, а также то, что в планы автора программы не входило написание вредоносного ПО, суд приговорил Морриса к 3 годам условно, 10 000 дол. штрафа и 400 ч общественных работ.

Datacrime (1989) – вирус с очень опасным поведением. Несмотря на сравнительно небольшое распространение, он вызвал повальную истерию в мировых средствах массовой информации. Особенность вредоносной программы состояла в том, что она инициировала низкоуровневое форматирование нулевого цилиндра жесткого диска, что приводило к уничтожению таблицы размещения файлов (FAT) и безвозвратной потере данных.

Aids Information Diskette (1989) – первая эпидемия троянской программы. Ее автор разослал около 20 000 дискет с вредоносом по адресам в Европе, Африке и Австралии, похищенным из баз данных Организации всемирного здравоохранения и журнала PC Business World. После запуска вредоносная программа автоматически внедрялась в систему, создавала свои собственные скрытые файлы и директории и модифицировала системные файлы. Через 90 загрузок операционной системы все файлы на диске становились недоступными, кроме одного – с сообщением, предлагавшим прислать 189 дол. на указанный адрес. Автор троянца, Джозеф Попп (Joseph Popp), признанный позднее невменяемым, был задержан в момент обналичивания чека и осужден за вымогательство. Фактически Aids Information Diskette – это первый и единственный вредонос, использовавший для массовой рассылки настоящую почту.

Cascade (1989) – резидентный зашифрованный вирус, вызывающий характерный видеоэффект – осыпание букв на экране. Вирус примечателен тем, что с его «лечения» берет свои истоки история «Лаборатории Касперского».

Дело в том, что Cascade был обнаружен Евгением Касперским на его рабочем компьютере, и с «лечения» этого вируса начался профессиональный путь Евгения в создании программ-антивирусов. В 1994 году антивирусный продукт AVP (Antiviral Toolkit Pro), прототип Антивируса Касперского, занял первое место в первом международном тестировании средств защиты от вирусов, проведенном лабораторией Гамбургского университета. А в 1997 году родилась антивирусная компания – «Лаборатория Касперского». До сих пор антивирус Касперского регулярно занимает высшие места в тестах международных исследовательских центров и компьютерных изданий.

Eddie (также известен как Dark Avenger, 1989) – первый вирус, противодействующий антивирусному программному обеспечению: он заражал новые файлы, пока антивирус проверял жесткий диск компьютера. Это достигалось применением особой технологии, позволяющей заражать не только COM/EXE- программы в момент их запуска, но и любые файлы при попытке прочтения.

Доинтернетовский период (1990–1998)

Компьютерные сети, появившиеся и использовавшиеся в 1970-х и 1980-х годах, теряют популярность и постепенно демонтируются. На смену им приходит единая сеть нового поколения – Интернет.

Начиная с 1990 года, проблема вирусов окончательно утрачивает связь с научными кругами и становится достоянием рядовых программистов, преследующих личные цели.

DiskKiller (1989–1990). Этим вирусом была заражена дискета бесплатного приложения к английскому компьютерному журналу PC Today. В июле 1990 года подписчикам разошлось около 50 000 экземпляров. Действие DiskKiller сводилось к уничтожению всей информации на жестком диске.

Chameleon (начало 1990 года) – первый полиморфный вирус. Его автор, Марк Уошбурн (Mark Washburn), за основу для написания программы взял сведения о вирусе Vienna из книги Ральфа Бюргера «Computer Viruses. The Disease of High Technologies» [Bur89] и добавил к ним усовершенствованные принципы самошифрации вируса Cascade – свойство изменять внешний вид как тела вируса, так и самого расшифровщика. Только в 1992 году был изобретен достаточно эффективный способ нейтрализации полиморфных вирусов – эмулятор процессора для дешифрации кодов. Эта технология является неотъемлемым атрибутом каждого современного антивирусного продукта.

Win.Vir (конец 1992 года) – первый вирус, поражающий исполняемые файлы Microsoft Windows 3.1. Эпидемии не вызвал, и его появление осталось практически

незаметным. Однако именно Win.Vir ознаменовал собой начало эпохи вирусов для Windows.

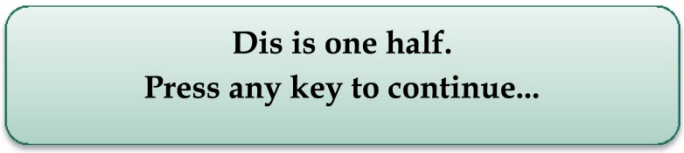
Вирусы начинают бороться с антивирусными программами – в 1992 году появляются первые анти-антивирусы.

Далее события начинают развиваться со всё увеличивающейся скоростью.

Shifter (1994) – первый вирус, заражающий объектные модули (OBJ-файлы).

SrcVir (1994) – семейство вирусов, заражающих исходные тексты программ (C и Pascal).

OneHalf (1994) – очень сложный резидентный файлово-загрузочный полиморфный вирус, вызвавший глобальную эпидемию во всем мире, в том числе в России. Его особенностью являлось то, что он постепенно шифровал информацию на диске. Это продолжалось до тех пор, пока весь винчестер не оказывался зашифрованным. Встроенная стелс-процедура позволяла вирусу при запросе зашифрованной информации производить расшифровку в режиме реального времени – следовательно, пользователь долгое время пребывал в неведении. Единственным визуальным проявлением вируса было сообщение



выводившееся в момент достижения количеством зашифрованных цилиндров диска половины от их общего числа. Однако при первой же попытке лечения, после вылечивания загрузочных секторов диска, вся информация на винчестере становилась недоступной, без возможности восстановления.

Concept (1995). В июле 1995 года случился один из поворотных моментов в истории вирусов и антивирусов: обнаружен первый вирус для текстового редактора Microsoft Word. Вирус, получивший название Concept, буквально за месяц «облетел» весь земной шар, заполонил компьютеры пользователей MS Word и прочно занял первые места в статистических исследованиях, проводимых различными компьютерными изданиями.

В течение четырех последующих лет макро-вирусы доминировали на вирусных «просторах».

Автор Concept применил инструкции языка WordBasic для модификации шаблона NORMAL.DOT, что сделало возможным внедрение кода вируса, представляв-

шего собой несколько автомакросов, в каждый документ, создаваемый пользователем после заражения. Таким образом, каждый пользователь, получив инфицированный документ, становился жертвой макровируса. Появление этой простой конструкции, давно предсказанное антивирусными разработчиками, имело далеко идущие последствия.

Во-первых, традиционные вирусы чаще всего писались на языке ассемблера, что требовало от злоумышленников определенных знаний, в то время как макровирусы создавались с помощью языка WordBasic, а позднее – VBA (Visual Basic for Applications), что было намного проще. Кроме того, макровирусы, как правило, хорошо видны, поэтому их легко копировать, модифицировать и повторно применять. Неожиданно поле вирусописательской деятельности оказалось открытым для широкого круга людей. В результате количество вирусов существенно возросло.

Во-вторых, внимание вирусописателей переключилось с исполняемого кода (программных файлов и секторов диска) на данные. Макровирусы стали первыми вредоносными программами, целенаправленно поражавшими файлы данных. Поскольку данными пользователи обменивались гораздо чаще, чем программами, у макровирусов появился более эффективный, чем у прежних вирусов, канал распространения. Эту проблему усугубил переход электронной почты в категорию популярных средств коммуникации и обмена данными: легкость прикрепления файлов к сообщению и появившаяся у обычных пользователей возможность доступа в Интернет также способствовали распространению макровирусов.

В-третьих, макровирусы не зависели ни от платформы, ни от операционной системы – они работали на уровне приложения. Существование версий Word для Windows 3.x, Windows 95, Windows NT и Macintosh делало эти системы уязвимыми для атаки. Вскоре проблема вышла за рамки Word. Поскольку язык VBA применялся и в других приложениях Microsoft Office (Word, Excel, PowerPoint, Access и Project), то все они стали мишенями для макровирусов. Существовали даже особые «гибридные» макровирусы, способные атаковать все офисные приложения.

Boza (начало 1996 года) – первый вирус для операционной системы Microsoft Windows 95.

Win.Tentacle (1996) – вызвал первую эпидемию среди пользователей Microsoft Windows 3.x.

Laroux (1996) – первый рабочий макровирус для заражения таблиц Microsoft Excel.

1997 год запомнился тем, что появился первый вирус для Linux, и тем, что был обнаружен первый сетевой вирус-червь, использовавший для своего распространения протокол передачи данных File Transfer Protocol (FTP). Итак,

Linux.Bliss (1997) – первый вирус для операционной системы Linux.

ShareFun (1997) – первый макровирус для MS Word 6/7, использующий для своего распространения возможности электронной почты, в частности почтовую программу MS Mail.

Homer (1997) – первый сетевой вирус-червь, использующий протокол передачи данных File Transfer Protocol (FTP).

В декабре 1997 года, вскоре после разработки технологии IRC (Internet Relay Chat), образовался новый класс вредоносных программ – IRC-черви.

В 1998 году жертвой вирусов стало еще одно популярное приложение из пакета MS Office – программа для создания презентаций PowerPoint.

Win95.HPS и Win95.Marburg (1998) – первые полиморфные Windows32-вирусы. Marburg известен также тем, что им были заражены компакт-диски, сопровождавшие английскую, словенскую, шведскую и итальянскую редакции журнала PC Gamer.

В 1998 году был обнаружен вирус тайваньского происхождения **Win95.CIH**, содержащий логическую бомбу на уничтожение всей информации на жестких дисках и порчу содержимого BIOS на некоторых материнских платах. Дата срабатывания программы (26 апреля) совпадала с датой аварии на Чернобыльской атомной электростанции, вследствие чего вирус получил второе имя – Чернобыль (Chernobyl). Масштабность эпидемии выяснилась 26 апреля 1999 года, когда по различным оценкам пострадало около полумиллиона компьютеров по всему миру, а общий ущерб составил сотни миллионов долларов США. Центром эпидемии стала Южная Корея, где было заражено более 300 тысяч компьютеров. В России Win95.CIH поразил не менее 100 тысяч машин.

Другим заметным событием 1998 года стало появление вредоносной программы нового типа – «бэкдор».

BackOrifice, Backdoor.BO (1998) – первая известная утилита скрытого администрирования удаленных компьютеров. Единственное отличие этого трояна от обычных программ для удаленного управления – несанкционированная установка и запуск. Действие утилиты сводилось к скрытому слежению за системой: ссылка на троянца отсутствовала в списке активных приложений, но при этом зараженный компьютер был открыт для удаленного доступа. Фактически, открывался свободный вход на зараженные компьютеры для других вредоносных программ. Впоследствии возник целый класс червей, размножение которых базировалось на оставленных BackOrifice дырах.

Во второй половине 1998 года вирусы активно начинают осваивать новые технологии: Java.StangeBrew – первый вирус, который заражал выполняемые модули

Java, VBScript.Rabbit – скрипты Visual Basic (VBS-файлы), HTML.Internal – первый HTML-вирус.

Интернет-этап (1999–2004)

Характеризуется появлением многочисленных вредоносных программ типа «компьютерные черви», а также компьютерными эпидемиями, приводящими к колоссальным убыткам.

Самые известные вирусы этой эпохи, такие как CodeRed или Nimda, продемонстрировали сочетание способности к практически мгновенному распространению и существенно усложненную, многоуровневую структуру. Для данного этапа можно выделить такие тенденции, как расширение спектра путей и методов проникновения, использование новых платформ и технологий, обновление вирусных кодов через интернет, новые вредоносные функции и активное противодействие антивирусным программам.

Открывается интернет-этап таким событием, как глобальная эпидемия почтового интернет-червя Happy99 в январе 1999 года. По сути, это был первый современный червь, открывший новый этап в развитии вредоносных программ. Он использовал для своего распространения программу MS Outlook, являющуюся корпоративным стандартом в США и во многих странах Европы.

Появление в марте 1999 года вируса **Melissa** знаменовало собой качественный скачок в процессе эволюции вирусных угроз. Принципиальная особенность этой вредоносной программы была в том, что она сочетала в себе характеристики макровируса для MS Word и функциональность почтового червя. Сразу же после заражения системы Melissa считывала адресную книгу почтовой программы MS Outlook и рассылала по первым 50 найденным адресам свои копии. Подобно Happy99 вирус Melissa делал это абсолютно незаметно для пользователя и, что примечательно, от его имени. Массовая рассылка позволяла Melissa распространяться быстрее, чем это делали все предыдущие макровирусы. Кроме того, Melissa угрожал стабильности инфраструктуры электронной почты из-за огромного объема генерируемого им почтового трафика.

Вирус Melissa послужил причиной существенных изменений характера вирусной угрозы. Теперь вредоносным программам уже не нужно было ждать, пока ничего не подозревающий пользователь разошлет инфицированный файл. Захватывая систему электронной почты, вирусы получали чрезвычайно эффективный механизм распространения и могли вызвать глобальную эпидемию за считанные дни или даже часы.

Компании Microsoft, Intel, Lockheed Martin были вынуждены временно отключить свои корпоративные службы электронной почты. По разным оценкам, совокупный ущерб от вируса оценивается в несколько десятков миллионов долларов США.

Через некоторое время был обнаружен и арестован автор вируса Melissa, Дэвид Л. Смит (David L. Smith). 9 декабря он был признан виновным и осужден на 10 лет тюремного заключения и к штрафу в размере 400 000 дол.

ZippedFiles (также известный как ExploreZip, 1999) – первый упакованный интернет-червь. Тело вредоносной программы было упаковано утилитой сжатия Neolite, обращаться с которой в то время антивирусные продукты не умели, что привело к эпидемии.

Bubbleboy (1999) – первый вирус из поколения червей-невидимок, распространявшихся по электронной почте без использования вложенных файлов и проникавших на компьютеры сразу же после прочтения зараженного письма. Вирус использовал различные уязвимости в системе безопасности Internet Explorer.

Babylonia (1999) – первый вирус-червь, который имел функции удаленного самообновления: он ежеминутно пытался соединиться с сервером, находящемся в Японии и загрузить оттуда список вирусных модулей.

В 2000 году основным средством транспортировки вредоносных кодов стала электронная почта – около 85 % всех зарегистрированных случаев заражения были вызваны проникновением вирусов именно при помощи этого источника. Помимо прочего, этот год также был отмечен всплеском активности создателей вирусов к Linux. В целом было зарегистрировано появление 37 новых вирусов и троянских программ для этой операционной системы.

