Оглавление

ВВЕДЕНИЕ.....2
1. КОМПЬЮТЕРНЫЕ ВИРУСЫ. ВРЕДОНОСНОЕ ПО.....4
1.1. Структура и классификация компьютерных вирусов.....4
1.1.1. Среда обитания.....5
1.1.2. Деструктивные возможности.....8
1.1.3. Классификация вирусов по мнению Лаборатории Касперского.....9
1.2. Типы вредоносных ПО.....18
1.2.1. Шпионские программы.....18
1.2.2. Компьютер-зомби.....20
1.2.3. «Бот».....20
1.2.4. Вымогатели.....22
1.2.5. Баннеры или программы-блокировщики.....22
1.2.6. Сниффинг.....23
1.2.7. Фарминг и фишинг.....23
1.2.8. Кардинг.....24
1.2.9. StalinLocker.....24
1.2.10. VegaStealer.....25
1.2.11. WannaCry.....26
1.2.12. Petya.....28
1.2.13. BadRabbit.....29
1.2.14. Slingshot.....30
2. АНТИВИРУСНАЯ ЗАЩИТА КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ.....31
2.1. Анализ вирусов. Методы защиты от вирусов.....31
2.2. Рейтинг антивирусных программ.....44
2.3. Стоимость услуг.....56
ЗАКЛЮЧЕНИЕ.....59
СПИСОК ИСТОЧНИКОВ.....60

ВВЕДЕНИЕ

В настоящее время общество тесно связано с персональными компьютерами и построением глобальной информационной Сети.

Применение персональных компьютеров оказалось связанным с появлением программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Проникнув в один компьютер, компьютерный вирус способен распространиться на другие компьютеры.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано много видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

В данной работе я расскажу о видах вирусов, об их классификации по среде обитания, по деструктивным возможностям, также расскажу о классификации вирусов по версии Лаборатории Касперского. И, конечно же, расскажу об антивирусной защите, о видах антивирусных программ, о достоинствах и недостатках бесплатных антивирусных программ, приведу собственные результаты тестирования антивирусов, сравню с результатами специалистов немецкой лаборатории “AV-Test” и компьютерного журнала“PCMag”.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяет избежать распространения вирусной эпидемии на другие компьютеры.

Актуальность этой работы обусловлена тем, что в настоящее время компьютерные вирусы совершенствуются и становятся опаснее с каждым днем.

Целью данной работы является ознакомление с разновидностями компьютерных вирусов, изучение механизмов их работы, а также борьба с ними с помощью антивирусного программного обеспечения.

Для достижения этой цели я поставила следующие задачи:

1. Определить понятие компьютерного вируса.
2. Рассмотреть структуру и классификацию компьютерных вирусов.
3. Рассмотреть типы вредоносных ПО.
4. Протестировать топ-3 антивирусов.
5. Организовать антивирусную защиту.

Объект исследования: коммерческая организация.

Предмет исследования: применение комплексной антивирусной защиты с целью обеспечения информационной безопасности.

Гипотеза исследования: существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере.

Методы исследования:

1. Обобщение различных источников по теме, взятых из Интернета и дополнительной литературы.
2. Анализ различных вирусов и антивирусных программ.

Теоретическая значимость заключается в

Практическая значимость: пользователь даже низкого уровня владения компьютером может использовать данную работу, чтобы ознакомиться с основными компьютерными вирусами и вредоносными ПО, а также бороться с ними.

1. КОМПЬЮТЕРНЫЕ ВИРУСЫ. ВРЕДОНОСНОЕ ПО

Компьютерным вирусом называется программа, которая без ведома пользователя внедряется в компьютеры и производит там различные несанкционированные действия. Также в его способности входит “размножение”, то есть создание своих дубликатов, после чего он их внедряет в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. Причем дубликаты вируса могут и не совпадать с оригиналом. "Размножение" вирусов ничем не отличается от, например, копирования программой файлов из одной директории в другую. Отличие лишь в том, что эти действия производятся без ведома пользователя, то есть на экране не появляется никаких сообщений. Во всем остальном вирус - самая обычная программа, использующая те или иные команды компьютера.

Компьютерные вирусы - один из подвидов большого класса программ, называемых вредоносными кодами. Сегодня эти понятия часто отождествляют, однако, с научной точки зрения это не верно. В группу вредоносных кодов входят также так называемые "черви" и "Троянские кони".

1.1. Структура и классификация компьютерных вирусов

Вирусы состоят, по крайней мере, из двух функционально разделенных компонентов. Один из них отвечает за размножение, а другой – за нанесение ущерба.

Компонент, ответственный за размножение, реализует все те функции, которые необходимы для распространения вируса, в частности поиск неинфицированных программ, внесение в них изменений, внедрение в оперативную память и, наконец, выполнение маскировочных мероприятий.

Компонент, реализующий нанесение ущерба, вступает в действие, как правило, после завершения работы той части вируса, которая отвечает за размножение. Почти всегда для этого компонента четко определяются условия начала его работы (пуска) и предусматривается их проверка при каждой

активизации вируса. В случае если эти условия не соблюдены, то работа данного компонента прекращается и не происходит ничего, что могло бы броситься в глаза. Это объясняет, почему вирусные инфекции очень часто могут оставаться незамеченными на протяжении длительного времени. Вирус “спит”, пока не наступит определенный момент.

1.1.1. Среда обитания

По среде обитания бывают файловые, системные, макро- и сетевые вирусы.

Файловые вирусы находятся в зараженном файле, активируются, когда пользователь включает эту программу. Эти вирусы составляют наиболее многочисленную группу и, в свою очередь, разделяются по способу воздействия на две подгруппы: вирусы необратимой модификации и вирусы гибкой модификации.

Вирусы необратимой модификации разрушают файлы благодаря своему механизму размножения. Измененные файлы становятся неработоспособными после воздействия на них, и в связи с этим данный тип вирусов быстро обнаруживается и его возможности по распространению и нанесению ущерба ограничены.

Вирусы гибкой модификации, называемые также прикрепляющимися вирусами, более опасны, поскольку их присутствие в системе обнаружить нелегко. Такие вирусы “повисают” на программах и, несмотря на произведенные изменения, способны восстановить прежний вид этих программ непосредственно перед их пуском. Обычно заражение вирусом можно обнаружить только путем сравнения размеров файла с оригиналом.

По способу использования оперативной памяти файловые вирусы подразделяются на резидентные (размещаемые в памяти резидентно) и нерезидентные (удаляются из памяти вместе с выгружаемой инфицированной программой). В специальной терминологии резидентные вирусы называются вирусами непрямого действия, а нерезидентные – вирусами прямого действия.

Системные вирусы работают на более глубоком уровне, внедряясь в дисковую структуру ОС, связанную с базовыми функциями ввода/вывода информации и запуска компьютера, затрагивающими пусковые (Boot)-секторы.

Активизация такого типа вируса, в отличие от других, происходит только при запуске (перезапуске) компьютера с зараженного диска, после чего вирус резидентно инсталлируется в оперативной памяти и начинает манипулировать пусковым сектором (загрузчиком) и другими элементами дисковой структуры. Распространение инфекции происходит при обращении ОС к другим дискам.

Обнаружить такой вирус и освободиться от него весьма трудно. Это объясняется, в первую очередь, тем, что он попадает в оперативную память в процессе запуска компьютера, т.е. еще до того, как сможет заработать какая-либо антивирусная программа. Единственная возможность обнаружить инфекцию состоит в проверке оперативной памяти сразу же после загрузки. При обнаружении вируса компьютер следует немедленно выключить и загрузить с неинфицированного диска.

Системные вирусы разделяются на два подтипа: вирусы пускового сектора и декомпозиционные вирусы. Разница между ними заключается в том, что вирус пускового сектора “оккупирует” пусковой сектор системного диска, в свою очередь декомпозиционный вирус проникает в пусковой сегмент логического несистемного диска.

Стоит отметить, что вирус пускового сектора может распространяться не только через системный диск. В случае, когда пользователь по ошибке попытается запустить компьютер с несистемного (не имеющего пусковой записи) диска, инфицированного вирусом пускового сектора, то компьютер выдаст на экран монитора сообщение об ошибке и попросит сменить диск. При этом считывание пускового сектора происходит в любом случае и, в случае если он содержит вирус, то последний немедленно попадает в оперативную память. После устранения ошибки и смены диска компьютер оказывается зараженным.

Воздействие системных вирусов чаще всего носит исключительно разрушительный характер.

Следует отметить, что в последнее время появились гибридные “диверсионные программы”, сочетающие в себе преимущества файлового и системного вирусов. Внешне этот вирус ведет себя как файловый вирус. При этом после его обнаружения и удаления зараженных файлов он снова распространяется по диску, инфицируя файлы из оперативной памяти, куда он попадает с пускового сектора.

Макровирусы - разновидность компьютерных вирусов, которые могут находиться на сайте, могут прислать по почте или в документах Wordи Excel. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MSWord. Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

1)привязки программы на макроязыке к конкретному файлу;

2)копирования макропрограмм из одного файла в другой;

3)возможность получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Стоит отметить, что среди ведущих антивирусных компаний существует мнение, что макровирусы больше не встречаются, однако для большинства пользователей вопрос борьбы с ними все еще актуален.

Сетевые вирусы–вирусы, которые используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Вирусы, проникая на компьютер через сеть, могут привести не только к повреждению важной информации, но и самой системы в целом. Самым главным принципом работы такого вируса является уникальная возможность передать свой код без сторонней помощи на рабочую станцию или удаленный сервер. Большинство сетевых вирусов, кроме возможности самостоятельно проникать через сеть на удаленные компьютеры, могут там же запустить на выполнение свой программный код, или, в некоторых случаях, немного «подтолкнуть» пользователя, что бы тот запустил инфицированный файл.

Также существуют сочетания вирусов – например, сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

1.1.2. Деструктивные возможности

По деструктивным возможностям вирусы можно разделить на:

1. Безвредные;
2. Неопасные;
3. Опасные;
4. Очень опасные.

Безвредные вирусы никак не влияют на работу компьютера, кроме уменьшения свободной памяти на диске в результате распространения.

Неопасные вирусы влияют на уменьшение свободной памяти на диске, а также на появление графических, звуковых и прочих эффектов.

Опасные вирусы приводят к серьезным сбоям в работе компьютера.

Очень опасные вирусы, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже способствовать быстрому износу движущихся частей механизмов – вводить в резонанс и разрушать головки некоторых типов винчестеров.

1.1.3. Классификация вирусов по мнению Лаборатории Касперского [1]

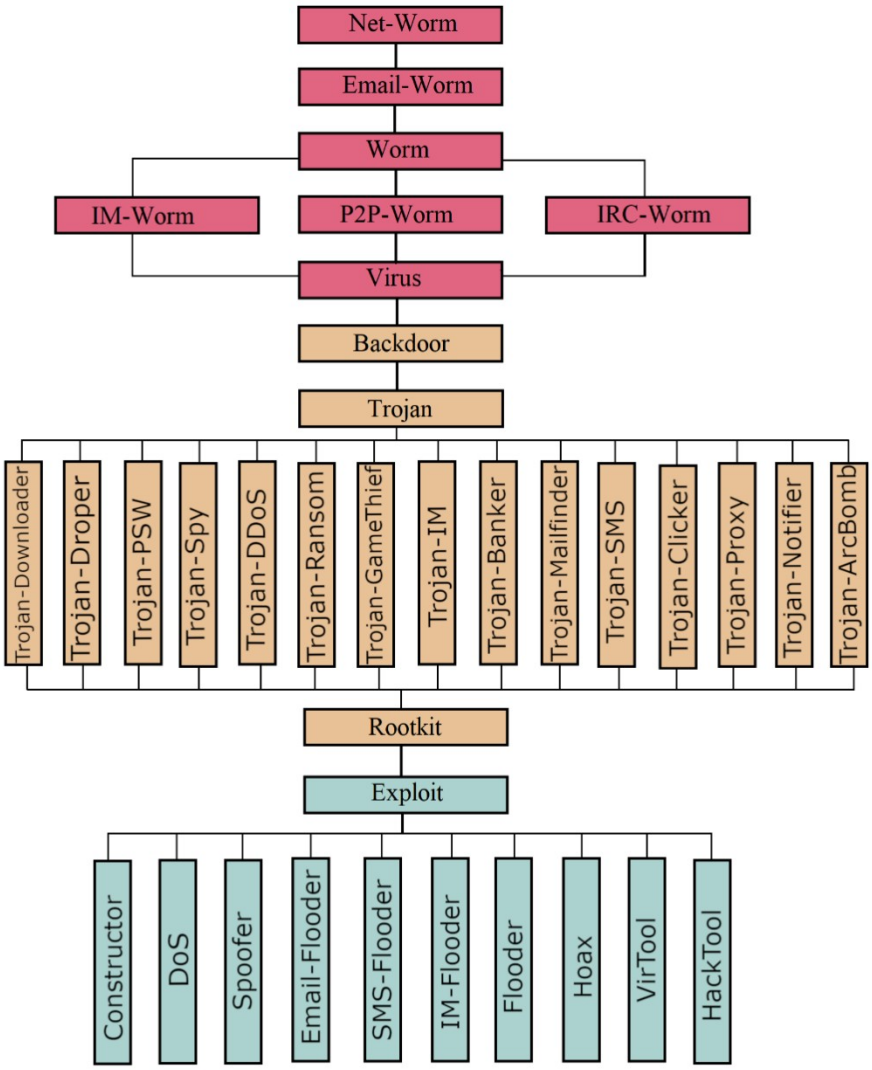


Рисунок 1 – Классификация вирусов

В самом низу схемы находятся наименее опасные угрозы. Такие как СМС-спам, спуффинг и так далее.