LoveLetter (2000) – знаменитый скрипт-вирус, побивший рекорд вируса Melissa по скорости распространения.

Существует несколько разновидностей почтовых червей. Одни распространяются в виде исполняемых файлов (примером может служить первый современный червь Happy99), другие – в виде скрипт-файлов (Visual Basic Script или Java Script), вложенных в почтовые сообщения, третьи – в виде скриптов, встроенных в HTML-сообщения. Общим для всех почтовых червей является то, что для их распространения используется электронная почта, обычно в сочетании с методами социальной инженерии, призванными убедить наивных пользователей запустить вредоносный код.

Червь LoveLetter стал одним из первых примеров успешного применения методов социальной инженерии. Для распространения червя использовались сообщения с темой ILOVEYOU и текстом следующего содержания, размещенным в теле

письма: «Kindly check the attached LOVELETTER coming from me» («Пожалуйста, прочтите мое любовное письмо, прикрепленное к письму»). Всего в течение нескольких часов были поражены миллионы компьютеров.

Экономический ущерб, причиненный вирусом, оценивается в сумму свыше 8 млрд дол. [CE1]. LoveLetter попал в Книгу рекордов Гиннесса как самый разрушительный компьютерный вирус в мире.

Pirus (октябрь 2000) – первый вирус, написанный на скрипт-языке PHP.

Fable (октябрь 2000) – первый вирус, скрывающийся в информационных файлах PIF.

В целом 2001 г. характеризуется весьма масштабными эпидемиями сетевых червей, использующих для своего проникновения в систему различные дыры в операционных системах и установленном программном обеспечении.

Ramen (2001) – вирус, за считанные дни поразивший большое количество крупных корпоративных систем на базе операционной системы Linux.

Sadmind (2001) – первый известный интернет-червь, заражающий компьютеры Sun Sparc с операционной системой Solaris/SunOS. Для размножения использовалась брешь в службе системного администрирования /usr/sbin/sadmind. Червь также атаковал HTTP-серверы с установленным Microsoft Internet Information Server (IIS).

CodeRed (2001) – представитель нового типа вредоносных кодов, бесфайловый («бестелесный») червь. В отличие от всех предыдущих вирусов, он не пытался инфицировать файлы на жестком диске заражаемого компьютера, существуя лишь в его оперативной памяти и в сетевых пакетах. CodeRed использовал уязвимость сервера Microsoft IIS [MS01-033 – «Переполнение буфера в расширении ISAPI сервера индексов допускает запуск кода на веб-сервере»] для атаки на серверы, работающие под управлением Windows 2000. CodeRed распространялся, пересылая TCP/IP-пакеты через порт 80 на удаленную машину, загружался в память, используя переполнение буфера, а затем таким же точно способом рассылал свой код на другие уязвимые серверы. CodeRed разошелся по Интернету в считанные часы.

CodeRed начал действовать 12 июля 2001 года и вызвал эпидемию, заразив по разным данным до 200 000 серверов по всему миру, и провел крупномасштабную DDoS-атаку на веб-сервер Белого дома, вызвав нарушение его нормальной работы.

Через неделю, 19 июля, появилась новая модификация CodeRed, показавшая чудеса распространения – более 350 000 машин за 14 часов (до 2000 компьютеров в минуту). Однако, по замыслу автора, 20 июля вирус прекратил свое распространение.

Следующая версия, CodeRed.c (CodeRed II), была обнаружена 4 августа 2001 года. После заражения (использовалась всё та же брешь в системе безопасности IIS) вирус ничем не выдавал свое присутствие один-два дня, после чего перезагружал компьютер и начинал активные попытки распространения, продолжавшиеся 24 часа (или 48, в случае использования китайской раскладки). Червь также устанавливал троянскую программу explorer.exe и использовал встроенную бэкдор-процедуру.

Sircam (2001) – почтовый червь, отличавшийся необычной процедурой выбора имени зараженного вложения. Для этого случайным образом на диске выбирался документ, к имени которого добавлялось расширение .pif, .lnk, .bat или .com. Полученная конструкция вида mydiary.doc.com служила темой рассылаемых писем и именем новой копии программы. К отобранному файлу дописывался код червя. Таким образом, Sircam мог привести к утечке конфиденциальной информации. При рассылке использовался собственный SMTP-клиент, в поле «От» указывался один из адресов, найденных на зараженном компьютере, а сообщение содержало текст вида «Hi! How are you? I send you this file in order to have your advice. See you later. Thanks». Кроме того, в определенный момент времени (в зависимости от системного времени и модификации вируса) на зараженном компьютере удалялись все файлы на системном диске.

Nimda (2001). Успех CodeRed означал, что одним эпизодом дело не ограничится. И действительно, двумя месяцами позже, в сентябре 2001 года, вирус Nimda, использующий уязвимость в Internet Explorer [MS01-020: «Неправильный заголовок MIME может привести к запуску вложения электронной почты обозревателем Internet Explorer»], стал причиной еще одной глобальной эпидемии.

В отличие от ранее известных угроз, связанных с массовыми почтовыми рассылками, Nimda не требовал запуска пользователем зараженного EXE-файла, вложенного в почтовое сообщение. Вместо этого он использовал уязвимость браузера для автоматического запуска своего кода на исполнение. К тому времени уязвимость MS01-020 уже полгода как была обнаружена, но на многие компьютеры закрывающие ее обновления еще не были установлены[5]. Поэтому Nimda сумел заразить компьютеры по всему миру – вирус-червь в течение 12 часов поразил до 450 000 компьютеров.

В годы, последовавшие за эпидемиями, вызванными CodeRed и Nimda, создание эксплойтов для системных уязвимостей стало обычным делом, поскольку авторы вредоносных программ нашли уязвимости во многих популярных программах и

[5] Хорошая иллюстрация для одного из базовых правил техники компьютерной безопасности: «Регулярно устанавливать обновления операционной системы и используемого ПО».

операционных системах. Ранее такие методы ассоциировались с деятельностью хакеров, а не вирусописателей. Сочетание «традиционных» технологий создания вирусов с хакерскими атаками стало очередным этапом развития вредоносных программ.

Klez (2001) – почтовый червь, модификации которого на протяжении следующих нескольких лет занимали первые строки в рейтингах популярности. Программа проникала в компьютер по сети или через электронную почту. Также вредонос имел встроенную функцию поиска и подавления антивирусного программного обеспечения. Klez дописывал свой код к одному из документов на зараженной машине и начинал массовую рассылку. В поле «От» подставлялся любой адрес, найденный в компьютере или же случайно сгенерированный. При этом список всех обнаруженных в зараженном компьютере адресов электронной почты также присоединялся к вложению. Кроме рассылки своих копий, червь обнаруживал себя по 13-м числам четных месяцев или шестым нечетных, в зависимости от модификации: в такой день все файлы на зараженных компьютерах заполнялись случайным содержимым.

В 2002 году наблюдается стремительный рост вредоносных программ, которые преследуют конкретные коммерческие цели – похищают конфиденциальные данные, финансовые средства, пароли доступа в Интернет или производят другие действия, наносящие какой-либо материальный ущерб пользователям зараженных компьютеров. Этот год положил начало стремительной криминализации интернета в годы последующие.

В 2003 году начинает набирать обороты новый вид электронного мошенничества – так называемый фишинг. На первых порах он проявился в форме рассылки поддельных писем с просьбой подтвердить персональные коды доступа к банковскому счету.

Но прежде всего этот год запомнился эпидемией компьютерного червя Slammer, которая впервые со всей очевидностью продемонстрировала человечеству всю масштабность и серьезность угроз, которые несет в себе вредоносное ПО. Впервые в результате деятельности вредоносной программы от интернета на 12 часов было отключено (экономически и технологически развитое) государство – Южная Корея.

В начале 2003 года грянула эпидемия интернет-червя **Slammer**, заражающего сервера под управлением Microsoft SQL Server 2000. Вредонос использовал брешь в системе безопасности SQL Server. После проникновения на SQL-сервер червь в бесконечном цикле начинал посылать свой код на случайно выбранные адреса в сети. Поскольку SQL-сервера часто используются в качестве стандартной базы данных на Web-серверах, то данный червь был в состоянии замедлить работу Интернета в глобальных масштабах.

Slammer имел крайне небольшой размер – всего 376 байт (CodeRed – 4 КБ, Nimda – 60 КБ) и присутствовал только в памяти зараженных компьютеров. Более того, при работе червя никакие файлы не создавались, и червь никак не проявлял себя (помимо сетевой активности зараженного компьютера).

Действие компьютерного червя Slammer привело к очень значительному ущербу. В частности, этому вредоносному ПО удалось на 12 часов отключить от Интернета Южную Корею.

В августе 2003 года около 8 миллионов компьютеров во всем мире оказались заражены интернет-червем **Lovesan/Blaster**. Для размножения использовалась очередная брешь – на этот раз в службе DCOM RPC Microsoft Windows. Кроме того, вредонос включал в себя функцию DDoS-атаки на сервер с обновлениями для Windows.

Sobig.f (2003). Вредоносная программа Sobig.f установила новый рекорд по скорости – доля зараженных ею писем доходила до 10 % всей корреспонденции. Это достигалось использованием спамерских технологий. Sobig.f также инициировала цепную реакцию: каждый новый вариант этого компьютерного червя создавал сеть инфицированных компьютеров, которая позднее использовалась в качестве платформы для новой эпидемии. Однако конец эпидемии запрограммировал сам автор – 10 сентября 2003 года Sobig.f прекратил размножение.

Swen (также известный как Gibe, 2003) – яркий пример использования методов социальной инженерии. Этот компьютерный червь распространялся по электронной почте в виде письма якобы от Microsoft Corporation Security Center и с темой «Internet Security Update». Во вложении находился файл с именем q216309.exe, а в самом сообщении говорилось о необходимости срочной установки вложенной заплатки.

В настоящее время активность вирусописателей всё больше смещается в сторону создания вредоносного ПО для мобильных платформ. В этой связи знаковым событием можно считать появление в 2004 году первого червя для смартфонов под управлением операционной системы Symbian и первой вредоносной программы для Windows Mobile. Кроме того, этот год запомнился сильнейшей эпидемией сетевого червя Sasser.

Sasser (2004). Этот сетевой червь парализовал работу более 8 млн компьютеров по всему миру, от него пострадали тысячи крупных и мелких компаний, университеты, государственные учреждения. Некоторые авиакомпании отложили или даже отменили рейсы (British Airways, Delta Air Lines), прекратили работу несколько банков (Goldman Sachs и Westpac Bank), а финский банк Samp закрыл все 130 своих отделений в качестве профилактической меры. На Тайване сетевой червь парали-

зовал работу трети почтовых отделений, в Гонконге оставил без компьютеров государственные больницы, остановил железную дорогу Австралии. Убытки от этого червя оцениваются почти в 1 млрд дол. Для проникновения Sasser использовал уязвимость в службе LSASS Microsoft Windows.

В этом же году разразилась так называемая война вирусописателей. Несколько преступных группировок, известных по вирусам Bagle, Mydoom и Netsky выпускали новые модификации своих программ буквально ежечасно. Каждая новая программа несла в себе очередное послание к противостоящей группировке, изобилующее нецензурными выражениями, а Netsky даже удалял любые обнаруженные экземпляры вирусов Mydoom и Bagle.

Почтовый червь **Bagle** впервые был обнаружен 18 января 2004 года. Для распространения он использовал собственный SMTP-клиент, код вируса пересылался во вложении с произвольным именем и расширением .exe. Рассылка производилась на адреса, найденные на зараженном компьютере. Также Bagle содержал встроенную backdoor-процедуру, открывающую порт 6777 на запуск команд и загрузку любых файлов. Следующие модификации содержали процедуры распространения через P2P-сети, методы социальной инженерии, активно противодействовали антивирусному программному обеспечению.

Mydoom (2004). Этот компьютерный червь известен, прежде всего, массированной 12-дневной DDoS-атакой на веб-сайт компании SCO Group[6], начавшейся 1 февраля 2004 года. За пару часов работа сервера была полностью парализована и вернуться в нормальный режим веб-сайт смог только 5 марта. В ответ руководители SCO Group объявили награду в размере 250 000 дол. за информацию об авторе компьютерного червя.

Другая модификация этой вредоносной программы применялась для проведения DDoS-атаки на сайт Microsoft.

Для распространения Mydoom использовал почтовую рассылку через собственный SMTP-клиент, а также P2P-сети (Kazaa).

NetSky (2004). Первая модификация почтового червя NetSky (также известен как Moodown) была обнаружена 16 февраля. Кроме электронной почты, для распространения были задействованы P2P и локальные сети. Вторая модификация NetSky отличилась тем, что в силу человеческого фактора ею были заражены тысячи писем,

[6] The SCO Group – американская компания, разрабатывающая системное и прикладное программное обеспечение.

отправленных известным финским производителем антивирусного ПО – компанией F-Secure – своим клиентам.

Cabir (2004) – первый сетевой червь, распространяющийся через протокол Bluetooth и заражающий мобильные телефоны, работающие под управлением OS Symbian. При каждом включении зараженного телефона вирус получал управление и начинал сканировать список активных Bluetooth-соединений. Затем выбирал первое доступное соединение и пытался передать туда свой основной файл caribe.sis. Ничего деструктивного Cabir не делал – только снижал стабильность работы телефона за счет постоянных попыток сканирования активных Bluetooth-устройств.

Однако вредоносные программы – это не только вирусы и трояны. Начиная с 2004 отмечается широкое распространение использования вирусных технологий для установки потенциально нежелательного ПО подтипов adware/pornware на целевые компьютеры.

Этот год также запомнился масштабными арестами вирусописателей – было осуждено около 100 хакеров, причем трое из них находились в двадцатке самых разыскиваемых ФБР преступников.

Современный криминальный этап (2005 – н. вр.)

Для современного криминального этапа характерно то, что вредоносное ПО в первую очередь используется в преступных целях. Оно становится всё более сложным, вирусописатели-непрофессионалы оттесняются на периферию. Постепенно всё большее значение приобретают угрозы, связанные с целевыми атаками. Другой заметной тенденцией нашего времени является более масштабное применение написанного на высоком профессиональном уровне вредоносного ПО в качестве кибероружия для мощных целевых кибератак и кибершпионажа.

Тенденции второй половины 2004 года сохранились и в последующих 2005 и 2006 годах. «Громких» инцидентов практически не происходит, но зато двукратно растет число разнообразных троянских программ, которые распространяются самыми разными способами: через интернет-пейджеры, веб-сайты, при помощи сетевых червей или традиционной электронной почты. При этом растет «популярность» именно сетевых непочтовых червей, которые проникают на компьютеры, используя различные дыры в программном обеспечении.

В 2005 году наметился некоторый спад активности почтовых червей. Фактически после Mydoom, NetSky и Bagle до середины лета 2005 года не наблюдалось ни одной сколько-нибудь значительной эпидемии.

Поэтому пальму первенства перехватили сетевые черви и программы, использующие для распространения различные интернет-пейджеры (прежде всего MSN Messenger). Первые активно используют бреши в операционных системах Microsoft Windows – чаще всего это уязвимости в службах RPC DCOM и LSASS, а также дыры, оставленные прошедшими ранее эпидемиями: это позволяет создавать ботнеты, включающие тысячи «компьютеров-зомби». Вторые – пользуются некомпетентностью и отсутствием опыта создателей программ обмена сообщениями в упреждении вирусных инцидентов.

Глобальных эпидемий в первой половине 2005 года зафиксировано не было, но это не означает уменьшение числа вирусов – наоборот, с каждым днем их появляется всё больше. При этом можно отметить увеличение избирательности вредоносных программ – становятся популярными черви, главной целью которых является похищение определенной информации. Кроме уже ставших привычными краж номеров кредитных карт, участились случаи воровства персональных данных игроков различных онлайн-игр – Ultima Online, Legend of Mir, Lineage, Gamania. В России также зафиксированы случаи с игрой «Бойцовский клуб», где реальная стоимость некоторых предметов на аукционах достигает тысяч долларов США.

Развитие получили вирусные технологии для мобильных устройств. Созданы вирусы всех трех типов – классические вирусы, черви и троянские программы. В качестве пути проникновения используются не только Bluetooth-устройства, но и обычные MMS-сообщения (червь ComWar).

К 2006 году криминальный бизнес в сети можно считать сформировавшимся. Непрерывно растут количество и качество троянских программ и червей, созданных с откровенно преступными намерениями. Продолжается формирование криминальных программ для мобильных телефонов.

2008 год показал, что эпоха эпидемий осталась в прошлом. Начавшись в 2000 году, она характеризовалась большим количеством червей, вызывавших глобальные эпидемии и использовавших для своего распространения сначала электронную почту, а ближе к концу периода – сетевые атаки. Пик эпидемий пришелся на 2003– 2005 годы.

2007–2008 годы стали началом нового периода со стремительным ростом количества троянских программ, ориентированных на кражу информации, которая в большинстве случаев относится к банковским аккаунтам и онлайн-играм. В это время вредоносное ПО практически перестало создаваться в некоммерческих целях.

Использование атак через браузер в 2010 году стало доминирующим способом проникновения вредоносного ПО на компьютеры пользователей. Уязвимости в браузерах (в Internet Explorer в первую очередь), а также во взаимодействующих с

браузерами приложениях, таких как Adobe Flash Player или PDF reader, продолжают выявляться практически каждый месяц, и каждую из них очень быстро начинают использовать злоумышленники.

2010–2011 годы можно охарактеризовать трояко:

1) первые свидетельства применения кибероружия (Stuxnet, Duqu);
2) рост популярности целевых атак;
3) резкий рост атак на мобильную платформу Android.

Для 2012–2013 годов характерно следующее:

- рост числа инцидентов, связанных с целевыми атаками;
- кибероружие становится всё более изощренным (Flame, Gauss, Careto). Борьба самых могущественных государств за доминирующее положение с применением кибершпионажа;
- атаки на разработчиков ПО и игр, таких как Adobe, Microsoft, Oracle и Sony;
- взрывной рост угроз, нацеленных на Android. Создание вредоносного ПО для мобильных платформ – один из основных трендов нашего времени.

Заключительные замечания по второй главе

Отличие ученого от вирусописателя состоит в целях, которые преследует автор программы. Вирусы могут не только воровать информацию о кредитных картах и рассылать от чужого имени спам. С помощью самораспространяющихся программ возможно моделирование в компьютерных системах искусственной жизни, воспроизведение поведения взаимодействующих друг с другом и эволюционирующих живых организмов. Но, по состоянию на сегодняшний день, можно уверенно констатировать: встречающиеся в живом виде вирусы несут угрозу нормальному функционированию компьютерных систем.

Подтверждением серьезности угрозы, исходящей от вредоносного ПО, может служить статистика. По данным Kaspersky Security Network, только в одном лишь 2013 году продукты «Лаборатории Касперского» заблокировали более 5 млрд вредоносных атак на компьютеры и мобильные устройства пользователей, отразили более 1 млрд атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира. В этом же году специалистами «Лаборатории Касперского» было зафиксировано более ста тысяч новых модификаций вредоносных программ для мобильных устройств (см. [KL_SecL_6]).

С ростом сети Интернет увеличивается количество потенциальных жертв вирусописателей, выход новых систем и платформ влечет за собой расширение спектра возможных путей проникновения в систему вирусов. Современный пользователь

компьютера не может чувствовать себя в безопасности перед угрозами, которые несет в себе вредоносное ПО. Это могут быть, например,

- фишинговые атаки на интернет-банкинг;
- кража конфиденциальной информации;
- заражение компьютера «бэкдор»-программами, с целью использовать его (без ведома пользователя) для преступной деятельности в составе ботнета;
- уничтожение информации на винчестере;
- особняком стоит одна из самых масштабных угроз нашего времени, которую, к сожалению, пользователи до сих пор недооценивают – атаки на мобильные платформы;
- на уровне компаний и государственных структур наиболее серьезной опасностью, связанной с использованием вредоносного ПО, становятся целевые атаки, в том числе с применением мощного кибероружия, о чем мы подробно расскажем в четвертой главе.

Контрольные вопросы

1. Расскажите о первой вирусной эпидемии для IBM-совместимых персональных компьютеров.
2. Чем примечательна первая эпидемия сетевого червя?
3. Первый макровирус. В чем его особенность?
4. Расскажите о методах социальной инженерии. Пример: e-mail-червь LoveLetter.
5. Чем примечательны эпидемии компьютерных червей Slammer и Sasser?
6. Каковы особенности современного криминального этапа в развитии вредоносного ПО?

Глава 3. Технологии детектирования вредоносного ПО

Антивирус (антивирусная программа) – программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

В настоящее время большинство ведущих антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Постоянная антивирусная защита запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия. Постоянная антивирусная защита проверяет не только файлы на различных носителях информации, но и оперативную память компьютера. Основная задача постоянной антивирусной защиты компьютера – обеспечивать максимальную безопасность при минимальном замедлении работы проверяемых на вредоносные действия программ.

Защита по требованию запускается самим пользователем и, как правило, заключается в полном или выборочном сканировании присутствующих на жестких и сетевых дисках компьютера файлов. Защита по требованию производит однократную проверку оперативной памяти компьютера. В большинстве случаев антивирусные сканеры гораздо более требовательны к ресурсам компьютера, нежели постоянная антивирусная защита.

В основные задачи антивируса входят:

- препятствование проникновению вредоносного (или потенциально нежелательного) ПО в компьютерную систему;
- обнаружение наличия вредоносного или потенциально нежелательного ПО в компьютерной системе.;
- удаление вредоносного или потенциально нежелательного ПО из компьютерной системы без нанесения повреждений другим объектам системы;
- восстановление зараженных (модифицированных) вредоносными программами файлов;
- минимизация ущерба от действий вирусов.

Развитие антивирусных технологий

Первые антивирусы

В 1984 году Энди Хопкинсом (Andy Hopkins) были созданы самые первые антивирусные программы с названиями CHK4BOMB и BOCHK4BOMB. Программа CHK4BOMB производила сканирование текста модуля загрузки для обнаружения подозрительных участков и текстовых сообщений в коде. Программа BOCHK4BOMB осуществляла перехват записи и форматирования, выполняемых через BIOS. Нежелательную операцию можно было как запретить, так и разрешить.

Первый антивирус в современном понимании этого термина, то есть резидентный, «защищающий» от вирусных атак, появился в 1985 году. Программа DRPROTECT создана усилиями Джи Вонг (Gee Wong). Разработка блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требовала перезагрузки системы.

Антивирусные программы до начала 1990-х годов представляли собой, по сути, набор из нескольких десятков сигнатур (образцов вирусного кода), которые хранились в теле программы. Предполагалась также процедура поиска этих сигнатур в файлах. Причем зачастую эти сигнатуры разработчики даже не шифровали. Получалось так, что один антивирус легко мог «найти вирус» в другом.

Вначале антивирусные программы осуществляли только проверку по требованию. Число новых вирусов росло медленно, а скорость их распространения по сегодняшним меркам была весьма низкой. Поэтому антивирусной программе в те времена достаточно было регулярно проводить проверку системы и удалять вредоносные программы, попавшие в офисные или домашние компьютеры. Для этих целей как нельзя лучше подходила чистая системная дискета: загрузка с нее обеспечивала отсутствие в памяти вирусов, которые могли бы помешать проверке и очистке диска.

Большинство антивирусных программ обновлялось раз в квартал. Некоторые антивирусные разработчики предлагали ежемесячные обновления, но это не считалось необходимым, и те, кому требовалась усиленная защита, платили за более высокую частоту обновлений дополнительные деньги. Обновления поставлялись на физических носителях, то есть на тех же гибких дисках.

Сигнатурное детектирование

Итак, на первых порах развития антивирусных технологий они сводились к сигнатурному методу детектирования – методу работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы.

Сигнатура (от англ. signature – подпись) может иметь сколь угодно разное представление.

Это могут быть: куски кода, контрольные суммы, метаданные (время создания, размер).

В результате работы детектора, основанного на сигнатурах, в самом простом варианте антивирус открывает все файлы на чтение и вычисляет их хеш, после чего сравнивает его с базой данных сигнатур. Иногда сравниваются только заголовки исполняемых файлов, иногда просто ищется определенная строка в тексте-коде. Иногда используется совокупность различных сигнатур.

Достоинства сигнатурного метода:

- высокая точность обнаружения – уникальность сигнатур (или их совокупностей) позволяет выделять вредоносные программы на фоне другого программного обеспечения;
- малая доля ложных срабатываний.

Недостатки:

- отсутствие способности выявления нового вредоносного ПО;
- беззащитность перед полиморфизмом и шифрованием;
- необходимость регулярного обновления баз данных сигнатур;
- ручная разработка сигнатур.

Одним из способов, который был разработан вирусописателями для затруднения сигнатурного детектирования, является обфускация.

Обфускация – совокупность приемов запутывания исходного кода программы, имеющих целью максимально затруднить его чтение и анализ, но полностью сохранить функциональность.

Наиболее характерно для обфускации разбавление основного кода информационным «мусором», с целью затруднить анализ кода программы.

Примеры простейшей обфускации: разбавление кода нейтральными (не изменяющими функционал программы) операторами; снижение его наглядности посредством использования чрезмерного количества безусловных (либо маскирующихся под условные безусловных) переходов.

Рост числа угроз и развитие методов их обнаружения

Однако к концу 1990 года число вирусов было уже достаточно значительным. Оказавшись перед лицом этой проблемы, разработчики антивирусов стали внедрять защиту, работающую в реальном времени. Это означало создание резидентных про-

грамм (TSR – Terminate and Stay Resident), которые вели мониторинг системы, т.е. перехватывали операции доступа к диску и файлам для проверки их на наличие известных вирусов.

В 1992 году появилась программа MtE – генератор полиморфного кода, которым мог воспользоваться не только опытный, но и любой начинающий программист. Полиморфные вирусы стали появляться каждый день, а всевозможные дополнительные способы борьбы, такие как усложнение алгоритмических языков сверки кода, – перестали работать.

Растущая угроза со стороны полиморфных вирусов заставила антивирусных разработчиков дополнить сигнатурный анализ другими методами, которые позволяли сканеру «просвечивать» слой (или слои) шифрования. Эти методы включали технологии редуцированной маски, криптографического и статистического анализа, а также эмуляции кода. Эмуляция кода также использовалась для более эффективного эвристического обнаружения, поскольку делала возможным динамический анализ кода.

Эмуляторы – модули, которые осуществляют исполнение программного кода в изолированной среде для последующего анализа его поведения.

Первой антивирусной программой с эмулятором кода стала программа Евгения Касперского AVP (Antiviral Toolkit Pro – прототип антивируса Касперского).

Логическим продолжением технологии эмуляции стала концепция «песочницы». При запуске анализируемой программы в «песочнице» программе предоставляется уже жестко контролируемый набор ресурсов. При этом доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают.

Кроме использования метода эмуляции, разработчики начали искать пути проактивного обнаружения вирусов с помощью эвристического анализа. Антивирусные компании постоянно изучали технологии, используемые при создании вредоносных программ, и применяли полученный опыт при составлении списка подозрительных характеристик, каждая из которых имела свой весовой коэффициент. Сканер анализировал код на наличие этих характеристик и, если суммарный коэффициент превышал заранее установленный порог, делал вывод о том, что файл, возможно, заражен вирусом.

Первые поведенческие блокираторы

Альтернативным решением проблемы резкого увеличения числа компьютерных угроз стал поведенческий анализ. В то время как традиционные антивирусные

сканеры хранили сигнатуры вредоносных программ в базах данных и при сканировании сверяли код с имеющимися в базах сигнатурами, поведенческий блокиратор определял, является ли программа вредоносной, исходя из ее поведения в системе. Если программа выполняла действия, не разрешенные правилами, определенными заранее, то выполнение этой программы блокировалось.

Основным преимуществом поведенческого блокиратора, по мнению его сторонников, является его способность отличать «хорошие» программы от «плохих» без помощи профессионального вирусного аналитика. Проблема в том, что существует некая промежуточная зона между явно вредоносными и допустимыми действиями. Кроме того, одни и те же действия могут быть вредоносными в программе, предназначенной для нанесения ущерба, и полезными в легитимном ПО. Например, низкоуровневая запись данных, используемая вирусом, червем или троянцем для того, чтобы стереть информацию с жесткого диска, совершенно легитимно применяется операционной системой. Как поведенческий блокиратор, установленный на файловом сервере, узнает, законно пользователь изменяет или удаляет документ, или это результат действий вредоносной программы?

Тем не менее поведенческий анализ получил свое дальнейшее развитие: в некоторых современных решениях по защите от информационных угроз он используется в сочетании с другими методами поиска, обезвреживания и удаления вредоносного кода.