В середине, оранжевым цветом, показаны угрозы средней опасности:

Trojan, трояны или троянские программы - это вредоносные программы, разработанные для кражи информации с компьютера жертвы. Логины, пароли, банковская и личная информация, большинство троянских программ воруют все что можно и отправляют эту информацию своему разработчику. Под видом троянских программ можно считать кей-логеры. Данные программы записывают все нажатия клавиш и действия пользователя за компьютером. После этого все

собранная информация отправляется разработчику вируса. Таким образом, могут быть украдены пароли и другие важные данные, которые пользователь не сохранял на компьютере.

Задачи, которые могут выполнять троянские программы, бесчисленны, но в основном они идут по следующим направлениям:

- Нарушение работы других программ (вплоть до зависания компьютера, решаемого лишь перезагрузкой, и невозможности их запуска);
- Настойчивое, независимое от владельца предложения в качестве стартовой страницы спам-ссылок, рекламы и т.д.;
- Распространение по компьютеру пользователя нежелательных материалов непристойного характера;
- Превращение языка текстовых документов в бинарный код;
- Мошенничество (например, при открывании определённого сайта пользователь может увидеть окно, в котором ему предлагают сделать определённое действие, иначе произойдёт что-то трудно поправимое — бессрочная блокировка пользователя со стороны сайта, потеря банковского счета и т. п., иногда за деньги, получение доступа к управлению компьютером и установки вредоносного ПО);
- Простое списывание.

Trojan-Downloader – предназначена для несанкционированной пользователем загрузки и установки на компьютер новых версий вредоносных программ, установки троянских программ или рекламных систем. Загруженные из Интернета программы затем либо запускаются на выполнение, либо регистрируются троянцем на автозагрузку. Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с “управляющего” Интернет-ресурса.

Данный тип вредоносных программ в последнее время стал часто использоваться для первоначального заражения посетителей заражённых веб-страниц, содержащих эксплойты.

Trojan-Droper – предназначен для скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в их теле.

Эти вредоносные программы обычно без каких-либо сообщений (или с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.) сохраняют на диск жертвы другие файлы и запускают их на выполнение.

Данные программы хакеры используют:

- для скрытой инсталляции троянских программ и/или вирусов;
- для защиты от детектирования известных вредоносных программ антивирусами, поскольку не все они в состоянии проверить все компоненты внутри подобных «троянцев».

Trojan-PSW- предназначены для кражи пользовательских аккаунтов с пораженных компьютеров. PSW – аббревиатура от PasswordStealingWare.

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

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

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

Trojan-DDoS - предназначены для проведения с пораженного компьютера DoS-атаки по заранее определенному адресу.

Суть атаки сводится к отправке на компьютер-жертву многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого

удаленного компьютера недостаточны для обработки всех поступающих запросов.

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

Trojan-Ransom - модифицирует данные на компьютере, с тем чтобы пользователь не мог ими воспользоваться, или блокирует работу компьютера. После того, как данные блокированы (или зашифрованы), у пользователя требуют выкуп за их расшифровку.

Деньги жертва должна передать злоумышленнику, после чего тот обещает выслать программу для восстановления данных или нормальной работы компьютера

Trojan-GameThief - предназначены для кражи конфиденциальной информации, относящейся к компьютерным играм. Найденная информация передается злоумышленнику.

Trojan-IM - предназначены для кражи учетных записей пользователей интернет-пейджеров (например, MSN Messenger, YahooPager, Skype и др.). Найденная информация передается злоумышленнику.

Trojan-Banker - предназначены для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт. Найденная информация передается злоумышленнику.

Трояны применяют следующие приемы:

- Сканирование файлов на компьютере для поиска номеров карточек (некоторые пользователи хранят все данные о карточках в обычных текстовых файлах).
- Кража данных с заполненных форм. В данном случае, троян не изменяет web-страницу, но крадет финансовую информацию при заполнении формы оплаты.

- Подмена официальных страниц банков и магазинов на фальшивые. В этом случае, в памяти компьютера присутствует троянская программа, которая на ходу изменяет web-страницу в браузере и перенаправляет пользователя на поддельную страницу, или же добавляет на web-страницу поддельные поля для ввода данных кредитной карточки.

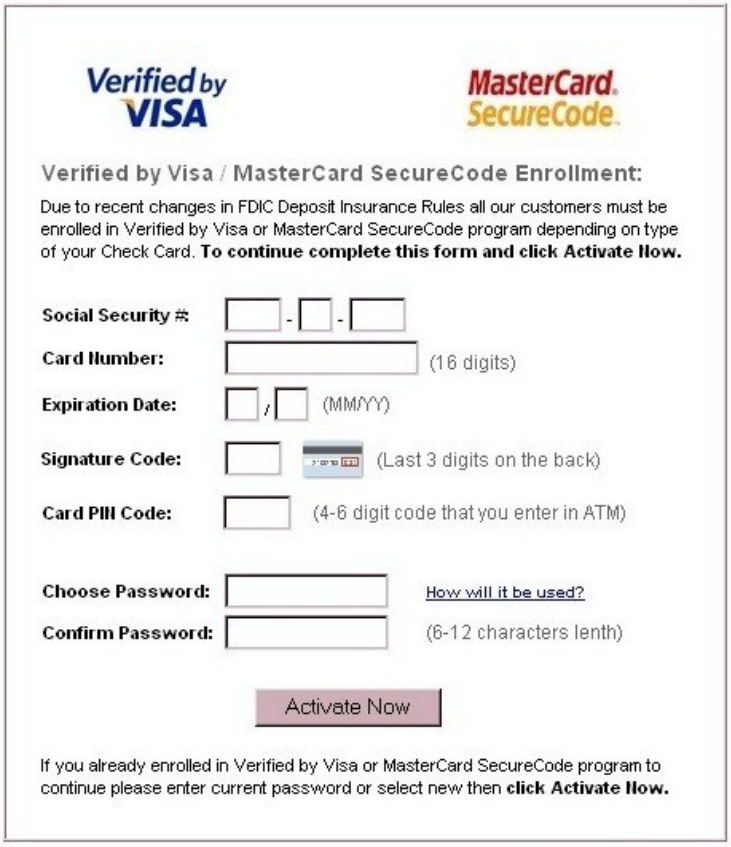


Рисунок 2 – Пример поддельной формы для "проверки кредитной карточки"

- Фальшивые антивирусы и программы оптимизаторы, которые находят на компьютере не существующие угрозы и предлагают их исправить, но конечно не бесплатно, а после оплаты их «полной версии».

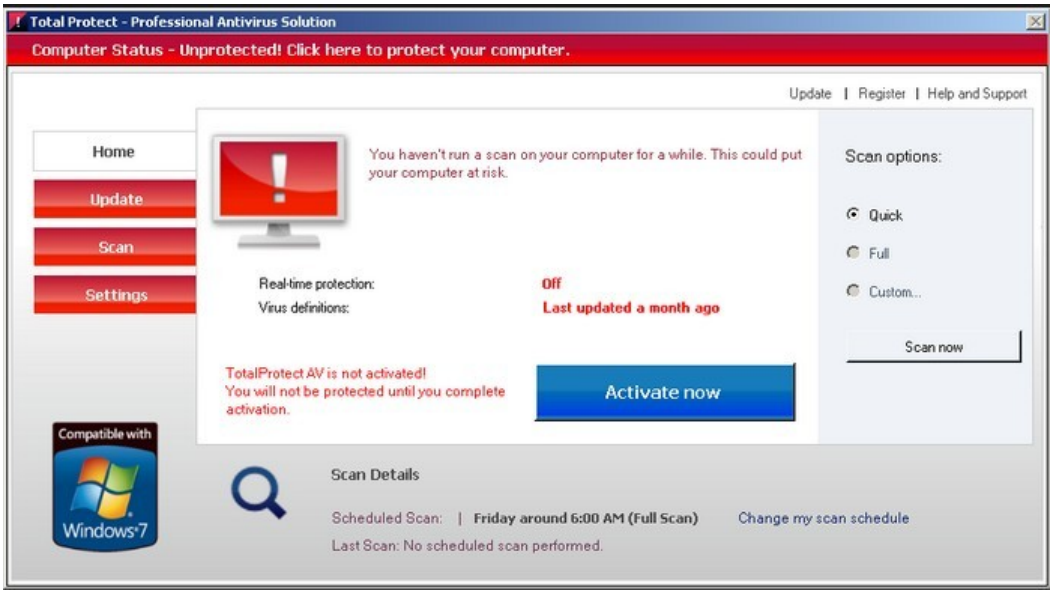


Рисунок 3 – Пример фальшивого антивируса, предлагающего приобрести "полную версию"

- Рекламные программы, которые терроризируют пользователя навязчивой рекламой, а потом перенаправляют его на сайт злоумышленников, где ему предлагается ввести данные кредитной карты для оплаты.
- Программы вымогатели, которые блокируют компьютер или же закриптовывают файлы на компьютере, а потом требуют оплату за восстановление работоспособности.

Trojan-Mailfinder - предназначены для сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику по электронной почте, через web, ftp или другими способами.

Украденные адреса используются злоумышленниками при проведении последующих рассылок вредоносных программ и спама.

Trojan-SMS - предназначены для кражи денежных средств с пораженных мобильных устройств, например, путем отсылки SMS сообщений на дорогостоящие платные номера, записанные в теле вредоносной программы.

Trojan-Clicker - предназначены для обращения к интернет-ресурсам. Достигается это либо передачей соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов.

У злоумышленника могут быть следующие цели для таких действий:

- увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;
- привлечение потенциальных жертв для заражения вирусами или троянскими программами.
- искусственная накрутка кликов в рекламных сетях с целью обогащения злоумышленников.

Trojan-Proxy - предназначены для осуществления злоумышленником доступа к различным интернет-ресурсам через компьютер. Такие вредоносные программы обычно используется для рассылки спама.

Trojan-Notifier - предназначены для передачи своему «хозяину» сообщения о том, что зараженный компьютер сейчас находится «на связи». При этом на адрес злоумышленника отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к web-странице злоумышленника.

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

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

Встречаются три типа подобных «бомб»:

- некорректный заголовок архива;
- повторяющиеся данные;
- одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива.

Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера.

Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов.

Backdoor – программа позволяет делать с компьютером все, что в них заложит автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. Представители этого типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые бот-сети/зомби-сети, что позволяет злоумышленникам централизованно управлять всей армией пораженных компьютеров для совершения злонамеренных действий. Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Рассмотрим наиболее опасные вирусы, находящиеся на самой вершине схемы:

Вирус - самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя. Вирусы можно подцепить разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте. При этом вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда

операционной системе. В настоящее время вирусы довольно редки, так как создатели вредоносных программ стараются держать свои программы и их распространение под контролем. В противном случае вирус довольно быстро попадает в руки антивирусных компаний.