Решения для почтовых серверов и шлюзов

С появлением макровирусов в 1995 году и с изменением общей картины угроз изменились и решения, направленные на защиту корпоративных сетей. До эпохи макровирусов антивирусное ПО было ориентировано на настольные компьютеры и, в меньшей степени, на файловые серверы. С появлением макровирусов начался процесс расширения антивирусной защиты сетей – теперь она должна была охватывать также почтовые серверы и интернет-шлюзы. Поскольку электронная почта служила основным механизмом распространения вирусов, проверка почтовых сообщений стала эффективным способом защиты рабочих станций. Однако это не отменяло необходимости установки на рабочие станции и файловые серверы антивирусных приложений, которые оставались важнейшим оружием в борьбе против вирусов. Но их следовало интегрировать в расширенные, многоуровневые, глубоко эшелонированные решения.

Одновременно разработчики антивирусов продолжали развивать возможности проактивной защиты, особенно в области generic-обнаружения, т.е. обнаружения и удаления группы угроз с помощью одной сигнатуры. В основе generic-обнаружения лежит тот факт, что наиболее «успешные» угрозы часто копируются подражателями или видоизменяются авторами, совершенствующими свои творения. В результате появляется множество (десятки, а то и сотни) вирусов, червей или троянцев, каждый

из которых уникален, но при этом все они принадлежат одному семейству. Generic-обнаружение стало еще одним методом детектирования неизвестных угроз без необходимости создания новых сигнатур.

Активное использование электронной почты в качестве инструмента бизнеса привело к появлению еще одной проблемы – нежелательных электронных рассылок, или спама. В этот период началась активная разработка решений в области контентной фильтрации. Они устанавливались преимущественно на интернет-шлюзы для фильтрации спама и другого нежелательного контента. Было налажено сотрудничество с разработчиками антивирусов, которые уделяли всё большее внимание фильтрации вредоносного кода на уровне почтовых серверов и интернет-шлюзов.

Персональные сетевые экраны

Одним из путей расширения возможностей защиты стало использование персонального сетевого экрана (файервола), контролирующего входящие и исходящие потоки данных и блокирующего нежелательный сетевой трафик. Как следует из названия, персональный сетевой экран (в отличие от традиционного межсетевого экрана, развертываемого на интернет-шлюзах) устанавливается на рабочую станцию или на сервер. Он работает как своеобразный «инспектор дорожного движения», досматривая как входящий, так и исходящий трафик и разрешая или блокируя соединения в соответствии с заданными политиками безопасности. Персональный сетевой экран, как правило, работает «на два фронта». С одной стороны, он обеспечивает фильтрацию на уровне приложений, т.е. позволяет задавать правила для популярных приложений (браузеров, программ мгновенного обмена сообщениями и др.). Кроме того, персональный сетевой экран обеспечивает пакетную фильтрацию: он анализирует передаваемые пакеты данных (заголовки, используемые протоколы, порты, IP-адреса и пр.) и осуществляет фильтрацию пакетов в соответствии с заданными политиками безопасности.

Системы предотвращения вторжений

Некоторые разработчики средств защиты используют «традиционные» технологии в сочетании с системами предотвращения вторжений (IPS – Intrusion Prevention System). Системы, предназначенные для защиты рабочих станций и серверов (host-based IPS), как правило, применяют для обнаружения вредоносного кода поведенческий анализ. Они контролируют все запросы, поступающие в систему, и сопоставляют их с политиками безопасности, определяющими «нормальное» поведение. Эти политики могут иметь достаточно высокую степень детализации, поскольку описывают поведение конкретных приложений. Такие действия, как открытие тех или иных портов, сканирование портов, попытки повышения привилегий в системе и внедрение кода в активные процессы, могут блокироваться как аномаль-

ное поведение. Некоторые IPS-системы дополняют поведенческий анализ использованием сигнатур известного вредоносного кода.

В целом поведенческий анализ позволяет контролировать активность приложений в реальном времени, блокировать любые подозрительные действия и даже обеспечивать откат – отмену изменений, произведенных вредоносным кодом в системе.

Сетевые IPS (network-based IPS) устанавливаются на пути передачи сетевого трафика и анализируют пакеты на наличие вредоносного кода. Они реагируют на такие характерные признаки атаки, как аномальная загрузка каналов и нестандартные (в частности, неправильно сформированные) сетевые пакеты. Сетевые IPS особенно эффективны в обнаружении атак, вызывающих отказ в обслуживании (DoS), и трафика, генерируемого интернет-червями.

Задача технологий предотвращения вторжений – обеспечить защиту от атак, нацеленных на кражу конфиденциальной информации, от сетевых червей и вредоносного кода, предназначенного для захвата компьютера, включения его в зомби-сеть и последующего использования для рассылки спама.

Компонентный состав современных продуктов безопасности

Надежная информационная защита требует комплексного подхода. Современные средства защиты состоят из нескольких компонентов, каждый из которых выполняет определенные задачи (рис. 3.1).

В данной модели можно выделить четыре основных группы компонентов: перехватчики, антивирусные движки, компонент контроля запуска и исполнения приложений, облачные сервисы.

Рассмотрим функциональные задачи каждого из компонентов.

Перехватчики – это некие «сенсоры», которые позволяют антивирусным продуктам встраиваться в процесс работы ОС так, чтобы другие компоненты антивирусной защиты имели возможность проверять объекты и события в нужный момент времени.

В качестве перехватчиков работают:

- драйвер, осуществляющий перехват обращения приложений к файлам. Перехватив обращение к файлу, антивирусный продукт может проверить этот файл на наличие вредоносного кода или проверить допустимость такой операции согласно правилам контроля активности приложений (HIPS). В случае наличия вредоносного кода или противоречия правилам активности приложения, драйвер может запретить либо обращение к файлу, либо запуск приложения;

- сетевой драйвер, позволяющий осуществлять контроль сетевой активности приложений (предотвращение утечек данных по сети, блокировка сетевых атак и т.д.);
- плагины – библиотеки (модули), встраиваемые в популярные приложения (в почтовые клиенты, браузеры, IM-клиенты и т.д.), обеспечивающие проверку передаваемых данных.

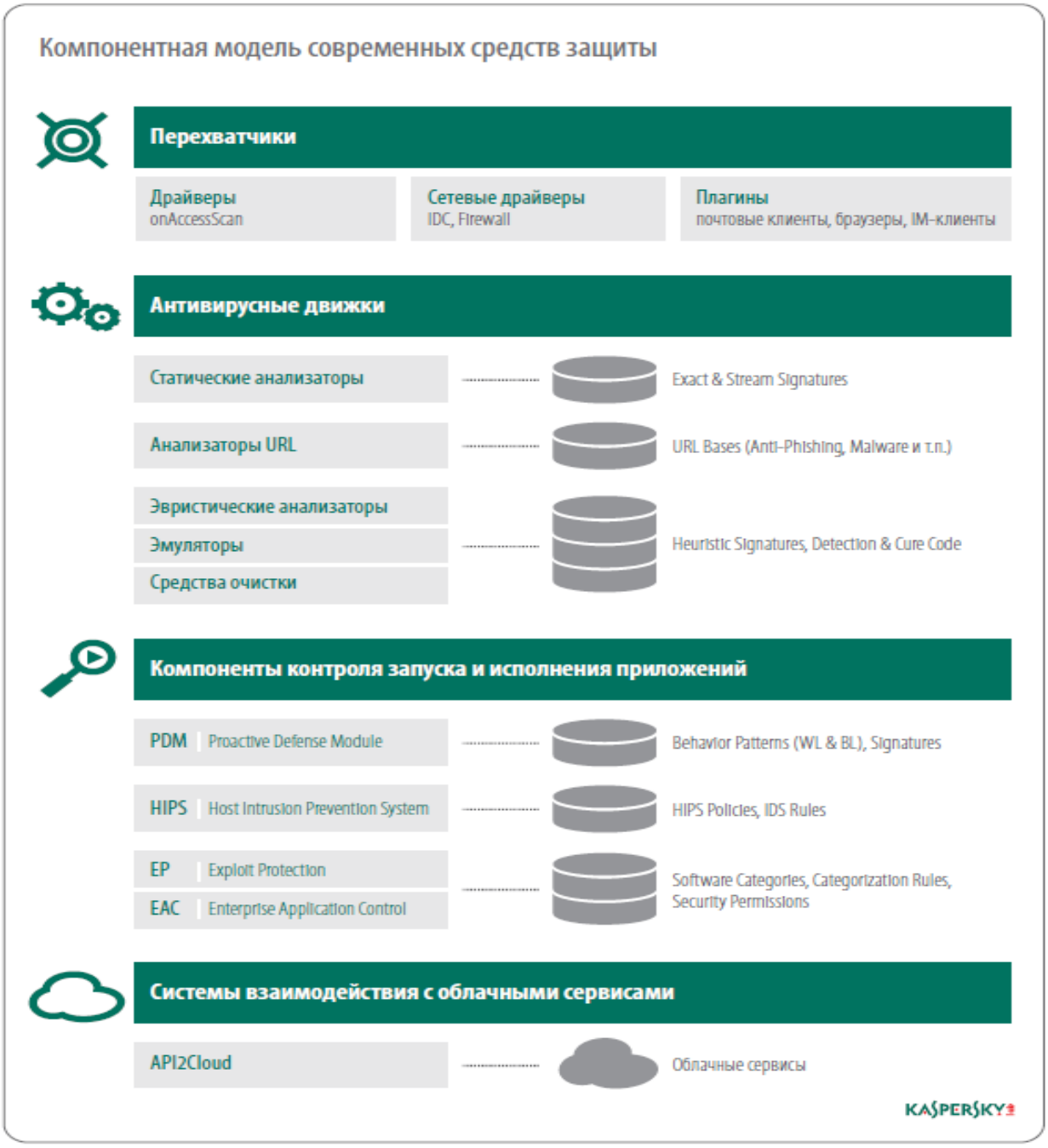


Рис. 3.1. Компонентная модель современных средств защиты

Антивирусные движки – модули продукта, предназначенные для проверки потенциально вредоносных объектов. Методов проверки может быть несколько, и их перечень и названия у каждого вендора антивирусных продуктов могут быть свои.

Можно выделить основные типы движков:

- статические анализаторы, позволяющие детектировать вредоносные объекты по каким-либо характерным статическим признакам (чаще всего это связано со структурой файлов специфичных форматов);
- анализаторы URL, проверяющие, есть ли URL-адрес, на который переходит пользователь или который ему прислали по почте, в базах вредоносных или фишинговых URL, в базе URL-адресов сайтов определенных тематических категорий (компонент «Родительский контроль»);
- эвристические анализаторы, дающие возможность одной сигнатурой детектировать множество вредоносных файлов, в том числе и ранее неизвестные модификации вредоносного ПО, одновременно позволяя добиться повышения качества детектирования и уменьшения размера антивирусных баз;
- эмуляторы – модули, которые осуществляют исполнение программного кода в изолированной среде для последующего анализа его поведения.

Контроль запуска и исполнения приложений (Application Control) – одна из составляющих информационной защиты в большинстве современных антивирусных продуктов, работающая с использованием событий от «перехватчиков». Обработка этих событий осуществляется с помощью разных компонентов:

- PDM (Proactive Defense Module). Поиск и обнаружение известных вредоносных моделей поведения программ (последовательностей, паттернов) по базам вредоносных паттернов поведения;
- HIPS (Host Intrusion Prevention System). Проверка каждого потенциально опасного действия программы (чаще атомарного действия) по перечню правил, определяющих допустимые для этой программы действия. Причем эти правила могут создаваться разными для разных категорий ПО. Например «доверенным» программам можно делать «все», а «неизвестным и подозрительным» что-то можно запрещать;
- Exploit Protection. Предназначен для защиты от вредоносного ПО, использующего уязвимости в программах и операционной системе. В настоящее время Exploit Protection есть в арсенале лишь некоторых компаний. «Лаборатория Касперского» считает данный уровень защиты необходимым и соответствующий набор технологий в ее программных продуктах называется Automatic Exploit Prevention (AEP). В его основе лежит анализ поведения эксплойтов, а также особый контроль приложений, которые чаще других подвергаются атакам злоумышленников.

AEP препятствует срабатыванию эксплойтов и развитию вредоносного поведения, если эксплойт всё-таки сработал;
- EAC (Enterprise Application Control). Запуск программ разных категорий и (или) версий ПО в соответствии с разными правилами.

Облачные сервисы. Взаимодействие с облачными сервисами (CLOUD Services) позволяет расширить возможности как антивирусных движков, так и технологий контроля активности программ. Использование облака позволяет скрыть часть логики проверки (чтобы осложнить злоумышленникам процесс реверс-инжиниринга) и уменьшить размер обновлений баз сигнатур и баз поведенческих шаблонов на стороне пользователя/клиента.

В заключение раздела отметим, что важной современной тенденцией является стремительный рост вредоносного ПО. Было время, когда один новый вирус появлялся каждый час, затем – каждую минуту. В настоящее время новый вирус рождается каждую секунду. Это значит, что борьба с вредоносным ПО становится всё более технологичной. Сейчас во всем мире работает около 60 компаний, разрабатывающих антивирусное ПО.

При написании раздела использованы статьи [KL_SecL_13], [KL_SecL_14].

Функции современного антивируса

Современные антивирусы обладают большим количеством основных и дополнительных функций. Перечислим наиболее типичные.

Предупреждение заражения

В эту функцию входят три пункта:
1) анализ новых файлов: анализ на наличие угрозы всех файлов, поступающих на машину «извне»;
2) анализ сетевого трафика: анализ входящего и исходящего сетевого траффика на наличие аномалий;
3) анализ процессов запущенных в системе.

Обнаружение вредоносного ПО

Данный модуль включает в себя сканирование по требованию (функция антивируса, позволяющая пользователю самостоятельно запустить сканирование системы) и проверку в режиме реального времени (функция антивируса, позволяющая реализовать непрерывный процесс сканирования).

Восстановление зараженных файлов

Функция восстановления зараженных файлов также является очень важной частью любого антивирусного ПО. Данный модуль включает в себя две функции: лечение файлов от вирусов (функция антивируса, позволяющая вылечить зараженный файл) и восстановление испорченных данных (функция антивируса, позволяющая восстановить поврежденные или уничтоженные файлы).

Самозащита

Ни для кого не секрет, что антивирус сам по себе является одной из целей вредоносного ПО. Для защиты от вредоносных программ в антивирус встраивается система самозащиты. Она включает в себя невозможность отключения антивируса без ведома пользователя, а также контроль целостности модулей (защита модулей антивирусного ПО от модификации).