Компьютерный червь— это разновидность вредительского ПО, которая самостоятельно распространяется по интернет просторам, с компьютера на компьютер. Также распространение идет внутри компьютера, от одной его части, к другой. Основная цель компьютерного червя - подобное дублирование себя на различных ЭВМ. Кроме прочего, черви запускаются и как вирусы, т.е. во время установки какого-либо софта. Также компьютерные черви могут появляться на ПК, когда ОС имеет большое количество ошибок. Компьютерные черви довольно часто попадают на компьютер из электронной почты. Это так называемые черви почтовики. Также такие черви могут перейти из чатов, социальных сетей и т.д.

Компьютерные черви делятся на два принципа функционирования: обычный и пакетный.

Обычный попадает на компьютер обычным путем. Затем, создаёт свои многочисленные дубли. Далее, проводит поиск на компьютере списков различных электронных адресов. Потом, по данным адресам рассылает свои многочисленные дубли.

Пакетный – ведет себя на ПК иначе. Попав на компьютер в виде специальных пакетов, пытается внедриться в оперативную память ПК. Делает он это в основном, для сбора информации, ваших личных данных. Уникален тем, что после выключения ПК не оставляет своих следов присутствия.

Классификация червей по методу распространения:

- *IM-Worm*– компьютерный червь. В основном работает через программы и сервисы быстрых сообщений. Человеку в подобном сервисе приходит сообщение с ссылкой, человек проходит по данной ссылочке и подхватывает червячка.

- *P2P-Worm* – компьютерный червь – в основном проникает на компьютер через файлообменник. Человек скачивает с файлообменника необходимую ему программу, распаковывает её, и при этом происходит заражение. Например, файлы с данным червем часто называются вроде: — «Как проникнуть в чужую электронную почту?» Или «Как проникнуть в чужой электронный кошелёк».
- *IRC-Worm*– предпочитает систему InternetRelayChat. Напоминает прошлого вредителя, но с большими возможностями. Он в своих сообщениях посылает не только ссылки, но и вложенные файлы. Когда человек открывает подобный файл, происходит заражение ПК.
- *Email-Worm* -попадает на компьютер в основном через электронную почту. Если после открытия письма, Вы переходите по ссылке на определённый сайт или открываете вложенный файл, то произойдет заражение компьютера. В дальнейшем, червь ищет на компьютере различные электронные адреса, по которым передает свои дубли.
- *Net-Worm* – инфицирование происходит через интернет, как через обычные софты. Так и на многих популярных сайтах. Подобный червь ищет уязвимость в операционной системе, инфицирует её приложения и заражает саму систему.

1.2. Типы вредоносных ПО

1.2.1. Шпионские программы для компьютера не наносят вреда – ни системе, ни программам, ни файлам. Однако такая программа задействует какое-то количество оперативной памяти, из-за чего компьютер может зависать и подтормаживать. Задачей шпионских программ является периодический сбор информации о пользователях:

- Содержание жесткого диска;
- Список посещаемых интернет-сайтов;
- Контакты электронной почты;
- Другая информация личного характера.

Вся собранная информация отправляется разработчикам шпионской программы. В большинстве случаев пользователь не подозревает, что находятся под наблюдением – шпионские программы работают незаметно, поскольку их разработчики заинтересованы в продолжительном получении нужной им информации.

Виды шпионских программ:

- Кей-логгеры- клавиатурные шпионы, они собирают и отправляют своему разработчику информацию обо всех нажатиях на клавиши клавиатуры на конкретном компьютере. Кей-логгеры или прописываются программой, или подсоединяются к компьютеру в качестве дополнительного аппаратного устройства.
- Сканеры жесткого диска - это шпионские программы, которые разрабатываются для изучения содержимого жестких дисков на компьютере пользователя. Сканеров интересует любая пользовательская информация, которая может пригодиться разработчику шпионской программы. Полученную информацию сканеры жесткого диска отправляют своему разработчику.
- Экранные шпионы – это программы, которые собирают информацию о том, чем именно пользователь занимается на компьютере. Через заданные промежутки времени такие экранные шпионы делают скриншоты, затем отсылают их по назначению – либо разработчику, либо напрямую заказчику. Разработку и внедрение экранных шпионов, в большинстве случаев, заказывают корпорации – например, руководство таким образом может осуществлять контроль офисных сотрудников, периодически просматривая, чем персонал занимается в рабочее время.
- «Прокси-шпионы» - шпионские программы, проникая в пользовательские компьютеры, превращают их в прокси-серверы. Злоумышленники могут прикрыться компьютером пользователя-жертвы для противозаконных действий. Типичным примером работы таких «прокси-шпионов» является рассылка спама с компьютера пользователя-жертвы.

- Почтовые шпионы – шпионские программы собирают информацию о контактах пользователя в электронной почте. Информация собирается в адресных книгах, почтовых клиентах, органайзерах и подобной программной среде. Затем все эти данные отправляются разработчику шпионской программы, а использует он все это для рассылки спама.

1.2.2. Компьютер-зомби - компьютер в сети, который был заражен специализированной вредоносной программой, предоставляющей злоумышленнику удаленный доступ и ресурсы машины. Программа, как правило, активно маскируется и без оффлайн-проверки файлов, контроля трафика или использования специального ПО вычислить такой компьютер достаточно сложно. Такой компьютер может быть использован третьими лицами без ведома владельца: для доступа в закрытую или коммерческую сеть, использования вычислительных ресурсов, рассылки спама и перенаправления трафика в момент совершения противоправных действий.

1.2.3. «Бот» - автоматизированный процесс, который взаимодействует с другими сетевыми службами. Боты часто автоматизируют задачи и предоставления информации и услуг, которые могли бы производиться человеком. Типичным использованием ботов является сбор информации, а также автоматизированное взаимодействие с человеком.

Вредоносный бот распространяет вредоносное ПО, которое заражает компьютеры и подключает их через бэкдоры (задача бэкдора поставить компьютер жертвы под контроль разработчика вируса. В случае заражения бэкдором вирусописатель может не только воровать данные, но и управлять компьютером) к центральному серверу управления, который может управлять всей сетью взломанных устройств. Используя бот-нет, злоумышленник может совершать DDOS-атаки на сайты или сервера конкурентов. DDOS-атаки представляют собой одновременное огромное количеству бессмысленных запросов на сервер, исходящих от множества устройств (зараженных компьютеров), что приводит к перегрузке и зависанию сервера и невозможности нормальной работы и передачи информации.

В дополнение к червеобразной способности самораспространяться, боты могут записывать нажатия клавиш, красть пароли, собирать финансовую информацию, совершать DDOS-атаки, рассылать спам. Боты имеют все преимущества червей, однако более универсальны и кроме того, объединены в сеть, которая позволяет контролировать зараженные компьютеры и совершать определенные действия по команде с контрольного центра. Создавая бэкдоры боты могут загружать на компьютер другие вредоносные программы, как вирусы или черви.

Боты в большинстве случаев стараются никак не проявлять себя для пользователя, поэтому опознать, что компьютер заражен бывает непросто.

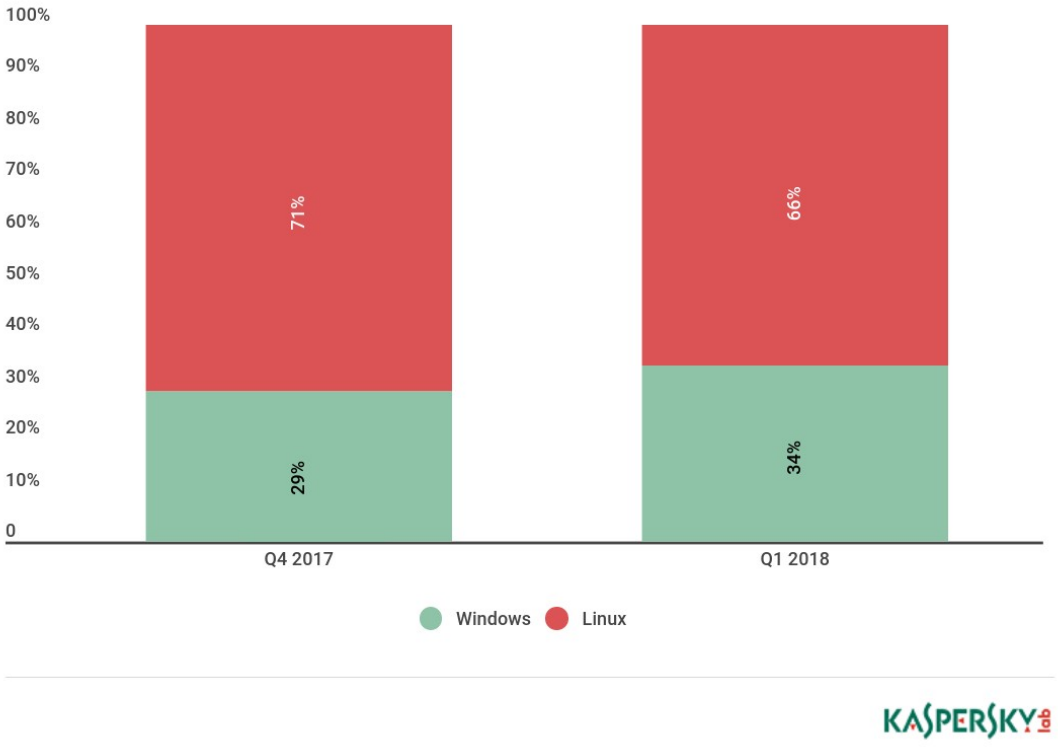


Рисунок 4 – Статистика соотношения атак с Windows–и Linux-ботнетов за первый квартал 2018 года

На рисунке №4 видно, что доля Linux-ботнетов уменьшилась по сравнению с четвертым кварталом 2017 года – 66% вместо 71%. Соответственно, количество Windows-ботнетов выросло с 29% до 34%.

1.2.4. Вымогатели блокируют доступ к компьютерной системе или предотвращает считывание записанных в нем данных, а затем требует выкуп для восстановления исходного состояния.

В настоящий момент существует несколько кардинально отличающихся подходов в работе программ-вымогателей:

- Шифрование файлов в системе;
- Блокировка или помеха работе в системе;

Шифрование файлов в системе – программа зашифровывает большую часть рабочих файлов. При этом компьютер остается работоспособным, но все файлы пользователя оказываются недоступными.

Блокировка или помеха работе в системе – программа блокирует компьютер с помощью системных функций и прописывается в автозагрузке. При этом на экране пользователь видит какое-либо сообщение с требованием заплатить выкуп. При этом компьютер остаётся в рабочем состоянии. Часто присутствует угроза уничтожения всех данных, но это всего лишь попытка запугать пользователя. Иногда в вирус все же включают инструменты уничтожения данных, таких как шифрование по ассиметричному ключу, но они либо не срабатывают должным образом, либо имеет место низкоквалифицированная реализация.

1.2.5. Баннеры или программы-блокировщики сразу же блокируют диспетчер задач, чтобы пользователь не смог выгрузить их из оперативной памяти. Баннеры могут закрывать собой весь рабочий стол, в результате чего невозможно войти в меню операционной системы или открыть какую-либо программу. Некоторые баннеры могут работать даже в безопасном режиме. Программа-блокировщик представляет собой окно, в котором обычно просят отправить СМС-сообщение с выкупом. Некоторые баннеры обнаружить очень сложно, потому что иногда они маскируются под конкретную программу, точнее под компонент программы, который имеет такой же «вес», такое же название и такой же формат.

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

Самая большая угроза сниффинга состоит в перехвате паролей часто используемых протоколов, которые передают информацию о пароле в сети в открытом виде. С помощью сниффинга можно перехватывать даже передаваемые по сети файлы, прикрепленные к какому-нибудь письму.

1.2.7. Фарминг и фишинг. Фарминг– процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура.

В классическом фишинге злоумышленник распространяет письма электронной почты среди пользователей социальных сетей, онлайн-банкинга, почтовых веб-сервисов, заманивая на поддельные сайты пользователей, ставших жертвой обмана, с целью получения их логинов и паролей. Банки, социальные сети, прочие веб-службы предупреждают о разнообразных мошеннических приемах с использованием методов социальной инженерии. Все это снижает количество откликов в фишинговой схеме – все меньше пользователей удается завлечь обманным путём на поддельный сайт. Поэтому злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название фарминга. Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит

посетить интересующие злоумышленника сайты. Вредоносные программы, реализующие фарминг-атаку, используют два основных приема для скрытного перенаправления на поддельные сайты – манипулирование файлом HOSTS или изменением информации DNS.

Популярные методы реализации Фарминг-атак:

- Изменение файла HOSTS;
- Изменение файла HOSTS вместе с изменением его местоположения;
- Модификация настроек DNS-серверов;
- Регистрация ложного DHCP-сервера.

1.2.8. Кардинг - целью являются средства клиентов банка. Атака связана с доступом к счетам через поддельные банковские карты. При этом данные об использованных в банкомате картах могут выгружаться непосредственно из компьютера банкомата. Другими словами, преступники, получая физический доступ к банкомату, подключают к нему портативное устройство с вредоносным ПО, которое позволяет обойти антивирус и скачать данные.

1.2.9. StalinLocker – одно из новых вредоносных ПО, которое уничтожает содержимое дисков на компьютере, если вводится неправильный код.



Уникальность вредоносной программы в том, что вирус после заражения копирует себя в %UserProfile%\AppData\Local\stalin.exe и создаёт механизм своего автозапуска, пытается прекратить остальные процессы компьютера, в частности завершая работу проводника. StalinLocker пытается ликвидировать все процессы, кроме Skype и Discord, завершает работу Explorer.exe и taskmgr.exe, а также пытается создать запланированную задачу DriverUpdate для запуска Stalin.exe. Пользователю отводится десять минут на то, чтобы ввести правильный код. При этом на экране появляется изображение Иосифа Сталина, а также исполняется гимн СССР. Эксперты по кибербезопасности установили, что код разблокировки можно определить путём вычисления разности между текущей датой и датой образования СССР — 30 декабря 1922 года.

Рисунок 5 – Экран зараженного компьютера

Если же не ввести код, отсчет дойдет до нуля, а после этого StalinLocker предпримет попытку удаления все файлов из системы жертвы, последовательно перебирая буквы томов от A до Z.

1.2.10. VegaStealer - вредоносное ПО, ворующий сохраненные учетные данные и сведения о банковских картах из браузеров Chrome и Firefox. Является

разновидностью AugustStealer. Наряду с уникальными функциями, Vega обладает набором позаимствованных у своего предка возможностей. Помимо кражи данных, как и его предшественник, умеет копировать с зараженного компьютера документы Word и Excel, а также файлы PDF и TXT. При этом программе August эти возможности не прописаны жестко, а конфигурируются через панель командного сервера. Код для кражи данных из Chrome в Vega частично повторяет код August, который умел извлекать информацию и из других приложений, таких как Opera или Skype. Помимо более узкой специализации, Vega отличается от предшественника новым протоколом сетевой связи и расширенными возможностями по краже данных из Firefox. Макрос скачивает полезную нагрузку в два этапа: сначала документ исполняет запрос, извлекающий обфусцированный скрипт JScript/PowerShell. Затем этот скрипт создает второй запрос, который загружает VegaStealer в пользовательскую папку с музыкой. После этого автоматически запускается из командной строки. Vega написан на языке .NET, и образец не был ни упакован, ни обфусцирован — код представлен в относительно голом виде. Vega может быть специализированной версией August, заточенной только под эту кампанию, но есть и доводы в пользу того, что в будущем программу ждет более широкое распространение.

1.2.11. WannaCry- вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая только компьютеры под управлением операционной системы MicrosoftWindows. Программа шифрует почти все хранящиеся на компьютере файлы и требует выкуп за их расшифровку. Ее массовое распространение началось в 2017 году. По количеству заражений лидирует Россия, Украина и Индия. В общей сложности пострадало более 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим организациям и правительственным учреждениям. По состоянию на 26 мая 2017 г., по данным сайта MalwareTechBotnetTracker, инфицированы более 410 000 компьютеров во всем мире, из них онлайн — 170 000. По состоянию на 6 июня 2017 г. заражены более 520 000 компьютеров и 200 000 IP-

адресов. 28 марта 2018 г. операционные системы авиастроительной корпорации Boeing подверглись кибератакам с применением WannaCry. Компанией были оперативно проведены восстановительные мероприятия программного обеспечения, и вирус не повлиял на производственную деятельность Boeing.

Вредоносная программа сканирует в Интернете узлы в поисках компьютеров с открытым TCP-портом. Обнаружив такой компьютер, программа предпринимает несколько попыток проэксплуатировать на нем уязвимость EternalBlue и, в случае успеха, устанавливает бэкдор, через который загружается и запускается код WannaCry.

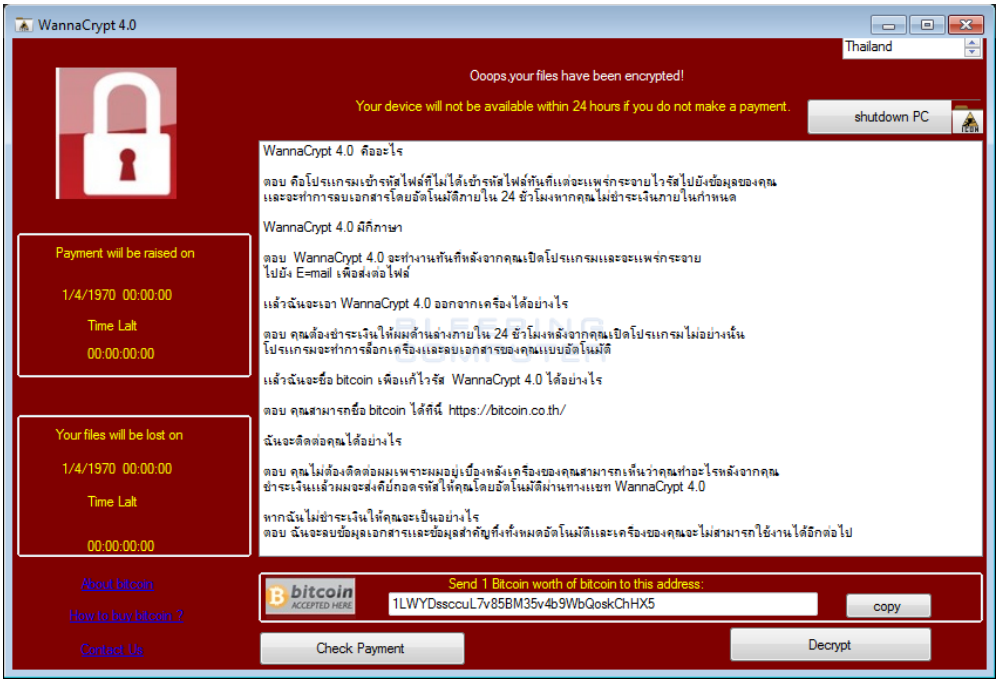


Рисунок 6 – Экран зараженного компьютера

При каждой попытке эксплуатации вредоносная программа проверяет наличие бэкдора, и в случае обнаружения загружается через этот бэкдор. После запуска программа действует как классическая программа-вымогатель. Затем WannaCry начинает сканировать систему в поисках пользовательских файлов,

оставляя критические нетронутыми. Каждый отобранный файл шифруется уникальным для каждого из них ключом, который в свою очередь шифруется открытым RSA-ключом инфицированной системы и сохраняется в заголовке зашифрованного файла. Пара RSA-ключей инфицированной системы шифруется открытым ключом злоумышленников и отправляется к ним на серверы управления, после чего все ключи из памяти инфицированной машины удаляются. Завершив процесс шифрования, программа выводит на экран окно с требованием перевести определённую сумму на указанный кошелёк в течение трёх дней. Если выкуп не поступит своевременно, то его сумма будет автоматически удвоена. На седьмой день, если WannaCry не будет удалён с инфицированной системы, зашифрованные файлы уничтожаются. Параллельно с шифрованием программа проводит сканирование произвольных адресов Интернета и локальной сети для последующего заражения новых компьютеров.

1.2.12. Petya- вредоносная программа, сетевой червь и программа-вымогатель, поражающая компьютеры под управлением MicrosoftWindows. 27 июня 2017 года началось массовое распространение новой модификации программы. На этот раз вирус использует те же уязвимости системы, что и WannaCry, а за восстановление доступа к данным требует отправить 300 долларов в биткойнах.

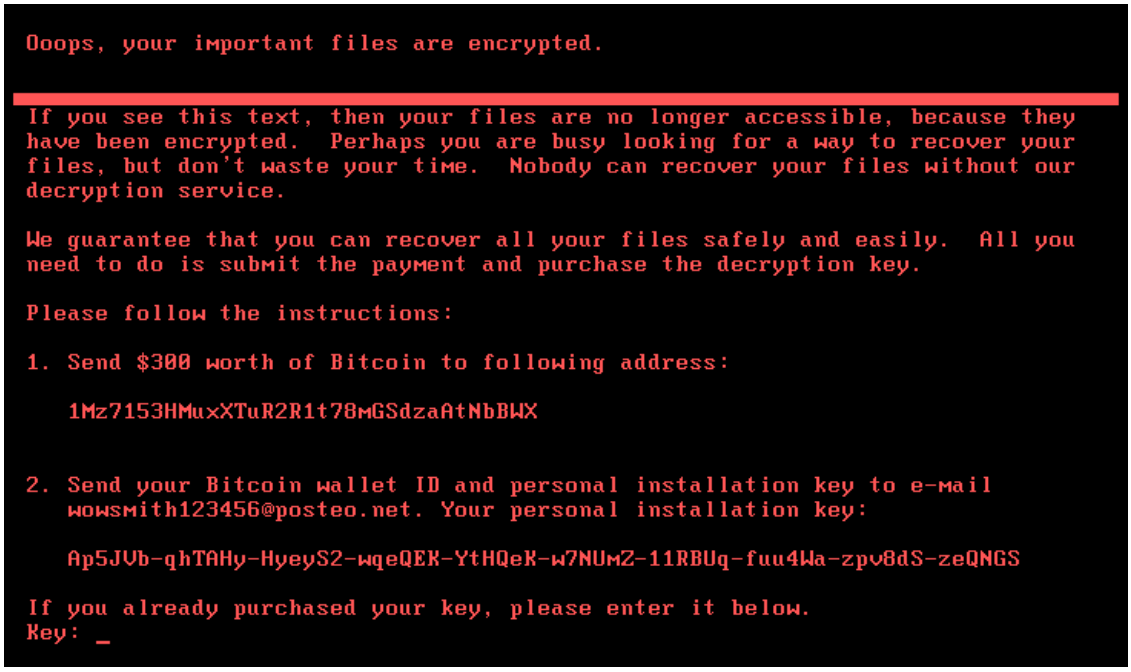


Рисунок 7 – Экран зараженного компьютера

Однако версия вируса 2017 года не предполагает возможности расшифровки информации на жёстком диске, а уничтожает её безвозвратно. Механизм вымогательства вредоносного ПО сконструирован неумело и являлся вовсе бесполезным: единственный адрес плохо зашифрован, то есть движение денег можно отследить. Ещё одной недоработкой можно отметить требование отправить 60-значный персональный идентификационный ключ заражённой машины с компьютера, который невозможно копировать и вставлять. Более того, специалисты Лаборатории Касперского выяснили, что в новой версии вируса этот ключ — ничего не значащий набор случайных символов. Это может говорить о том, что создатели вируса, скорее всего, и не собирались расшифровывать данные.