Дополнительные функции

Как уже упоминалось выше, многие антивирусные продукты представляют собой комплекс различного защитного ПО. Очень часто, помимо непосредственной защиты от вирусов, пользователю также предлагаются следующие полезные функции:

1. Межсетевой экран – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
2. Родительский контроль – функция антивируса, позволяющая установить для каждой учетной записи на компьютере ограничения доступа использования компьютера и Интернета.
3. Мастер паролей – функция антивируса, позволяющая безопасно работать с паролями.
4. Антифишинг – функция антивируса, реализующая защиту от фишинга.
5. Системы предотвращения вторжений (IPS) – функция антивируса, представляющая собой систему сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Контрольные вопросы

1. Дайте определение антивируса. Перечислите его основные задачи.
2. В чем сильные и слабые стороны метода сигнатурного детектирования?
3. Расскажите о методах эмуляции и эвристического анализа.
4. В чем суть поведенческого анализа?
5. Каков компонентный состав современных продуктов безопасности.

Глава 4. Целевые атаки и кибершпионаж

Целевая атака начинается с поддельного письма

По данным японо-американской компании Trend Micro, которая работает в сфере защиты информации, 91 % целевых кибератак предшествует малотиражная спам-рассылка, как правило, вредоносная. Она использует элементы социальной инженерии и ориентирована на конкретное лицо или группу адресатов в атакуемой организации.

Главная причина популярности подобной практики у организаторов целевых атак в том, что в тщательно подготовленную ловушку может угодить даже самый искушенный и осмотрительный пользователь.

Вредоносные сообщения, открывающие злоумышленникам доступ во внутреннюю сеть организации, персонализируются с помощью данных, предварительно найденных в Интернете. Такие письма зачастую снабжены вложением, маскирующимся под невинный документ – привычный участник обмена в корпорациях и госструктурах. Получателя под тем или иным предлогом провоцируют открыть вложенный файл и загрузить вредоносное ПО, цель которого – кража конфиденциальной информации.

Проанализировав такого рода вредоносные рассылки, проведенные в феврале-сентябре 2012 года, Trend Micro обнаружила, что 94 % из них используют вредоносные вложения, а остальные снабжены ссылками на зараженные ресурсы. Вредоносные ссылки обычно предлагаются представителям активистских и прочих общественных организаций из разных стран. Опасные вложения, распространяемые при проведении целевых атак, используют такие форматы, как RTF (38 %), XLS (15 %), ZIP (13 %), RAR (11 %), PDF (8 %), DOC (7 %). Формат EXE редко встречается в целевых атаках, так как исполняемые файлы, присланные в виде вложения к письму, обычно блокируются на входе в корпоративную сеть.

Основными мишенями целевых спам-рассылок, по данным Trend Micro, являются правительственные организации и активистские группы. Информация о госслужбах и их составе обычно публикуется на общедоступных правительственных сайтах. Как оказалось, почти половина адресов получателей вредоносных e-mail посланий, зафиксированных экспертами, легко отыскивается простым обращением к Google. Больше половины тех e-mail, что не попали на страницы выдачи Google, можно было угадать, совместив имя адресата с почтовым доменом его компании, т.е. по образцу имя_получателя@имя_компании.com.

Ярким примером целевой атаки, начавшейся с узконаправленной спам-рассылки, является инцидент 2011 года, обернувшийся кражей уникальной технологии RSA.

Краткая справка. RSA – криптографический алгоритм с открытым ключом. Название представляет собой аббревиатуру, образованную первыми буквами фамилий Rivest, Shamir и Adleman, трех ученых из Массачусетского технологического института (MIT) , которые во второй половине 1970-х годов создали этот алгоритм. RSA стала первой криптосистемой, пригодной как для шифрования информации, так и для цифровой подписи.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел, скажем, *p* и *q*. Их произведение $n = p \cdot q$ задает нам алгебраический объект Z_n – так называемое кольцо вычетов по модулю *n*, в котором и будут производиться все вычисления. Для шифрования используется операция возведения в степень в кольце Z_n.

В начале восьмидесятых изобретатели алгоритма RSA основали компанию RSA Data Security, которая позже была поглощена компанией EMC.

Итак, кража технологических секретов RSA, которая заставила изрядно поволноваться всех клиентов компании EMC, обязана своим успехом одному из сотрудников компании, открывшему вредоносный файл, полученный в спаме.

Это был типичный пример целевой атаки, использующей приемы социальной инженерии и эксплойт нулевого дня. Неизвестные злоумышленники отослали ряд спам-сообщений, адресованных разным группам служащих EMC среднего звена. По всей видимости, этому предшествовал сбор личной информации сотрудников, опубликованной в Интернете – в первую очередь в социальных сетях. Авторам целевой спам-рассылки удалось заинтриговать лишь одного из получателей, но и этого оказалось достаточно. Письмо «План расширения кадрового состава в 2011 году» с вложенным в него зараженным xls-файлом было извлечено из «мусорной корзины», куда его направил защитный спам-фильтр, после чего xls-таблица была открыта.

В результате запуска эксплойта, внедренного в файл Excel[7], в систему был установлен «бэкдор» — один из вариантов Poison Ivy. Чтобы скрыть командный трафик, программа удаленного администрирования сама подключалась к центру управления для получения дальнейших инструкций. Проникнув во внутреннюю сеть EMC через эту брешь, хакеры начали поиск нужной информации и сотрудников с соответствующим уровнем доступа.

[7] Использовалась тогда еще не пропатченная уязвимость CVE-2011-0609.

Всё, что удалось скопировать из корпоративных хранилищ, злоумышленники вывели по ftp-каналам на сторонние (взломанные) серверы, скачали и удалили следы своего присутствия. Следует отметить, что с момента проникновения во внутреннюю сеть EMC незваные гости действовали очень оперативно. Защитные механизмы компании зафиксировали кибератаку, но оказались не в состоянии предотвратить кражу.

EMC не преминула поставить клиентов в известность о неприятном инциденте и начатом расследовании, а также заверить их, что принимает все надлежащие меры по усилению защиты своей IT-инфраструктуры. Представитель компании пояснил, что украденная информация касается технологии, заложенной в линейку продуктов SecurID — генераторов одноразовых паролей, карт персонального доступа к защищенным данным и прочих средств многоуровневой аутентификации. По мнению экспертов, последствия в виде целевых атак против систем SecurID на местах маловероятны. Тем не менее похищенные данные потенциально могут быть использованы для подавления конкретного механизма двухуровневой авторизации в ходе комплексной кибератаки.

При написании параграфа использована статья [KL_SecL_1].

Целевая атака с участием Android-троянца

На основе материалов статьи [KL_SecL_2].

В марте 2013 года был взломан электронный ящик известного тибетского активиста, и с него впоследствии совершались целевые фишинговые атаки против других активистов и правозащитников. Особенностью этих целевых атак является то, что рассылаемые злоумышленниками письма содержали вложение формата APK – зловред под Android. Фишинговые письма рассылались по списку контактов и выглядели так, как на рис. 4.1.

Что означает:

«22 марта 2013. Всемирный уйгурский конгресс

В беспрецедентной встрече действующих совместно ведущих уйгурских, монгольских, тибетских и китайских активистов, а также других ведущих международных экспертов, мы были глубоко тронуты колоссальным энтузиазмом, содействием и желанием всех присутствующих сделать данное событие по-настоящему значимым, чтобы в результате были бы приняты конкретные практические решения в ответ на наши общие трудности. Вложение представляет собой письмо от имени «Всемирного уйгурского конгресса» (WUC), «Организации наций и народов, не имеющих представительства» (UNPO) и «Общества народов, находящихся под угрозой» (STP)».

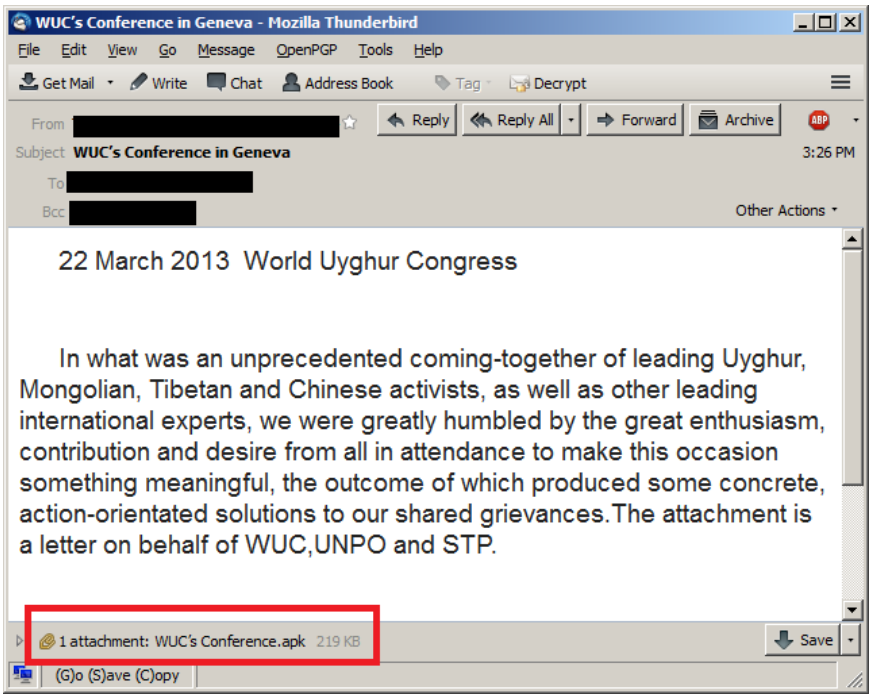


Рис. 4.1. Пример фишингового письма

Что касается Android Package (APK)-файла, то он был прикреплен к письму, и нес в себе Android-приложение под названием «WUC's Conference.apk». Этот вредоносный файл имеет размер в 334 326 байт. Распознается продуктами «Лаборатории Касперского» как «Backdoor.AndroidOS.Chuli.a».

Если открыть данный файл, то после установки вредоносного приложения на рабочем столе появляется приложение под названием «Conference» (рис. 4.2).

В результате запуска пользователем этого приложения, он видит текст, в котором сообщаются факты о предстоящей конференции в Женеве (рис. 4.3).

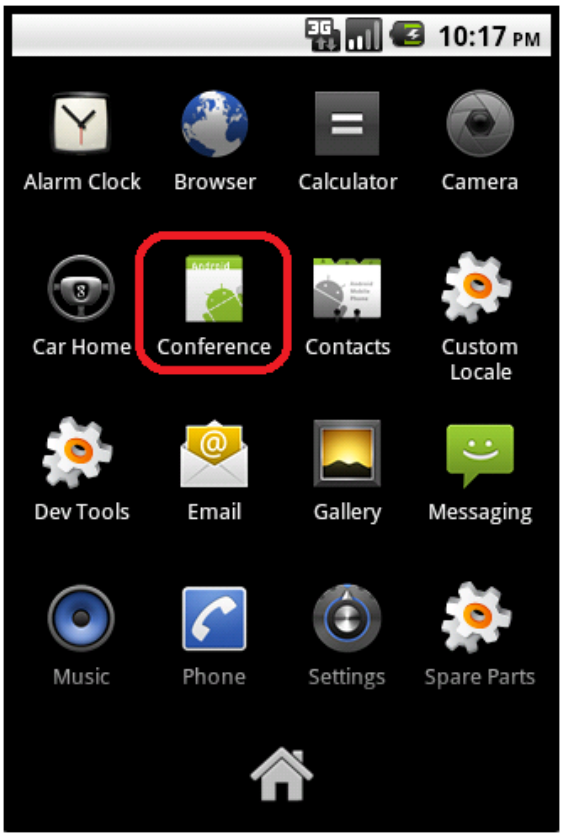


Рис. 4.2. Значок вредоносного ПО на рабочем столе

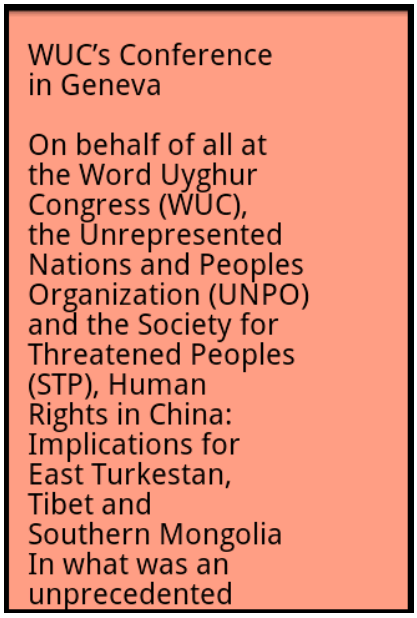


Рис. 4.3. Текст сообщения вредоносного ПО

Текст похож на текст из письма. В этом сообщении обращает на себя внимание ошибочное написание «Word» вместо «World».

В то время как пользователь читает это фальшивое сообщение, вредоносная программа тайно сообщает на командный сервер об успешном заражении, затем начинает собирать информацию, хранящуюся на устройстве. Собираются следующие данные:

- списки контактов (хранящиеся как на телефоне, так и на SIM-карте);
- журналы звонков;
- SMS-сообщения;
- данные геолокации;
- информация о телефоне (номер, версия ОС, модель телефона, версия SDK).

Важно отметить, что данные не загружаются на командный сервер автоматически. Троянец ожидает входящих SMS-сообщений и проверяет их на наличие одной из следующих команд: «sms», «contact», «location», «other». Если находится одна из этих команд, вредоносное ПО шифрует украденные данные при помощи системы Base64 и загружает их на командный сервер.

Командный сервер расположен по IP-адресу 64.78.161.133. Этот IP-адрес расположен в Лос-Анджелесе, США. Хостинг предоставляется компанией Emagine Concept Inc. Командный сервер работает под Windows Server 2003, настроен на китайский язык. По этому признаку и ряду других можно сделать вывод, что хакеры говорят на китайском языке.

На данный момент наилучшей стратегией защиты от аналогичных целевых атак будет избегание запуска любых APK-приложений, приходящих на мобильные телефоны через электронную почту.

Сетевой червь Stuxnet

На основе статей [KL_Main_1], [KL_SecL_4].

Одним из первых широко известных примеров кибершпионажа – новой современной и очень опасной угрозы в области компьютерной безопасности – является целевая атака сетевого червя Stuxnet (полное название: Worm.Win32.Stuxnet).