1.2.13. BadRabbit- вирус-шифровальщик, разработанный для ОС семейства Windows и обнаруженный 24 октября 2017 года.

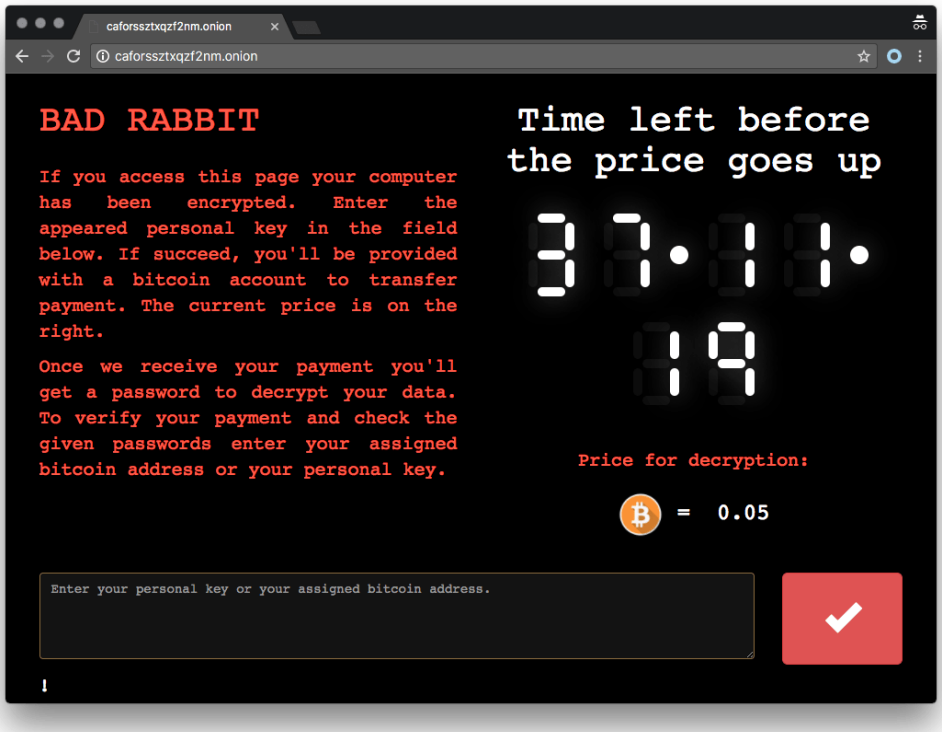


Рисунок 8 - Экран зараженного компьютера

По предположениям аналитиков, программа имеет сходство отдельных фрагментов с вирусом Petya. Для первоначальной установки Вирус не

использует каких-либо эксплойтов или уязвимостей: инсталлятор вируса, маскирующийся под установку обновления для AdobeFlashPlayer, должен быть скачан и запущен вручную пользователем, он запрашивает подтверждение повышения полномочий. После установки приложение регистрируется в штатном механизме планирования заданий и начинает самостоятельное распространение по локальной сети при помощи перехвата токенов и паролей и перебора паролей на удаленных узлах Windows для ряда распространенных имен пользователей.

1.2.14. Slingshot- опасный вирус, атакующий персональные компьютеры через подсоединенные к ним роутеры, обнаружили специалисты «Лаборатории Касперского». Основную опасность Slingshot представляет из-за его многоуровневой системы, что позволяет ему проводить сразу несколько атак используя маршрутизаторы. Через роутеры зараженные файлы распространяются гораздо быстрее, а если к устройству подключены несколько ПК или других гаджетов, то атака будет производиться сразу и на них. Этот вирус имеет улучшенную систему защиты, позволяет вирусу маскироваться под систему защиты. Например, Slingshot сам запускает протоколы проверки безопасности. Если роутеру сделать полную перезагрузку и даже переустановить программное обеспечение, вирус все равно «выживет», благодаря многократному самокопированию вредоносного ПО. Более того в «Лаборатории Касперского» говорят о том, что скорее всего у вируса есть и другие системы самозащиты [2]. В первую очередь, вирус, получив доступ, похищает все сохраненные пароли, личную информацию, изображения. Slingshot может использовать сетевой трафик.

2. АНТИВИРУСНАЯ ЗАЩИТА КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Использование современных технологий позволяет компаниям добиться значительных результатов своей деятельности в кратчайшие сроки. Но и развитие вирусных угроз, которым подвергается современный бизнес, совершенствуется с каждым днем. Злоумышленники придумывают все новые методы для обхода защиты информации, создавая все новые, более сложные угрозы.

2.1. Анализ вирусов. Методы защиты от вирусов

Стать жертвой вирусов может компьютер любого пользователя. Нанесенный вред может заключаться от простого торможения системы до полного выхода машины из строя и порчи файлов.

Для начала рассмотрим рисунок №9. На нем показаны исследования компании Balabit в области информационных угроз в компаниях за 2018 год.

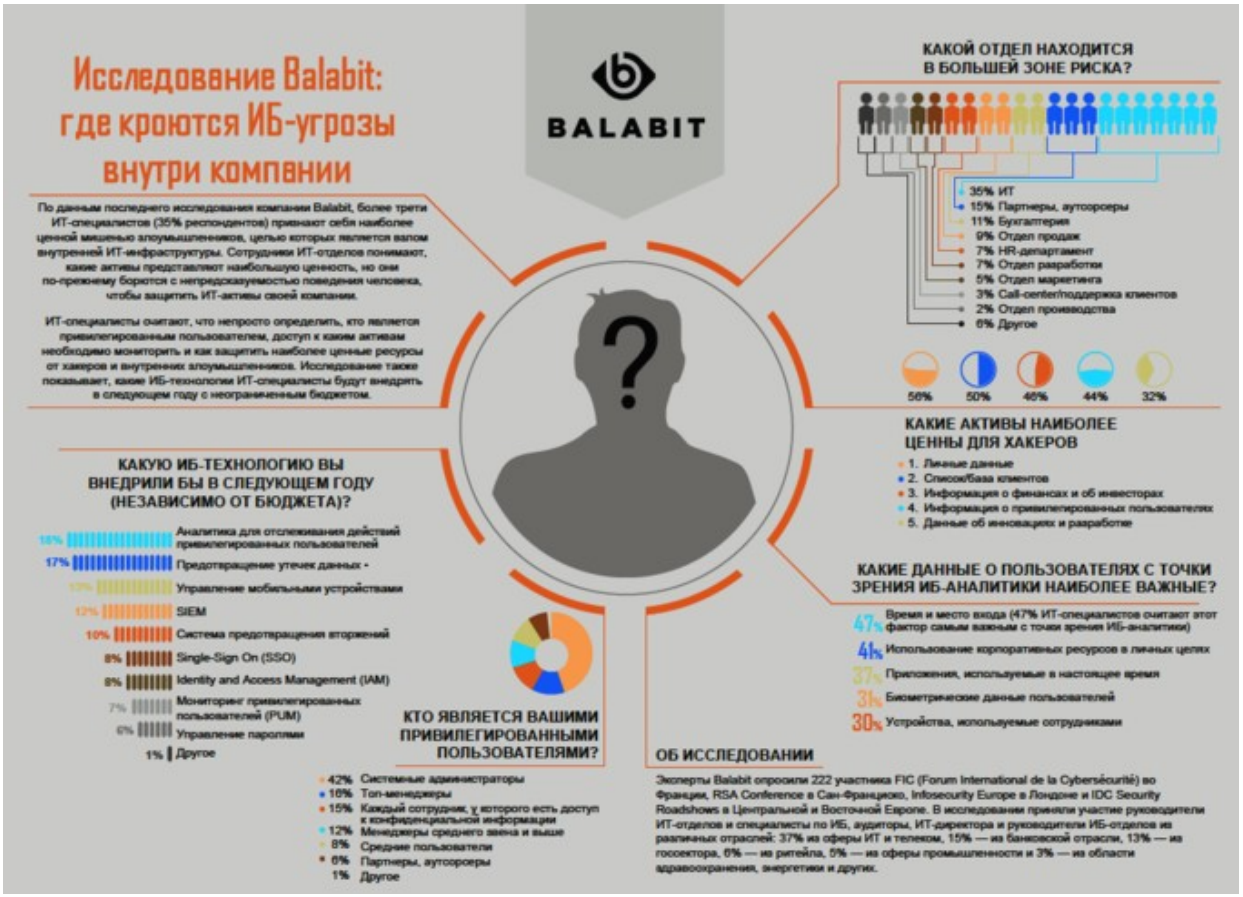


Рисунок 9 – Статистика за 2018 год в области информационных угроз в компаниях

По статистике видно, что наиболее привилегированными пользователями компаний являются системные администраторы (42%). Наиболее ценными активами для хакеров являются личные данные, база клиентов, информация о финансах и об инвесторах, информация о привилегированных пользователях, данные об инвесторах и разработке. Также по статистике IT-отдел находится в наибольшей зоне риска (35%), далее следуют партнеры и аутсорсеры (15%) и бухгалтерия (11%).

В связи с этим мы рассмотрим наиболее актуальные угрозы для коммерческой организации.

Троян

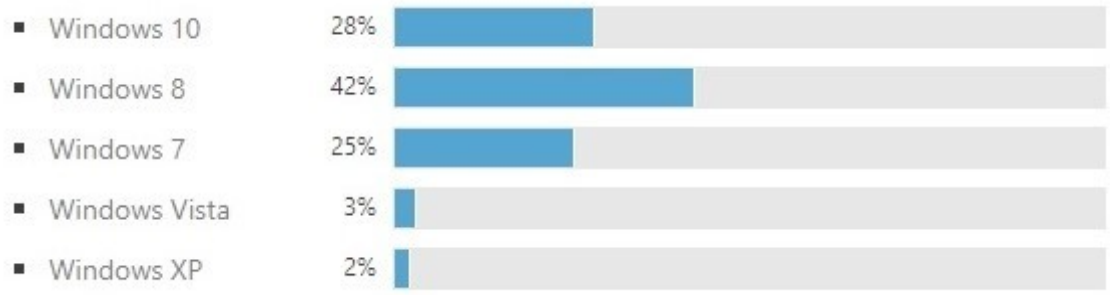
На рисунке №10 приведена статистика заражения трояном за май 2018 года по версии Лаборатории Касперского [3].



Рисунок 10 – Статистика заражения трояном за май 2018 года

Рассмотрим некоторые из них:

Trojan.js.miner.m – проникает в компьютер и портит операционную систему. Вирус использует процессор, из-за чего тот нагревается - это приводит



к непродолжительной жизни процессора. Также троян изменяет системный реестр и необходимые для операционной системы файлы и папки. Вирус может вызвать некоторые программы для замораживания, чтобы появились сбои в антивирусных программах. Троян запрограммирован для выполнения различных вредоносных операций. Такие как шпионаж (при помощи отслеживания нажатий клавиш), кража компьютерных ресурсов и важных файлов. Трояном можно заразиться через Torrent, спам, поддельные обновления, зараженные веб-сайты и т.д. [4].

Рисунок 11 – Статистика ОС Windows по количеству заражения вирусом

Метод защиты:

Для начала перезагрузите компьютер в безопасном режиме, держа кнопку F8 при загрузке системы, выберите пункт “Безопасный режим”. Далее следует открыть командную строку, вписать команду regedit для открытия редактора реестра и там удалить поврежденные и вредоносные записи. Также следует просканировать все файлы и папки, связанные с трояном и сразу же их удалить.

Trojan.Script.Generic–компьютер подключается к неизвестному удаленному серверу. Хакеры используют угрозу, чтобы украсть личную информацию, такую как номер счета, пароль и другие банковские реквизиты. Открывает в системе черных ход, который позволяет другой угрозе войти в систему. К данному семейству относят программы, обладающие типовыми характеристиками вредоносных скриптов-троянцев [5].

	Страна	% атакованных пользователей*
1	Российская Федерация	36,52
2	Германия	5,33
3	Бразилия	4,32
4	Испания	3,68
5	Франция	3,45
6	Украина	2,99
7	Индия	2,95
8	США	2,14
9	Казахстан	1,96
10	Саудовская Аравия	1,82

**Процент от всех уникальных пользователей продуктов «Лаборатории Касперского», атакованных зловредом*

Рисунок 12 – Статистика стран по количеству атакованных пользователей (%)

Метод защиты:

Для начала нужно завершить процесс в диспетчере задач. Если вирус все еще активен, нужно удалить процесс в панели управления. Также можно удалить запись в реестре с помощью командной строки и команды regedit.

Для автоматического удаления вируса можно использоватьSpyHunter. После сканирования компьютера, программа выдаст окно, в котором выводится список найденных угроз. Также можно просмотреть информацию об определенном вирусе. Программное обеспечение предоставляет защиту системы, которая препятствует входу угроз в систему.

Trojan.Script.Miner.gen – чрезвычайно опасный вирус. При попадании в компьютер, он ослабляет функции системы и всей защиты в целом. В вирусе всегда содержатся спам-сообщения, которые выглядят как банковские счета, кредитные карты или что-то важное. При открытии такого сообщения происходит инфицирование компьютера. Однако обнаружить такой вирус довольно нетрудно. Его появление в компьютере связано с уменьшением производительности и скорости компьютера, а также с появлением “экрана смерти”. При загрузке какого-либо документа или изображения, компьютер не сможет открыть это сразу из-за недостаточного быстродействия. Кроме того, вирус может взять под контроль всю систему, заразив почти каждый уголок компьютера.

Метод защиты:

Рассмотрим защиту компьютера на примере Windows 10.

Сперва нужно войти в настройки системы, выбрать вкладку “приложения и функции”, там удалить вирус и соответствующие приложения. Далее удаляем расширения из браузеров, связанные с вирусом. Рассмотрим удаление на примере браузера Google Chrome. В настройках браузера выбрать “другие инструменты” - “расширения”. Удалить подозрительные расширения, связанные с вирусом. Затем следует устранить вредоносные файлы из реестра, созданные вирусом. Для этого нужно зайти в командную строку (Win+R), ввести команду regedit. Нажать кнопку “Правка” – “Найти…”, ввести название вируса. При нахождении вредоносных файлов – удалить. Последний шаг – сбросить веб-браузеры, чтобы избавиться от рекламного ПО, связанных с вирусом. В настройках браузера, ввести “reset”, подтвердить сброс данных.

Далее рассмотрим, как можно удалить обычный троян с ПК.

Если антивирус не находит самостоятельно троян, а возможность присутствия вируса высока, то можно попробовать обнаружить троян, воспользовавшись специальными утилитами типа TrojanRemover. Этот способ доступен даже самому неопытному пользователю ПК, к тому же этот софт

можно приобрести бесплатно. Для начала разберемся в том, как можно удалить троян вручную.

При обнаружении неизвестной записи, т.е. той, которая не принадлежит нормальным приложениям (перед этим следует изучить данные ветви реестра в чистой системе и найти соответствия запись/приложение), смело можно ее удалить. Следует также просмотреть все, что прописано в автозагрузке. Для этого вводим команду Win+R, набираем msconfig, переходим на закладку “автозагрузка”. Просто нажимаем “отключить” ту или иную программу и при следующей загрузке Windows блокируется. Однако, если троян не был обнаружен в процессах диспетчера задач, стоит запустить утилиту XRun или аналоги. Также стоит изучить список типичных процессов диспетчера задач, чтобы избежать путаницы.

Если признаки заражения трояном до сих пор налицо (слишком большой трафик, неизвестные процессы в оперативной памяти и т.д.), то необходимо просканировать ПК извне на наличие открытых портов. Для такой операции потребуется сканер портов, например, TrojanRemover. Данный способ высокоэффективен, и с его помощью выявляются даже самые скрытные трояны. При обнаружении нестандартных портов следует закрыть их в настройках брандмауэра.

Такие майнинг-вирусы были обнаружены в конце 2017 года экспертами RedLock в компании Tesla, где злоумышленники использовали облачную AWS-инфраструктуру для майнинга криптовалюты Monero.

Злоумышленники сначала проникли в принадлежащий Tesla Kubernetes, так как консоль не была защищена паролем.

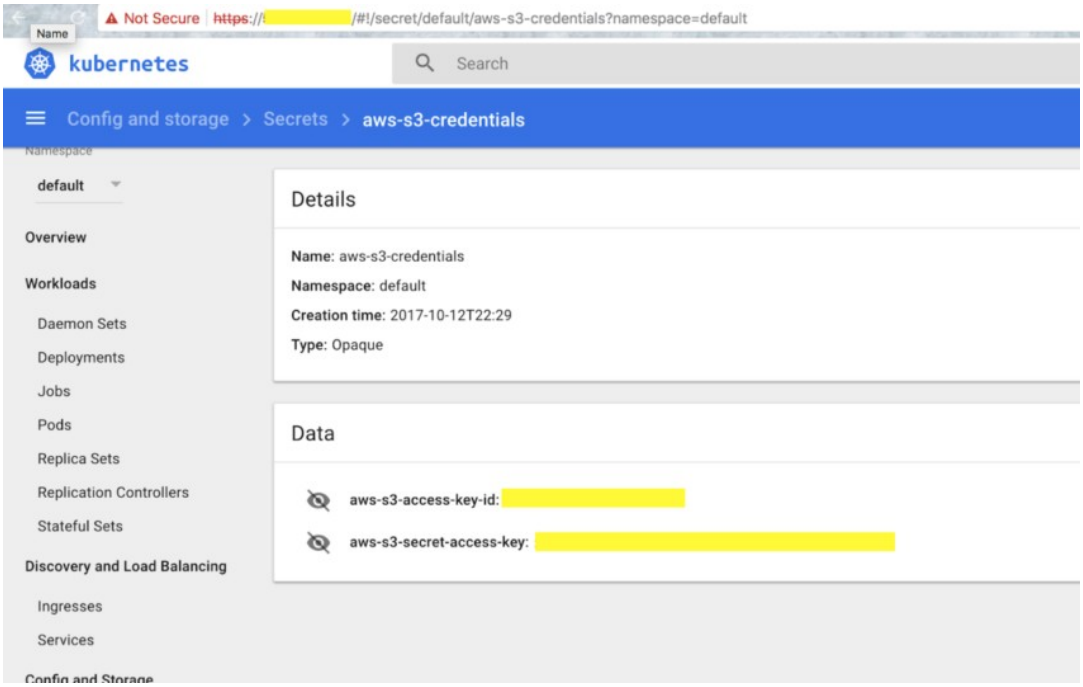


Рисунок 13 – Взломанный Kubernetes

Там они нашли учетные данные для AWS, в котором содержались конфиденциальные данные. Однако представители Tesla заверили, что пользовательских данных там не было. Как бы то ни было, в облаке Tesla обнаружили решение для “добычи” криптовалюты Monero. При этом атакующие настроили майнер таким образом, чтобы его было сложнее заметить: malware использовала CloudFlare и нестандартный порт для выхода в интернет, не оттягивала на себя все мощности ЦПУ и т.д. Специалисты RedLock сразу же уведомили о находке представителей Tesla, после чего те за считанные часы обезопасили пострадавшие части инфраструктуры [6].

Эксперты Лаборатории Касперского в начале ноября 2017 года обнаружили троян, который воровал криптовалюту из кошельков пользователей. Целью злоумышленников стали Bitcoin, Monero и другие.

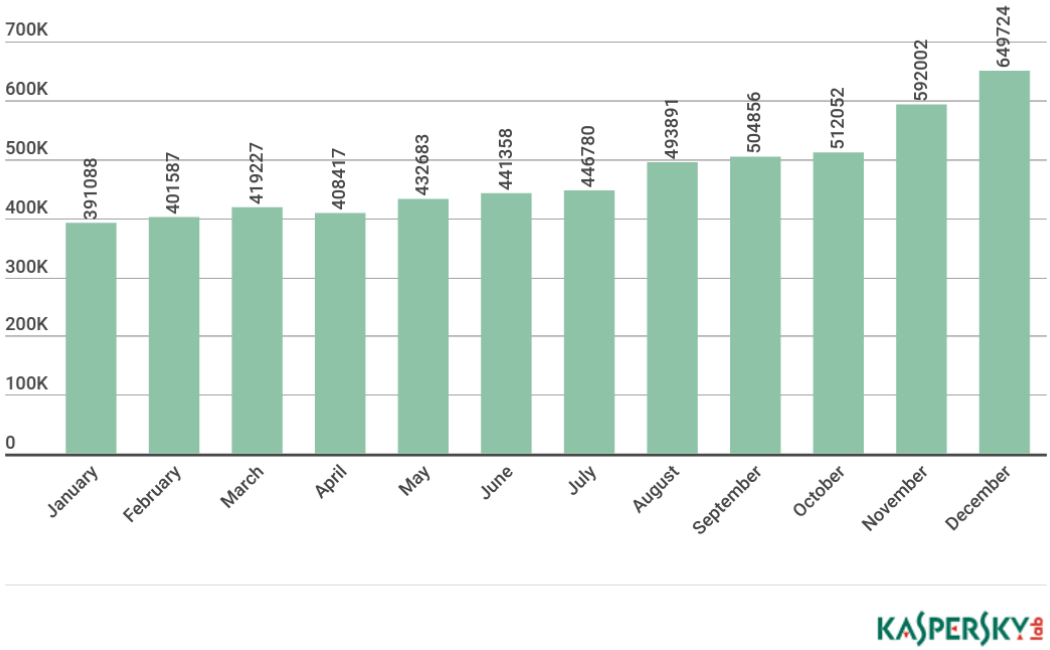


Рисунок 14 – Статистика заблокированных программ-майнеров на компьютерах пользователей за 2017 год [7]

Авторы трояна “CryptoShuffler” больше всего преуспели на атаках Bitcoin-кошельки, украв в общей сложности примерно $140 тыс. По словам экспертов компании, принцип действия трояна довольно прост: он эксплуатирует человеческую невнимательность. Для того, чтобы перевести деньги с одного криптокошелька на другой, пользователю необходимо указать идентификационный номер получателя. Он состоит из множества символов, поэтому запомнить его практически невозможно. В итоге операция выполняется функцией «копировать — вставить». Именно на этом этапе активизируется CryptoShuffler. После загрузки он начинает следить за буфером обмена устройства и, когда обнаруживает там предполагаемый адрес кошелька, подменяет его на свой собственный. В результате, если пользователь на замечает подлога, деньги отправляются напрямую злоумышленникам [8].

Червь

Черви, после удачного инфицирования памяти сохраняют код на жестком диске и принимают меры для последующего запуска этого кода. Зачастую инфекционная часть таких червей содержит нагрузку, которая загружается в

ОЗУ и может догрузить по сети само тело червя в виде отдельного файла. Загружаемое таким способом тело червя отвечает за дальнейшее сканирование и распространение уже с инфицированной системы по локальной сети.

Поэтому компьютерный червь весьма опасен в организациях, где компьютеры связаны по локальной сети.

И если компьютерный червь все-таки появился на компьютере, то первым делом нужно доверить всю работу по удалению антивирусу. Прежде всего нужно обновить базы антивирусной программы. Далее следует отключить интернет, выдернув сетевой кабель или полностью отключив Wi-Fi, чтобы червь не мог передать документы и файлы по сети. Запустите глубокую проверку компьютера.

Для защиты компьютеров от червей можно использовать утилиты, например, SuperAntiSpyware.

После этого нужно запустить утилиту. Она начнет сканирование ПК. Утилита заблокирует активное заражение файлов, просканирует оперативную память, также очистит системный реестр. После сканирования нужно перезагрузить компьютер.

После того, как червь будет окончательно удален, компьютер следует проверить еще раз. Можно воспользоваться, как иным антивирусом, так и воспользоваться утилитой, например, “Dr.Web CureIt!”. Данный продукт отлично дополняет антивирус Касперского.

Чтобы червь не появился снова, необходимо защитить свою сеть. Антивирус Kaspersky Internet Security хорошо справится со своей задачей, также можно усилить безопасность вручную, внеся желаемые изменения в настройках.

Также следует проверить внешние накопители точно также антивирусной программой. Однако делать это нужно аккуратно, не открывая проводник и не просматривая содержимое.

Спам и фишинг

«Значимые международные события всегда привлекают мошенников. На волне всеобщего ажиотажа и повышенного интереса они рассчитывают выманить из невнимательных пользователей ценную информацию и деньги. Довольно часто они даже создают вполне себе похожие на настоящие сайты: с работающим интерфейсом, качественными страницами и https в адресной строке. Так что бдительность в интернете никогда не стоит терять. И лучше доверить распознавание мошеннических страниц качественным защитным решениям», – поясняет Андрей Костин, ведущий контент-аналитик «Лаборатории Касперского» [9].