Stuxnet был обнаружен в июне 2010 года. Этот сетевой червь поражал компьютеры с установленной ОС MS Windows и использовал сразу четыре неизвестные на то время уязвимости этой операционной системы. Главный антивирусный эксперт «Лаборатории Касперского» Александр Гостев отмечает, что «факт наличия сразу четырех уязвимостей, впервые использованных в Stuxnet, делает данную вредоносную программу действительно уникальным явлением в истории. До сих пор нам не приходилось сталкиваться с угрозами, которые содержали бы в себе столько сюрпризов. Стоит отметить и очень высокий уровень программирования, продемонстрированный авторами червя» [KL_SecL_4].

Компьютерный червь Stuxnet примечателен тем, что, являясь по сути, инструментом промышленного шпионажа, – он предназначен для получения доступа к системе Siemens WinCC, которая отвечает за сбор данных и оперативное диспетчерское управление производством.

Для своего распространения по сети Stuxnet, в первую очередь, использует уязвимость в службе «Диспетчер печати» («Print Spooler») Windows, которая позволяет передать и выполнить вредоносный код на удаленном компьютере. Исходя из особенностей уязвимости, заражению подвержены компьютеры, использующие принтер и предоставляющие к нему общий доступ. Заразив компьютер внутри локальной сети, через данную лазейку Stuxnet пытался проникнуть на другие машины.

Упомянутые уязвимости в Windows были обнаружены и устранены в ходе сотрудничества «Лаборатории Касперского» и Microsoft.

Сразу после обнаружения уязвимости эксперты «Лаборатории Касперского» уведомили Microsoft о найденной проблеме; их выводы были подтверждены специалистами производителя ОС. Уязвимость классифицирована как Print Spooler Service Impersonation Vulnerability, и ей был присвоен статус критической. В Microsoft немедленно приступили к созданию соответствующего патча MS10-061, который был выпущен 14 сентября 2010 г.

Кроме того, специалисты «Лаборатории Касперского» обнаружили еще одну уязвимость «нулевого дня», относящуюся к классу Elevation of Privilege, которая использовалась червем для получения полного контроля над зараженной системой. Вторая аналогичная уязвимость (EoP) была обнаружена специалистами Microsoft. Обе уязвимости были исправлены в обновлениях для ОС Windows.

Червь Worm.Win32.Stuxnet успешно детектируется и нейтрализуется всеми продуктами «Лаборатории Касперского».

2011 год: компьютерный червь Duqu

Еще в 2010 году, во время анализа Stuxnet, эксперты «Лаборатории Касперского» пришли к выводу, что имеют дело с платформой-носителем, к которой был добавлен отдельный модуль, отвечавший за работу с PLC[8].

По сути, Stuxnet был настоящей ракетой – у нее был разгонный модуль (собственно червь) и боеголовка (блок для SCADA/PLC[9]).

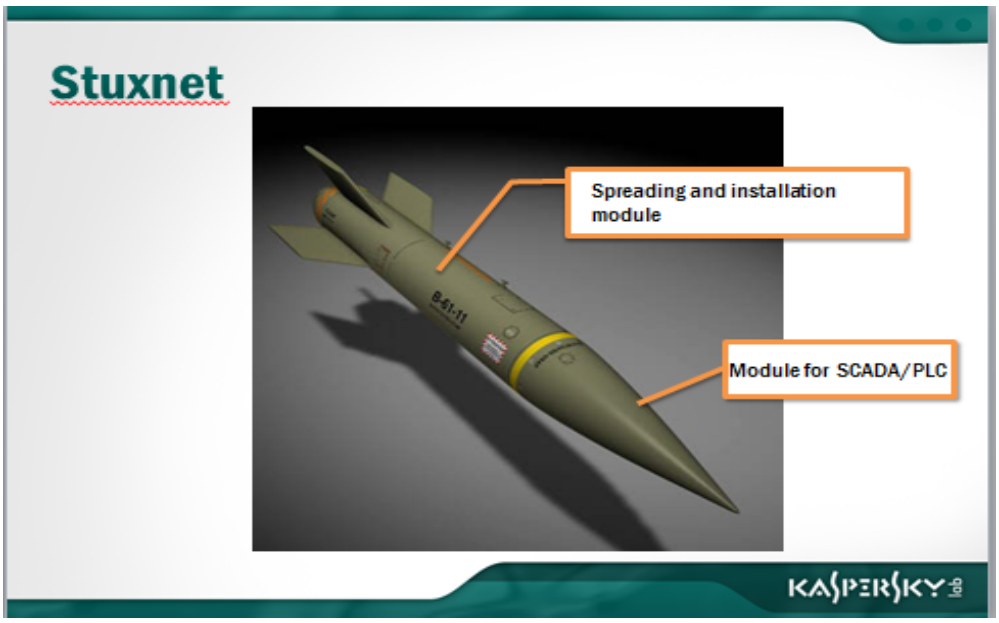


Рис. 4.4. Stuxnet

Специалисты «Лаборатории Касперского» предположили, что Stuxnet, вероятно, разрабатывался двумя разными командами, которые могли даже не знать о существовании друг друга или о цели проекта.

Часть, отвечающую за распространение червя и его работу в системе, могли использовать снова, но уже с другой «боеголовкой». Это и произошло с Duqu. Точнее, в свет была выпущена версия без «боеголовки» – но с возможностью установки любой «боеголовки» в любой момент времени против любой конкретной цели.

[8] PLC (programmable logic controller) – программируемый контроллер – электронная составляющая промышленного контроллера, специализированного (компьютеризированного) устройства, используемого для автоматизации технологических процессов.

[9] SCADA (supervisory control and data acquisition) – программный пакет, целью которого является выполнение функций диспетчерского управления и сбора данных.

Прежде всего, необходимо внести ясность в некоторую путаницу с именами файлов и самими файлами, относящимися к данной истории. Название «Duqu» не имеет никакого отношения к той части вредоносной программы, которая представляет из себя модуль доставки. Дело в том, что доставленная этим модулем на компьютер вредоносная программа троянец-шпион в ходе своей работы сохраняет собранные данные в файлы с именами вида ~DQx.tmp. Из этого расширения DQ и возникло название вируса. Что касается функционала троянца, то это совершенно самостоятельная вредоносная программа, которая может работать и без основного модуля доставки. Точно так же, как и основной модуль может работать без наличия в системе троянца-шпиона.

Количество инцидентов

В конце 2011 года авторы Duqu попытались уничтожить все следы своей деятельности. Были очищены все серверы, которые они использовали как минимум с 2009 года. Всего, основываясь на данных «Лаборатории Касперского» и данных, полученных из Symantec, на март 2012 года был зафиксирован 21 инцидент Duqu [KL_SecL_8].

Некоторые из модификаций Duqu, которые будут описаны ниже, несмотря на разные файлы, были обнаружены в ходе расследования одних и тех же инцидентов. Соответственно такие модификации объединены в один инцидент.

Большинство жертв Duqu находится в Иране (рис. 4.5).

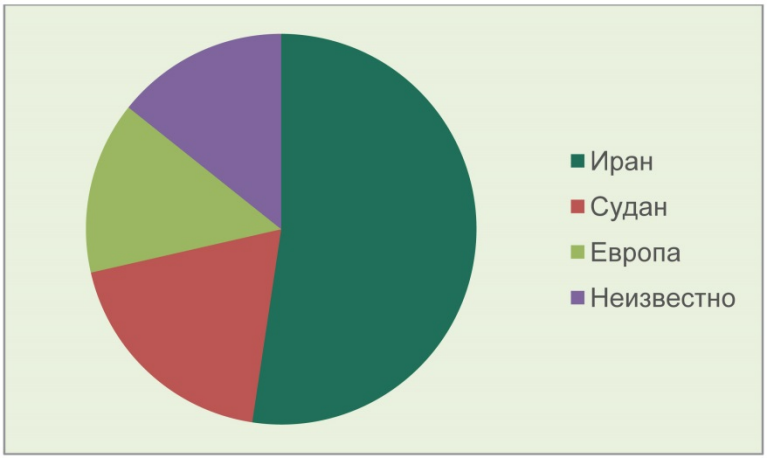


Рис. 4.5. Географическое распределение инцидентов Duqu

Анализ деятельности организаций-жертв и характер информации, интересовавшей авторов Duqu, свидетельствует, что основной целью атакующих в иранских инцидентах была любая информация о системах управления производством в раз-

личных отраслях промышленности Ирана, а также информация о торговых отношениях ряда иранских организаций.

Несомненно, что число атакованных Duqu больше, однако специалисты «Лаборатории Касперского» полагают, что оно вряд ли превышает несколько десятков.

При написании раздела использованы материалы статьи [KL_SecL_5].

Flame: новый виток в истории кибершпионажа

В 2012 году было обнаружено самое, пожалуй, изощренное кибероружие из всех, с чем приходилось сталкиваться до тех пор, – червь Flame. Это вредоносное ПО, созданное для кибершпионажа, попало в поле зрения экспертов «Лаборатории Касперского» при проведении исследования по запросу Международного союза электросвязи (МСЭ), обратившегося к компании за содействием в поиске неизвестной вредоносной программы, которая удаляла конфиденциальные данные с компьютеров, расположенных в странах Ближнего Востока.

В процессе расследования специалистам «Лаборатории Касперского» удалось выявить некоторые отличительные черты модулей Flame. Основываясь на этих чертах, они обнаружили, что в 2009 году в состав первого варианта червя Stuxnet входил модуль, созданный на платформе Flame. Это подтвердило, что группы, которые создавали платформы Flame и Stuxnet/Duqu, каким-то образом взаимодействовали между собой [KL_SecL_9].

Без сомнения, Flame является одной из самых сложных киберугроз за всю историю их существования. Программа имеет большой размер и невероятно сложную структуру. Она заставляет переосмыслить такие понятия, как «кибервойна» и «кибершпионаж».

Что именно представляет собой Flame? Каков его функционал?

Flame представляет собой весьма хитрый набор инструментов для проведения атак, значительно превосходящий по сложности Duqu. Это троянская программа – «бэкдор», имеющая также черты, свойственные червям и позволяющие ей распространяться по локальной сети и через съемные носители при получении соответствующего приказа от ее хозяина.

Исходная точка входа Flame неизвестна – но есть основание подозревать, что первоначальное заражение происходит путем целевых атак. После заражения системы Flame приступает к выполнению сложного набора операций, в том числе к анализу сетевого трафика, созданию снимков экрана, аудиозаписи разговоров, пе-

рехвату клавиатурных нажатий и т.д. Все эти данные доступны операторам через командные серверы Flame.

В дальнейшем операторы могут принять решение о загрузке на зараженные компьютеры дополнительных модулей, расширяющих функционал Flame. Всего имеется около 20 модулей с различным назначением.

Насколько сложен Flame?

Прежде всего, Flame – это огромный пакет, состоящий из программных модулей, общий размер которых при полном развертывании составляет почти 20 МБ. Вследствие этого анализ данной вредоносной программы представляет огромную сложность. Причина столь большого размера Flame в том, что в него входит множество разных библиотек, в том числе для сжатия кода (zlib, libbz2, ppmd) и манипуляции базами данных (sqlite3), а также виртуальная машина Lua.

Lua – это скриптовый язык, т.е. язык программирования, легко поддающийся расширению и интеграции с кодом, написанным на языке C. Для многих компонентов Flame логика верхнего уровня написана на Lua – при этом подпрограммы и библиотеки, непосредственно реализующие заражение, компилируются с C++.

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
        end
```

Рис. 4.6. Декомпилированный код Flame на языке Lua

По сравнению с общим объемом кода часть, написанная на Lua, относительно невелика. По нашей оценке, объем разработки на Lua составляет порядка 3000 строк кода. Для среднего разработчика на создание и отладку такого объема кода требуется около месяца.

Кроме того, вредоносная программа использует для внутренних нужд локальные базы данных с вложенными SQL-запросами, применяет несколько методов шифрования, различные алгоритмы сжатия, создает скрипты с помощью Windows Management Instrumentation, использует пакетные скрипты и т.д.

Запуск и отладка вредоносного ПО – нетривиальная задача, поскольку вредоносная программа представляет собой не обычный исполняемый файл, а несколько DLL-библиотек, загружаемых при запуске операционной системы.

В целом можно констатировать, что Flame – одна из наиболее сложных угроз, обнаруженных на сегодняшний день.

В чем основные отличия Flame от других троянцев-бэкдоров?

Прежде всего, для вредоносного ПО нехарактерно использование Lua. Достаточно большой размер набора инструментов для проведения атак также нетипичен для вредоносного ПО. Как правило, современные вредоносные программы имеют небольшой размер и пишутся на языках программирования, обеспечивающих максимальную компактность, что помогает скрыть присутствие этих программ в системе. Сокрытие с помощью большого объема кода – это новая черта, реализованная в Flame.

Запись аудиоданных со встроенного микрофона – тоже достаточно новый прием. Конечно, существуют и другие вредоносные программы, способные записывать аудио, однако ключ в универсальности Flame – способность этой вредоносной программы красть данные столь разнообразными способами.

Еще одна любопытная функция Flame – использование Bluetooth в устройствах, поддерживающих такой способ передачи данных. Если Bluetooth поддерживается зараженным компьютером и включен в настройках, программа собирает информацию об обнаруживаемых устройствах, находящихся вблизи зараженной машины. Если в конфигурации включены соответствующие настройки, Flame может превратить зараженную машину в радиомаяк, настроив разрешение на его обнаружение другими Bluetooth-устройствами и сообщая общие данные о состоянии заражения, зашифрованные в передаваемой по Bluetooth информации об устройстве.

Программа способна записывать аудиосигнал через микрофон, если таковой имеется. Записанный звук хранится в сжатом формате, причем сжатие обеспечивается с помощью общедоступной библиотеки. Записанные аудиоданные регулярно, по расписанию, скрытым образом пересылаются на командный сервер через SSL-канал.

Вредоносная программа способна также регулярно делать снимки экрана; более того, она делает скриншоты в процессе работы определенных «интересных» приложений, таких как системы мгновенного обмена сообщениями. Снимки экрана хранятся в сжатом формате и регулярно пересылаются на командный сервер – так же, как и аудиозаписи.

По наблюдениям специалистов «Лаборатории Касперского», хозяева Flame искусственно поддерживают количество зараженных систем на некоем постоянном уровне. Это можно сравнить с последовательной обработкой полей: они заражают несколько десятков машин, затем проводят анализ данных, взятых на компьютерах жертв, деинсталируют Flame из систем, которые им неинтересны, и оставляют в наиболее важных, после чего начинают новую серию заражений.

География распространения Flame

На рис. 4.7 представлены семь стран, подвергшихся наибольшему количеству атак.

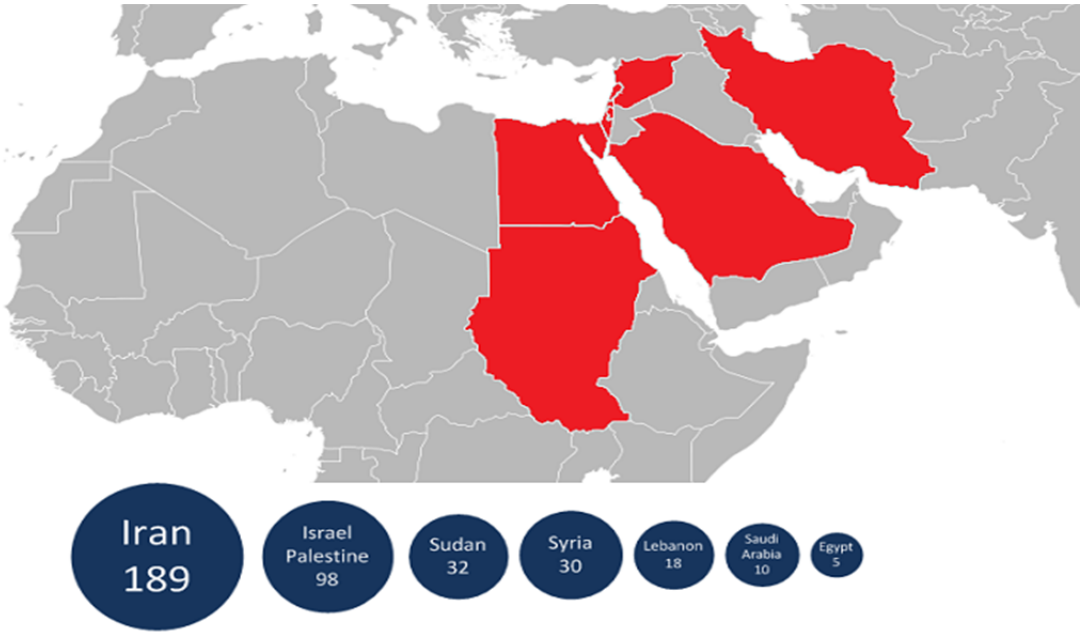


Рис. 4.7. География распространения Flame

Нацелен ли Flame на конкретные организации?

Первоначальный анализ указывает на то, что создатели Flame стремятся получить любые данные: электронные письма, документы, сообщения, разговоры на территории секретных объектов – практически всё. Нет каких-либо указаний на кон-

кретную цель Flame, скажем, на энергетическую отрасль. Это позволяет считать, что Flame является универсальным набором инструментов для проведения атак, разработанным для кибершпионажа в широком смысле.

Если анализировать организации, на которые нацелен Flame, то очевидной системы также не наблюдается. Спектр жертв широк – от отдельных личностей до некоторых окологосударственных организаций и образовательных учреждений.

При написании раздела использованы материалы статьи [KL_SecL_10].

Gauss

На основе материалов статьи [KL_SecL_11].

Gauss – новейшая система кибер-слежки, открывшая еще одну страницу в саге о Stuxnet, Duqu и Flame. Вредоносная программа, по-видимому, была создана в середине 2011 года и впервые применена в августе-сентябре того же года.

Gauss представляет собой «банковский» троянец, созданный государством, и инфицирующий компьютеры на базе Windows. В сравнении с другими «банковскими» троянцами, Gauss, вероятно, подвергся «тонкой настройке» в том смысле, что он не нацелен на сотни финансовых учреждений, а рассчитан на несколько избранных систем (в частности, на Citibank и PayPal). Gauss содержит отдельный зашифрованный код, который записывается на USB-накопители при подключении устройства к зараженной системе. Если накопитель подключается к незараженному компьютеру, вредоносное ПО осуществляет сканирование системных настроек для определения ОС, сетевых папок, данных прокси-серверов и истории посещения страниц. Далее вирус сопоставляет проверенные данные с информацией, заложенной во вредоносном коде. Если сопоставление не было найдено, троянец удаляет себя, чтобы избежать обнаружения.

Вредоносная программа устанавливает до восьми отдельных модулей на целевую машину. Модули нацелены на хищение CMOS- и BIOS-данных, информации о сетевых интерфейсах, доменах и дисках. Помимо этого, они также устанавливают плагины, которые отслеживают историю просмотра web-страниц пользователя и собирают пароли. Остальные модули контролируют деятельность вируса, а также отвечают за установку других вредоносных программ, цель которых в настоящее время неизвестна.

Программа Gauss была обнаружена в ходе расследования, которое проводилось по инициативе Международного союза электросвязи (МСЭ). Цель проводимой работы – снижение рисков, которые несет кибероружие. Это ключевой элемент усилий по достижению главной цели – мира в глобальном киберпространстве.

Обнаружение Gauss ознаменовало собой новый уровень в осознании угрозы, связанной с кибероружием. Важно отметить, что Gauss базируется на платформе Flame, таким образом, оба проекта по разработке вредоносного ПО – Gauss и Flame – связаны между собой. Программа имеет общие функциональные элементы с Flame, такие, как, например, подпрограммы заражения USB-носителей.

С конца мая 2012 года облачным защитным сервисом «Лаборатории Касперского» зарегистрировано более 2500 заражений Gauss; при этом, по оценкам Лаборатории, общее реальное число жертв вредоносной программы измеряется десятками тысяч.

Как и в случае с Flame, по-прежнему неизвестно, каким образом компьютеры жертв заражаются Gauss. Антивирусные аналитики не обнаружили механизма самораспространения (как у червей) в Gauss, однако большее число жертв, чем у Flame, может указывать на наличие функции самораспространения.

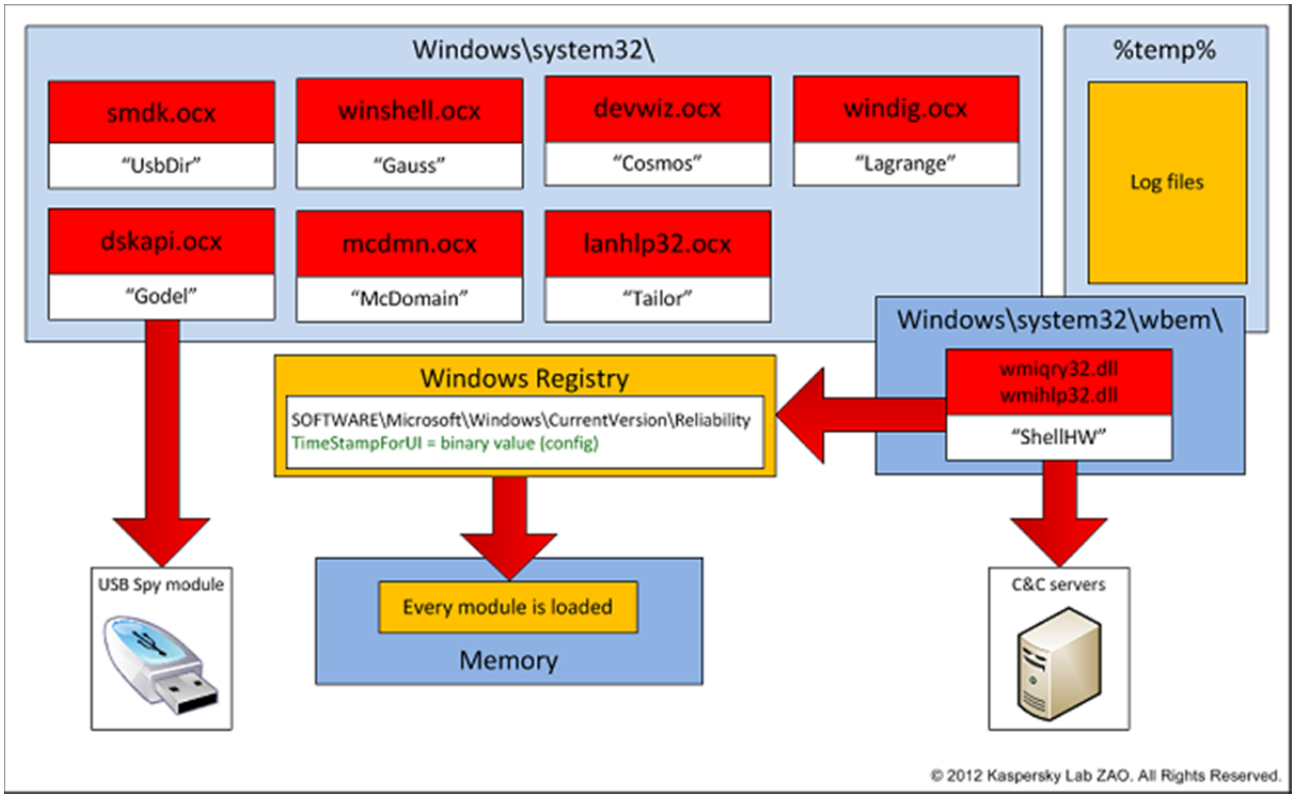


Рис. 4.8. Архитектура вредоносного комплекса Gauss

Строго говоря, Gauss – это даже не вредоносная программа, а вредоносный комплекс программ, который имеет модульную структуру и поддерживает удаленное развертывание операторами нового функционала, который реализуется в виде дополнительных модулей. Эти модули выполняют:

- перехват cookie-файлов и паролей в браузере;
- сбор и отправку злоумышленникам данных по конфигурации системы;
- заражение USB-носителей модулем, предназначенным для кражи данных;
- создание списков содержимого системных накопителей и папок;
- кражу данных, необходимых для доступа к учетным записям различных банковских систем, действующих на Ближнем Востоке;
- перехват данных по учетным записям в социальных сетях, почтовым сервисам и системам мгновенного обмена сообщениями.

Как видно из рис. 4.8, большинство модулей вредоносного комплекса названо именами известных математиков – Гаусса, Лагранжа, Гёделя, Тэйлора. Модуль под названием Gauss – наиболее важный элемент вредоносной системы, поскольку в нем реализованы возможности, связанные с кражей банковских данных, поэтому весь вредоносный комплекс также был назван по имени этого компонента.

Таинственный вирус Wiper

В апреле 2012 года было опубликовано несколько сообщений о таинственной атаке с использованием вредоносного ПО, которая привела к отказу компьютерных систем в компаниях по всему Ирану.

В нескольких статьях говорилось, что ответственность за атаки лежит на вирусе под названием Wiper (в переводе – чистильщик). Однако не было найдено ни одного образца вредоносной программы, использованной в этих атаках, что заставило многих усомниться в точности сведений, содержащихся в этих сообщениях.

После этих инцидентов Международный союз электросвязи (МСЭ) обратился к «Лаборатории Касперского» с просьбой провести расследование данных инцидентов и определить потенциальные деструктивные последствия активности этого нового вредоносного ПО.

В процессе расследования таинственной апрельской вредоносной атаки экспертам «Лаборатории Касперского» удалось получить и проанализировать образы нескольких жестких дисков, атакованных Wiper. Теперь можно с уверенностью утверждать, что инциденты действительно имели место, и что вредоносная программа, использованная в этих атаках, существовала в апреле 2012 года. Кроме того, стало известно о нескольких очень похожих инцидентах, имевших место с декабря 2011 года.

Создатели Wiper сделали все возможное, чтобы уничтожить абсолютно все данные, которые можно было бы использовать для анализа инцидентов. Поэтому в каждом из случаев, которые были проанализированы, после активации Wiper от

вредоносной программы не оставалось почти никаких следов. Здесь важно подчеркнуть, что именно «почти никаких», потому что кое-какие следы всё же остались, и они позволили экспертам лучше понять, как осуществлялись эти атаки.

В результате проведенного анализа было установлено, что у Wiper, с одной стороны, и у Duqu и Stuxnet, с другой, использовались одинаковые схемы именования файлов, что дало основания предположить о возможной связи между этими программами, однако факт наличия такой связи нельзя признать наверняка.

Новая вирусная суперугроза «Маска»

По материалам статьи [KL_Blog_1].

Много лет полным ходом прямо на наших глазах идет масштабный, можно даже сказать, глобальный, конфликт. Но происходит он не на улицах, и предметом битвы является не захват чужой территории. Всё гораздо интереснее: мы живем во время ожесточенных боевых действий, происходящих исключительно в рамках киберпространства, за один-единственный ресурс – информацию. И главным оружием в этой войне выступает кибершпионаж.

В предыдущих разделах мы рассказывали о том, как за последние годы разными специалистами в области кибербезопасности была обнаружена и обезврежена целая плеяда мощных шпионских программ: Stuxnet, Flame, Duqu и Gauss. И вот теперь благодаря исследователям из «Лаборатории Касперского» к этому списку прибавилось еще одно имя – Careto, что в переводе с испанского означает «маска» или «уродливое лицо». По словам экспертов, данная вредоносная программа, ставшая основной для глобальной сети кибершпионажа, является одной из самых сложных и искусно выполненных на сегодняшний день[10]. Что она собой представляет, как работает и кто за всем этим стоит? Разберемся по порядку.

«Маска» – чрезвычайно сложное и профессионально разработанное вредоносное ПО, используемое для кибершпионажа как минимум с 2007 года. Основными мишенями Careto являются преимущественно государственные учреждения, энергетические предприятия, исследовательские институты и частные инвестиционные фонды. Всего же, по предварительным данным, существует не менее 380 уникальных жертв из 31 страны (включая США, Китай и многие европейские государства), чьи компьютеры были атакованы «Маской». Причем есть основания полагать, что это лишь верхушка айсберга.

[10] Февраль 2014 года.


«МАСКА»
Завоевание кибермира
Пострадавшие страны: 31
Количество зараженных IP-адресов: 1000+
ГОДЫ СОЗДАНИЯ МОДУЛЕЙ «МАСКИ»:
2013
2012
2011
2010
2009
2008
2007
ШВЕЙЦАРИЯ 33
Берн
ВЕЛИКОБРИТАНИЯ 109
Лондон
США 22
Вашингтон
БРАЗИЛИЯ 137
Бразилия
Париж
МАРОККО 384
Рабат
ФРАНЦИЯ 53
ИСПАНИЯ 51
Мадрид
Тунис
ТУНИС 3
Триполи
ЛИВИЯ 26
Претория
Каракас
Тегеран
ЮАР 4
ИРАН 13
Каир
ЕГИПТ 2
ВЕНЕСУЭЛА 4
Брюссель
БЕЛЬГИЯ 3
Анкара
ТУРЦИЯ 3
Сан-Хосе
ГИБРАЛТАР 2
КОСТА-РИКА 1
ИРАК 1
ПОЛЬША 2
Варшава
Алжир
Берлин
ГЕРМАНИЯ 3
Багдад
Гавана
АЛЖИР 1
МЕКСИКА 1
КУБА 1
Пекин
КИТАЙ 1
Мехико
Буэнос-Айрес
АРГЕНТИНА 1
— Активисты
— Частные компании
— Правительственные органы
— Образовательные учреждения
— Дипломатические организации
— Финансовые/Инвестиционные компании
KASPERSKY

Рис. 4.9. «Маска»

Основа распространения «Маски» – это фишинговые сообщения. В них встроены ссылки на вредоносные сайты, на которых содержатся эксплойты, рассчитанные на разные конфигурации атакуемого компьютера. После попадания в систему Careto берет контроль над всеми каналами обмена информацией и начинает перехватывать определенные данные. Обнаружить шпиона при этом крайне трудно: вредоносное ПО эффективно прячется в системе и практически не выдает своего присутствия даже во время активной работы. Ситуацию усугубляет еще и тот факт, что встроенные функции «Маски» могут дополняться модулями, значительно расширяющими возможности этой программы. Практически это позволяет злоумышленникам совершать любые зловредные действия на пораженной системе.