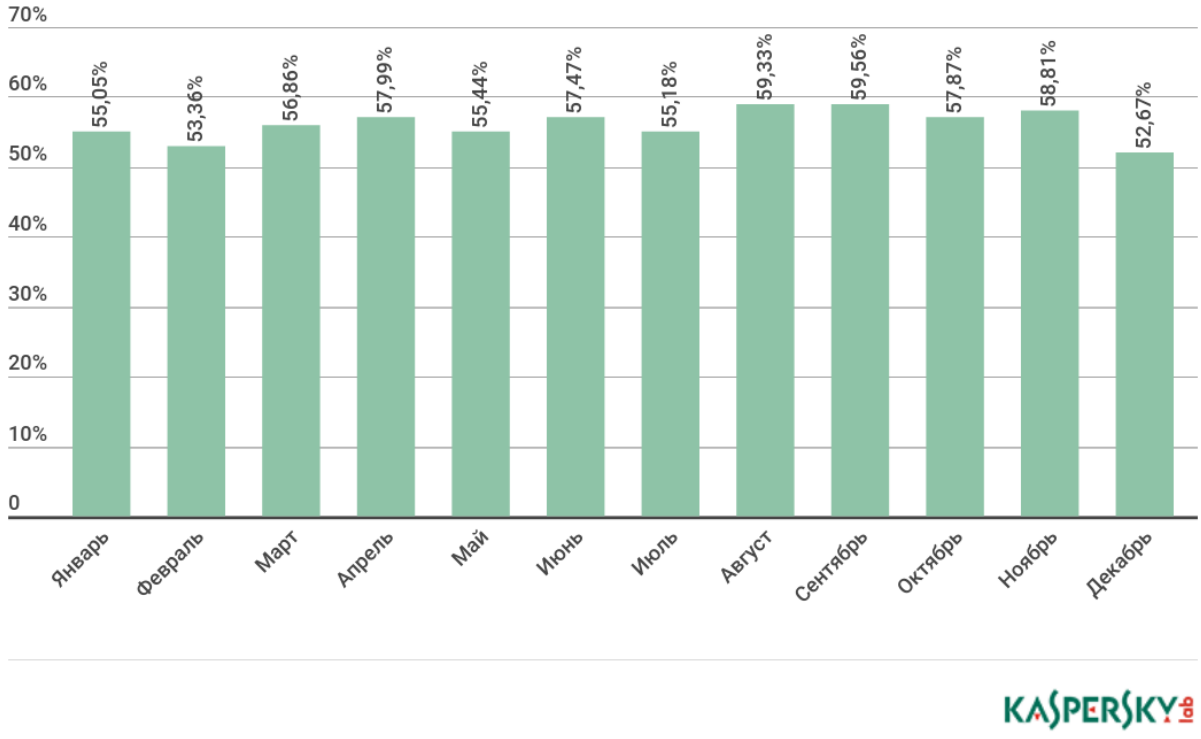


Рисунок 15 – Статистика доли спама в почтовом трафике за 2017 год

На рисунке №15 видно, что самый низкий показатель зафиксирован в конце года – 52,67%. Самый высокий – в сентябре (59,56%) [10].

В 2017 году Лабораторией Касперского было зафиксировано 246 231 645 срабатываний системы “Антифишинг” при попытках перехода на фишинговые сайты. Всего было атаковано 15,9% пользователей.

Чтобы не стать жертвой, «Лаборатория Касперского» советует соблюдать несколько несложных правил:

- По возможности заведите отдельную банковскую карту для онлайн-покупок и ограничьте хранимую на ней сумму;
- Не открывайте ссылки и вложения из писем неизвестных вам отправителей;
- Проверяйте адреса ссылок в оповещениях от известных вам сервисов и в случае даже малейших подозрений не переходите по предлагаемой ссылке – лучше откройте сайт, самостоятельно набрав его адрес в браузере;
- Не покупайте товары, рекламируемые посредством спама, – никто не сможет дать вам никаких гарантий;
- Используйте защитные решения, которые блокируют все актуальные киберугрозы, в том числе фишинг и спам;
- Постоянно проверяйте свои банковские счета на наличие лишних операций;
- Не используйте один и тот же пароль для разных сервисов;
- Регулярно обновляйте ПО, связанное с безопасностью компьютера.

Также стоит проверить компьютер утилитами Kaspersky AVP Tool или Dr.Web CureIT. Проверить в браузере настройки прокси-сервера, возможно, троянская программа изменила их и компьютер попадает на указанное в поле для прокси адрес, где и выходит сообщение с фишинговой ссылкой.

Шпионское ПО

Более мягкое рекламное и шпионское программное обеспечение просто производит мониторинг и отслеживание посещаемых вами сайтов, для того что бы компании могли определить привычки веб-серфинга пользователей, для облегчения своей маркетинговой политики. Однако, многие шпионские

программы выходят за рамки простого отслеживания и фактически контролируют нажатия клавиш, ввод паролей, и другой конфиденциальной информации.

Для удаления такого шпионского и рекламного обеспечения был создан ряд бесплатных и условно-бесплатных программ. Также существует несколько простых шагов, чтобы избежать, обнаружить и удалить такие программы с компьютера.

Метод защиты:

Заходя на сайт, прежде чем нажимать какую-либо кнопку на высветившимся окне – прочитайте, о чем там идет речь. Не рекомендуется, в любом случае, нажимать на это окно.

Защищайте свою систему антивирусными программами. В настоящее время имеется огромный ассортимент антивирусов, поэтому следует выбрать удобный Вам антивирус и использовать его.

Сканируйте время от времени компьютерную систему. Даже с установленным антивирусом, некоторые шпионские программы могут нанести вред компьютеру и данным.

Adware

Такие программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Располагается в рабочем интерфейсе.

Метод защиты:

Чтобы удалить такие программы автоматически, можно скачать утилиты, например, AdwCleaner или Dr.Web CureIT! Эти утилиты помогут обнаружить и избавиться от Adware.

Также можно удалить Adware вручную. Для этого нужно:

1. Нажать пуск – панель управления – удаление программы.
2. Удалите все подозрительные приложения. В первую очередь те, которые явно не устанавливали.

3. Далее нужно зайти в редактор реестра (Win+R – команда regedit), найти и удалить ключи с названием подозрительного приложения (правка – найти).

4. Следует проверить настройки файла Hosts. Для этого нужно перейти в директорию: диск C – Windows – System32 – drivers – etc. Открыть hosts в блокноте, под строкой «# ::1 localhost» не должно быть каких-либо записей; если таковые имеются, удалите их. Сохраните файл.

Rootkit

Руткиты помогают атакующим действовать на компьютерах незамеченными. Действует на зараженном компьютере скрытно и при этом позволяет удаленно контролировать ПК. Руткит может содержать различные вредоносные инструменты, такие как клавиатурный шпион, вор сохраненных паролей, сканер данных о банковских картах, дистанционно управляемый бот для осуществления DDoS-атак, а также функции для отключения антивирусов. Руткит обычно имеет фунции бэкдора.

Метод защиты:

Существуют утилиты, специально созданные для поиска руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа. Удаление руткита – многоэтапный процесс, который редко сводится к удалению пары файлов. Для менее сложных и вредоносных руткитов удаление может быть осуществлено с помощью обычной функции лечения в Kaspersky Internet Security.

Для борьбы с руткитами можно воспользоваться утилитой TDSSKiller. Все, что нужно, так это скачать утилиту, запустить её и дождаться окончания сканирования и лечения.

Ransomware

Программы-вымогатели, попав в систему, шифруют файлы пользователя. Все процессы происходят в фоновом режиме. Закончив шифрование, программа выводит на экран сообщение о том, что нужно заплатить немаленькую сумму в

биткойнах, чтобы эти файлы вернули. “Вылечить” данные без ключа практически невозможно, новые версии программ-вымогателей используют очень стойкое шифрование. Поэтому легче предотвратить заражение системы, чем бороться с последствиями.

Метод защиты:

- Регулярно делать резервные копии всех важных файлов, например, в облаке.
- Настроить спам-фильтр в почте и никогда не открывать вложения к письмам, отправленные незнакомыми людьми.
- Такую программу могут прислать со взломанного аккаунта друга в социальных сетях, так что лучше воздержаться от открытия вложений.
- Включить функцию “Показывать расширения файлов” в настройках. Так будет легче увидеть подозрительный файл. Так как это программа, то файл будет подозрителен с расширением “exe”,”vbs”,”scr”. Но мошенники могут замаскировать под расширение изображения, поэтому всегда нужно быть внимательным.
- Регулярно ставить обновления для ОС, браузера, антивируса.
- Установить качественный антивирус.

Спуфинг

Спуфинг – прием выдачи себя за другое лицо, чтобы обмануть сеть или конкретного пользователя с целью вызвать доверие в надежность источника информации. Злоумышленники могут попытаться применить технику спуфинга IP и DNS – запросов, чтобы обмануть сеть пользователя и переадресовать его на мошеннические сайты, маскирующиеся под настоящие, в результате чего компьютер будет заражен. Распознать спуфинг можно по почте, которую отправил злоумышленник. В сообщении будет требоваться личная информация. Необходимо запомнить, что ни одна частная или государственная организация не запрашивает персональные данные таким путем. Если сайт или его поведение

вызывают малейшее сомнение, стоит сразу отказаться от пользования им, тем более от передачи данных.

Метод защиты:

- Не при каких условиях не сообщать свои персональные данные по электронной почте, даже если репутация отправителя не вызывает сомнения.
- Не отвечать на сообщения, в которых просят прислать свои данные.
- Внимательно проверять адрес отправителя.
- Обращать внимание на странности в поведении или отличия в деталях привычных сайтов.

2.2. Рейтинг антивирусных программ

Антивирусная программа – неотъемлемая часть в создании комплексной защиты организации. Поэтому так важно тщательно тестировать и проверять антивирусы перед установкой на компьютеры. В настоящее время довольно много компаний и исследователей проводят независимые тестирования антивирусных программ. Мы рассмотрим результаты тестирований из двух разных источников, на основе которого я составлю собственный рейтинг антивирусов.

Для начала рассмотрим результаты тестирования немецкой лаборатории “AV-Test”.

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
AhnLab	V3 Internet Security	TOP PRODUCT	6.0	6.0	6.0	18.0
Avira	Antivirus Pro	TOP PRODUCT	6.0	6.0	6.0	18.0
Kaspersky Lab	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5
McAfee	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5
Trend Micro	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5

Рисунок 16 – Результат тестирования за 2018 год специалистами немецкой лаборатории “AV-Test”

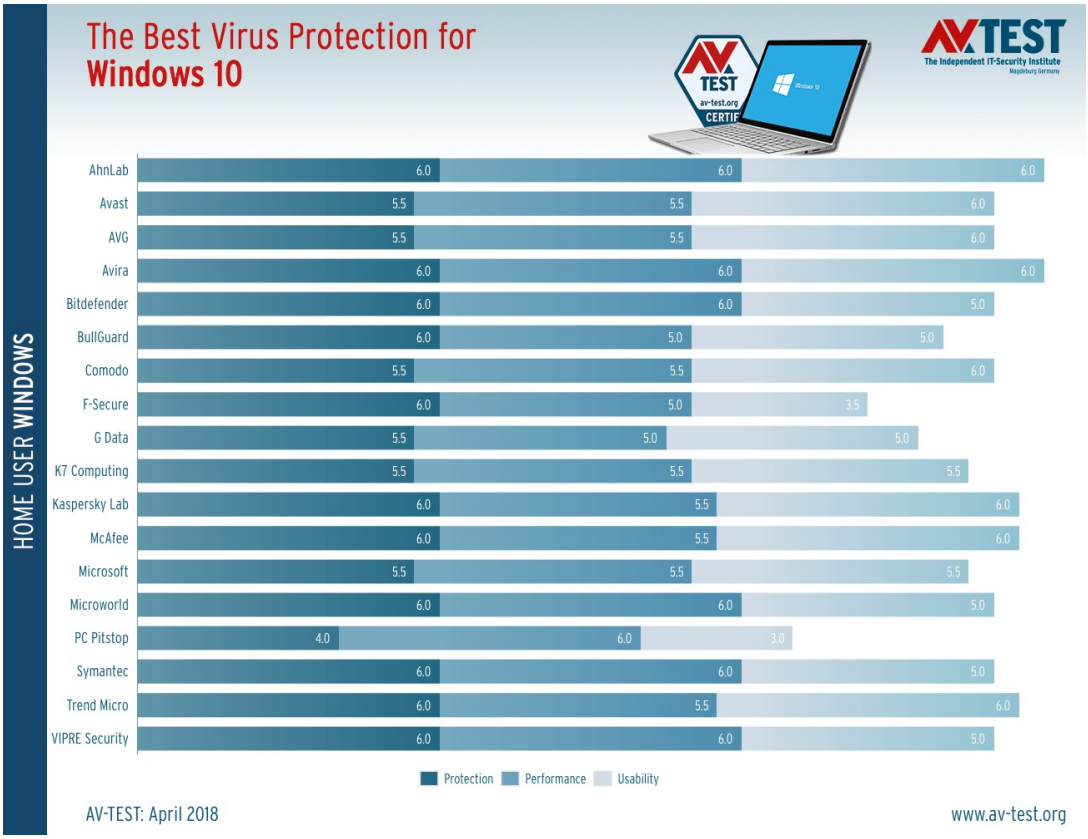


Рисунок 17 – Результат тестирования за 2018 год специалистами немецкой лаборатории “AV-Test”

В этом списке результатов тестирования рассмотрим топ-5. Начнем с последнего места.