На сегодняшний день точно известно о существовании версий «Маски» под Windows и Mac OS X. Заражение Linux также вероятно, но точного подтверждения этому пока нет. Кроме того, анализ командных серверов злоумышленников выявил возможность существования угрозы для устройств на базе iOS и Android.

Careto способен собирать целый ряд данных, в том числе ключи шифрования, файлы конфигурации VPN, текстовые документы, таблицы и т.д. «Маске» были доступны и специфические файлы с неизвестными расширениями, которые предположительно могут являться инструментами шифрования военного уровня.

Определить автора «Маски» – задача чрезвычайно сложная, и улик, явно указывающих на определенного человека или круг лиц, пока не найдено. Анализ кода программы дает все основания полагать, что родным языком создателей Careto является испанский, однако точно определить страну происхождения пока не представляется возможным.

В то же время некоторые факты, в том числе нетипичный для обычных киберпреступников исключительный профессионализм в выполнении атак и уровне самозащиты, выявленные при анализе «Маски», позволяют предполагать, что данная кампания поддерживалась одним из государств.

Активность «Маски» прекратилась в январе 2014 года, когда эксперты «Лаборатории Касперского» проводили расследование, подключившись к командным серверам. Учитывая, что кампания длилась как минимум с 2007 года, а ее заказчики и исполнители пока остаются неизвестны, активность вредоносной программы может возобновиться.

Впрочем, текущие версии продуктов «Лаборатории Касперского» успешно обнаруживают и удаляют все известные версии Careto.

Контрольные вопросы

1. В чем особенность целевых атак?
2. Чем примечателен сетевой червь Stuxnet?
3. Каков функционал Flame? В чем отличие этого вредоносного ПО от других троянцев-бэкдоров?
4. Расскажите о банковском троянце Gauss.
5. Каковы основные мишени вредоносного ПО «Маска»? Как оно распространяется? Для каких операционных систем существуют версии «Маски»? Каков функционал этого вредоносного ПО?

Глоссарий

Б

Ботнет – сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor'ы позволяют киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются ботами.

«Бэкдоры» (Backdoor)

Являются разновидностью троянских программ, предоставляющих злоумышленнику возможность несанкционированного удаленного управления зараженным компьютером.

Доступные злоумышленнику действия определяются функционалом подобной программы. Как правило, злоумышленник может принимать и отсылать файлы, запускать и уничтожать их, выводить различные сообщения, стирать информацию, перезапускать компьютер и т. п. Таким образом, «бэкдоры» могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и пр.

В

Вирус (классический вирус)

К данной категории относятся вредоносные программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от сетевых червей компьютерные вирусы не используют сетевых сервисов для проникновения на другие компьютеры.

Вирус-полиморфик (полиморфный вирус)

Вирус, предпринимающий специальные меры для затруднения своего обнаружения и анализа. Не имеет сигнатур, т. е. не содержит ни одного постоянного участка кода.

В большинстве случаев два образца одного и того же вируса-полиморфика не будут иметь ни одного совпадения. Достигается это за счет шифрования основного тела вируса и существенной модификации от копии к копии модуля-расшифровщика.

Вирус резидентный – вирус, загружающий в оперативную память компьютера резидентную часть, которая постоянно присутствует в оперативной памяти до перезагрузки или выключения компьютера. Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу.

З

Зловред – русскоязычная калька со слова Malware – вредоносное ПО.

К

Компьютерный червь

К данной категории относятся программы, распространяющие свои копии по локальным и (или) глобальным сетям.

Большинство известных сетевых червей распространяются в виде файлов: вложений в электронные письма, ссылкой на зараженный файл на каком-либо веб- или FTP-ресурсе, в ICQ-сообщениях и пр.

Некоторые сетевые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

М

Макровирус – разновидность компьютерных вирусов, написанных на макроязыках.

Макрос – программный алгоритм действий, набор инструкций, записанный пользователем. Служит для автоматизации действий (например, в программах Word или Excel).

Макроязык – набор правил для объявления и использования макросов.

О

Обратная разработка (программы) – исследование программы с целью понять принцип ее работы.

Обфускация – совокупность приемов запутывания исходного кода программы, имеющих целью максимально затруднить его чтение и анализ, но полностью сохранить функциональность.

П

Песочница – в компьютерной безопасности механизм для безопасного исполнения программ. Обычно представляет собой жестко контролируемый набор ресурсов для исполнения гостевой программы – например, место на диске или в памяти [Wik].

Поведенческий блокиратор определяет, является ли программа вредоносной, исходя из ее поведения в системе. Если программа выполняла действия, не разрешенные правилами, определенными заранее, то выполнение этой программы блокируется.

Полиморфный вирус – см. вирус-полиморфик.

С

Серверное программное обеспечение (сервер) – программный компонент вычислительной системы, выполняющий сервисные (обслуживающие) функции по запросу клиента, предоставляя ему доступ к определенным ресурсам или услугам.

Сигнатура атаки – сигнатура, образец IP-пакета данных, характерного для какой-либо определенной хакерской атаки. Блокируя подобные IP-пакеты, можно останавливать атаки, не нарушая при этом работоспособность сетевого подключения.

Сигнатура вируса – фрагмент кода компьютерного вируса, который позволяет его идентифицировать.

«Стелс»-вирусы (вирусы-невидимки) – программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме того, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы. К «стелс»-вирусам относятся вирусы «Frodo», «Fish#6», «Brain» и некоторые другие.

Социальная инженерия – комплекс нетехнических методов, применяемых с целью заставить пользователей пренебречь стандартными мерами безопасности. В контексте вирусов и червей это, как правило, означает прикрепление вредоносного кода к совершенно безобидному на первый взгляд почтовому сообщению.

Т

Троянская программа

Вредоносная программа, которая не обладает способностью к самораспространению, в отличие от вирусов и червей, которые распространяются самопроизвольно.

Ф

Фишинг

Компьютерное преступление, мошенничество, основанное на принципах социального инжиниринга. Злоумышленником создается практически точная копия сайта выбранного банка. Затем при помощи спам-технологий рассылается письмо, составленное таким образом, чтобы быть максимально похожим на настоящее письмо от выбранного банка. Используются логотипы банка, имена и фамилии реальных руководителей банка.

В таком письме, как правило, сообщается о том, что из-за смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя ПО банка или же нападение хакеров.

Х

Хеш

Хешем называется результат обработки неких данных хеш-функцией. Хеш-функция – это преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

Ц

Целевая атака

Эта атака характеризуется тем, что специально нацелена на конкретную жертву, в качестве которой может выступать один человек, группа людей, компания или государственная структура. Для такого рода атак не характерна массовость. Опасность целевой атаки состоит, прежде всего, в том, что она разработана специально для жертвы. Проводится такая атака, как правило, тихо и незаметно.

Э

Эвристический анализ

Относится к несигнатурным технологиям детектирования. Методы эвристического анализа основаны на сравнении исследуемого кода с характеристиками уже известных вирусов с помощью правил эвристической верификации – знаний о механизме полиморфизма сигнатур.

В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода считывает инструкции в буфер антивируса, разбирает их на инструкции и производит их исполнение по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет ее с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала – программа определена [Wik].

Эксплойт – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

Эксплойт нулевого дня – киберугроза, использующая ошибку или уязвимость в приложении или операционной системе и появившаяся сразу после обнаружения данной уязвимости, пока разработчики ПО еще не успели создать патч, а IT-администраторы – принять другие меры безопасности.

Эмуляторы – модули, которые осуществляют исполнение программного кода в изолированной среде для последующего анализа его поведения.

D

DoS-атака (Denial of Service , атака типа «отказ в обслуживании») – атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен.

DDoS-атака (Distributed Denial of Service) – разновидность DoS-атаки, которая выполняется одновременно с большого числа компьютеров.

DNS (Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах. Распределенная база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определенному протоколу.

I

IIS (Internet Information Services) – набор серверов для нескольких служб Интернета от компании Майкрософт. IIS распространяется с операционными системами семейства Windows NT.

Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP.

M

Malware – сокращение от Malicious Software – вредоносное ПО.

Литература

[LK09] «Компьютерные угрозы: методы обнаружения и анализа», Москва, 2009. ЗАО «Лаборатория Касперского». Составитель: А. Адамов.

[Bur89] R.Burger «Computer Viruses: A High-Tech Disease», 1989. Published by Abacus Software.

[Coh83] F. Cohen. Computer Viruses // ASP Pittsburgh, 1985 (текст диссертационной работы на получение степени PhD).

[Coh87] F. Cohen: «Computer Viruses – Theory and Experiments», 1987, Computers & Security 6, pp.22-35, Elsevier Science Publishers B.V. (North-Holland).

[Neu66] von Neumann, J. «Theory of Self-Reproducing Automata», 1966. Edited and completed by A.W. Burks. Urbana, Illinois: University of Illinois Press.

[Pen59] L. S. Penrose, «Self-Reproducing Machines», Scientific American, vol. 202, pp. 105-114, 1959.

Интернет-источники

[KL_SecL] Сайт http://www.securelist.com/ ЗАО «Лаборатория Касперского».

[KL_SecL_1] www.securelist.com, «Целевая атака начинается с поддельного письма», Татьяна Никитина, 06.12.2012.

[KL_SecL_2] www.securelist.com, «Целевая атака с участием Android-троянца», Курт Баумгартнер, Костин Раю и Денис Масленников, 28.03.2013.

[KL_SecL_3] www.securelist.com, «Flashfake – Mac OS X ботнет», Игорь Суменков, 09.04.2012.

[KL_SecL_4] www.securelist.com, «Мирт и гуава: Эпизод MS10-061», Александр Гостев, 14.09.2010.

[KL_SecL_5] www.securelist.com, «Тайна Duqu: часть первая», Александр Гостев, 20.10.2011.

[KL_SecL_6] www.securelist.com, «Kaspersky Security Bulletin 2013. Основная статистика за 2013 год», 11.12.2013.

[KL_SecL_7] www.securelist.com, Раздел «Детектируемые объекты».

[KL_SecL_8] www.securelist.com, «Тайна Duqu: часть десятая», Александр Гостев, 27.03.2010.

[KL_SecL_9] www.securelist.com, «miniFlame, он же SPE: «Элвис и его друзья»», 15.10.2012.

[KL_SecL_10] www.securelist.com, «Flame: часто задаваемые вопросы», Александр Гостев, 30.05.2012.

[KL_SecL_11] www.securelist.com, «Gauss: государственный кибершпионаж плюс «банковский» троянец», 13.08.2012.

[KL_SecL_12] www.securelist.com, «Спам в феврале 2014», Мария Вергелис, Татьяна Щербакова, 20.03.2014.

[KL_SecL_13] www.securelist.com, «Вирусы и антивирусы: гонка вооружений», Дэвид Эмм, 17.04.2008.

[KL_SecL_14] www.securelist.com, «Контроль запуска программ как залог безопасности сети. Часть 1», Андрей Ефремов, Владимир Заполянский, 19.02.2013.

[KL_SecL_15] www.securelist.com, «Что это там был за Wiper?», исследовательский центр «Лаборатории Касперского» (GReAT), 29.08.2012.

[KL_Main] Сайт http://www.kaspersky.ru/ ЗАО «Лаборатория Касперского».

[KL_Main_1] www.kaspersky.ru, «Новая Windows-уязвимость, используемая Stuxnet, закрыта при сотрудничестве «Лаборатории Касперского» и Microsoft», 15.09.2010.

[KL_Blog] Сайт http://blog.kaspersky.ru/ ЗАО «Лаборатория Касперского».

[KL_Blog_1] http://blog.kaspersky.ru/, «Кто прячется за «Маской»?», 11.02.2014.

[KL_Blog_2] http://blog.kaspersky.ru/, «Как защититься от сложных атак?», 01.10.2013.

[Wik] http://www.wikipedia.org/

[YTb1] http://www.youtube.com/watch?v=lnedOWfPKT0

[CE1] http://www.computereconomics.com/article.cfm?id=133

Полезные ссылки

[KL_Acad] Сайт http://academy.kaspersky.com/ ЗАО «Лаборатория Касперского».

[KL_Acad_FcBk] «Kaspersky Academy» в facebook:
https://www.facebook.com/KasperskyStudentConference?ref=profile

[KL_FcBk] «Лаборатория Касперского» в facebook:
https://www.facebook.com/KasperskyLabRussia

О «Лаборатории Касперского»

«Лаборатория Касперского» – одна из наиболее динамично развивающихся компаний в сфере информационной безопасности. Она входит в четверку ведущих мировых производителей программных решений для защиты конечных устройств (Endpoint Protection) и является крупнейшей в мире частной компанией, специализирующейся в области разработки программных решений для обеспечения IT-безопасности.

На сегодняшний день в компании работают более 2800 высококвалифицированных специалистов. «Лаборатория Касперского» осуществляет свою деятельность более чем в 200 странах и территориях мира, имеет локальные представительства в 30 странах, а ее продукты и технологии используют более 300 млн конечных пользователей и более 250 тыс. корпоративных клиентов по всему миру. Компания предлагает широкий спектр продуктов и решений для разных сегментов рынка, уделяя особое внимание крупным корпорациям, а также малому и среднему бизнесу.