Trend Micro - японская компания, основанная в 1988 году в США. Специализируется на разработке средств защиты для серверов, облачных сервисов, бизнеса различного уровня, а также для домашнего использования. Продукция фирмы в области виртуализации и облачной безопасности пользуется большим спросом у таких корпораций, как Microsoft, Amazon, VMware и др. На российском рынке занимает заметное место на уровне с Dr. Web.

Следует отметить, что отзывы пользователей этого антивируса довольно разнообразные. В основном люди сходятся во мнении, что антивирус

недостаточно быстрый, и от этого скорость загрузки компьютера заметно снижается.

McAfee – американская компания, основанная в 1987 году. Основная цель антивирусного комплекса - защита компьютера, приватности и данных пользователя.

В 2017 году производилось тестирование данного антивирусного ПО. Результаты тестирования McAfee в лабораториях являются средними. Продукт получил сертификацию уровня A в Simon Edwards Labs. Из трех тестов AV-Comparatives, McAfee показал проходной балл в одном из них и получил рейтинг на ступень выше в остальных двух испытаниях. В сравнительном тесте AV-Test, McAfee получил 16 баллов из 18 возможных. За защиту продукт получил 4,5 балла из 6. Антивирус не смог пройти два теста от MRG-Effitas - один на защиту от банковских троянов, а другой на блокировку различных видов угроз. Совокупный результат McAfee равен 7,9 баллам из 10 возможных.

В 2018 году McAfee провалил оба теста от MRG-Effitas - на защиту от банковских троянов и на противодействия различным видам вредоносного ПО.

Kaspersky Lab - бесплатный Антивирус Касперского. Решение предлагает файловую защиту в режиме реального времени, веб-антивирус, IM и почтовый антивирус, а также облачные технологии Kaspersky Security Network. В тестах независимых лабораторий Kaspersky систематически получает отличные баллы. Совокупный результат тестирования продукта равен 9,8 баллов из 10 возможных. Тем не менее, Kaspersky эффективно справился с мошенническими угрозами.

В тесте на защиту от фишинга продукт смог обойти Norton Security Premium сразу на 4 процентных пункта и уверенно превзошел встроенные в Chrome, Firefox и Internet Explorer контент-фильтры.

Для проверки защиты от сетевых атак использовалась коллекция из 30 эксплойтов, сгенерированных с помощью инструмента CORE Impact. Kaspersky обнаружил и заблокировал рекордное число тестовых эксплойтов - 73% и смог сместить Norton с 63%-ным уровнем обнаружения на 2-ое место. В любом

случае, даже пропущенные эксплойты не смогли нарушить безопасность полностью пропатченной системы.

Так, Kaspersky вообще не тормозит загрузку файлов с Интернета — от слова «вообще». Файлы качаются с той же скоростью, что и без антивируса. Практически незаметно проходит и копирование файлов, а запуск стандартных программ и установка сторонних проходят вполовину быстрее, чем по индустрии в среднем. Загрузка сайтов также проходит достаточно быстро.

Таблица 1

Тест	Количество проб	Результат	Средний результат по индустрии
Задержка при открытии веб-сайтов	39	13%	11%
Задержка при скачивании файлов	20	0%	4%
Задержка при запуске стандартных программ	12	6%	15%
Задержка при установке сторонних программ	19	14%	26%
Задержка при копировании файлов	7 915	4%	7%

Данные: AV-Test

Avira - это ряд продуктов, обеспечивающих защиту от вредоносного ПО и прочих нарушений безопасности системы и конфиденциальных данных. Бесплатная антивирусная программа для Windows и MacOS сканирует файлы в реальном времени с регулярным обновлением вирусных баз. Версия Pro блокирует проникновение вредоносных и потенциально нежелательных программ через сайты, электронные письма и внешние USB-носители, а также защищает персональные и финансовые данные в интернете. Некоторые вендоры стимулируют покупку за счет добавления внушительной коллекции дополнительных инструментов безопасности. Как это не парадоксально, но Avira Antivirus Pro, наоборот, добавляет не слишком много функций к возможностям

бесплатного антивируса, и не все из них работают хорошо. Единственная реальная причина для покупки Avira Antivirus Pro - защита корпоративной среды.

В 2017 году антивирус участвовал в испытаниях 4 отслеживаемых лабораторий, и совокупный результат продукта равен 9,7 баллов из 10 возможных. За неполное удаление некоторых зловредов позволили Avira набрать только 8,9 баллов за блокировку.

Avira Pro включает дополнительный компонент веб-защиты, который отсутствует в бесплатном антивирусе. При повторном проведении испытания плагин Browser Safety был отключен. На этот раз Avira заблокировала 91 процент вредоносных загрузок. Примечательно, что веб-защита смогла заблокировать только половину угроз, остальные образцы были заблокированы уже в процессе скачивания защитой реального времени. В большинстве случае антивирус запускал быструю проверку, чтобы убедиться, что угроза была тщательно удалена. Во время этих сканировании нагрузка Avira на процессор возрастала до 95 процентов или даже выше.

С Avira файлы в Windows 10 копируются всего на 3% медленнее, чем без антивируса. Загрузка сайтов и скачивание файлов также замедляются настолько незначительно, что это можно проигнорировать. Стандартные приложения Windows при работающем Avira запускаются где-то на 18% медленнее, а сторонние программы устанавливаются чуть ли не вполовину быстрее, чем в среднем по индустрии.

При этом Avira нельзя назвать лучшим антивирусом для Windows 10 — лишь одним из самых быстрых. В плане антивирусного сканирования Avira справляется не на отлично: из 10 684 свежих вирусов сканер находит где-то 97%.

Таблица 2

Тест	Количество проб	Результат	Средний результат по индустрии
Задержка при открытии веб-сайтов	39	8%	11%
Задержка при скачивании файлов	20	8%	4%
Задержка при запуске стандартных программ	12	18%	15%
Задержка при установке сторонних программ	19	12%	26%
Задержка при копировании файлов	7 915	3%	7%

Данные: AV-Test

AhnLab - корейский антивирус, обеспечивающий комплексную и эффективную защиту ПК, с минимальным потреблением системных ресурсов. Предоставляет все необходимые функции для осуществления безопасности на компьютере, предотвращает установку нежелательных программ и вредоносных интернет-угроз в вашу систему. Принцип защиты основан на облачных технологиях.

Обеспечивает защиту системы от стороннего воздействия в режиме реального времени, управление политиками сетевой безопасности, фильтрацию вредоносного веб-содержания и вложений электронной почты, оптимизацию системы и т.д.

В особенности антивируса входят: антивирус и антишпион, веб-защита, защита электронной почты и сообщений, системы предотвращения вторжений и персональный фаервол, сканирование USB-носителей, безвозвратное удаление данных, оптимизация работы компьютера.

Статистика AV-TEST утверждает, что AhnLab практически не замедляет стандартных операций Windows 10: копирование файлов (и локально, и по сети) при запущенном антивирусе тормозится так минимально, что этим можно

пренебречь; то же самое можно сказать о процессах инсталляции программ, скачивания файлов с Интернета и запуска стандартных программ Windows. Слегка «подтормаживает» только загрузка сайтов, но всего на 1% больше, чем в среднем по индустрии. При этом антивирус обнаруживает 100% вредоносного ПО из 10 684 образцов вирусов, собранных в Сети за последние 4 недели.

Тест	Количество проб	Результат	Средний результат по индустрии
Задержка при открытии веб-сайтов	39	12%	11%
Задержка при скачивании файлов	20	4%	4%
Задержка при запуске стандартных программ	12	8%	15%
Задержка при установке сторонних программ	19	7%	26%
Задержка при копировании файлов	7 915	2%	7%

Данные: AV-Test

Таблица 3

Теперь рассмотрим результаты тестирования компьютерного журнала PCMag.

Таблица 4

Вендоры	Антивирусы	Рейтинг PCMag
Avast	Avast Free Antivirus	●●●●◐
Avast	AVG AntiVirus Free	●●●●◐
Bitdefender	Bitdefender Antivirus Free Edition	●●●●○
Check Point	ZoneAlarm Free Antivirus+	●●●●○
«Лаборатория Касперского»	Антивирус Kaspersky Free	●●●●○
Sophos	Sophos Home	●●●●○
Avira	Avira Free Antivirus	●●●◐○
Adaware	Adaware Antivirus Free	●●●○○
Comodo	Comodo Antivirus	●●●○○
Panda Security	Panda Free Antivirus	●●●○○

В этом списке результатов тестирования рассмотрим топ-3 антивируса по набранным баллам.

Антивирус Kaspersky Free – бесплатный антивирус и веб-защита в режиме реального времени с облачными технологиями.

Антивирусное решение включает все необходимые компоненты для обеспечения базовой защиты вашего компьютера, важных данных и онлайн-активности в Интернете от самых современных угроз.

В Kaspersky Free 2018 появились следующие новые возможности:

- Добавлена защита от заражения во время перезагрузки операционной системы.
- Добавлено уведомление от Веб-Антивируса о страницах с рекламными программами и другими легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или вашим данным.
- Улучшена скорость некоторых сценариев установки, первого запуска программы и первого обновления баз и программных модулей.
- Увеличено время до отображения уведомления об устаревших базах и программных модулях при выходе компьютера из режима сна.

Основные возможности антивируса:

- Файловый антивирус – компонент запускается при старте ОС, постоянно проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере.
- Почтовый антивирус – проверяет все входящие и исходящие почтовые сообщения на компьютере.
- Веб-антивирус – перехватывает и блокирует выполнение скриптов, расположенных на веб-сайтах, если эти скрипты представляют угрозу безопасности компьютера.
- IM-антивирус – обеспечивает безопасность работы с IM-клиентами. Защищает информацию, поступающую на компьютер по протоколам IM-клиентов.

- Безопасное соединение – защищает данные при работе в общественных сетях Wi-Fi, обеспечивает анонимность в интернете и дает возможность посещать заблокированные сайты.
- Участие в Kaspersky Security Network – использует защиту из облака. Защита из облака реализуется с помощью инфраструктуры Kaspersky Security Network, использующей данные, полученных от пользователей во всем мире.

Check Point ZoneAlarm Free Antivirus+ - бесплатное комплексное решение, в которое интегрированы антивирус и фаервол для максимальной защиты компьютера и информации от любых Интернет-угроз. Антивирусный движок основан на технологиях Антивируса Касперского.

В основные возможности антивируса входит:

- Антивирус и антишпион;
- Двусторонний фаервол;
- Контроль программ;
- Защита загрузок;
- Защита персональных данных;
- Онлайн резервное копирование.

Ограничения антивируса:

- В бесплатной версии обновление антивирусных баз данных доступно один раз в сутки;
- Нет доступа к ряду настроек антивируса, в отличие от платной версии;
- Отсутствуют: облачная защита в реальном времени, веб-монитор для блокировки онлайн-угроз до попадания на компьютер, проверка файлов электронной почты при сканировании, сканирование файлов на сетевых дисках;
- Возможности персонального фаервола на уровне бесплатной версии;
- Ограничена функциональность планировщика задач.

Недостатки:

- Интегрированы не все возможности антивируса Касперского;

- Отсутствует защита от фишинга;
- Компонент поведенческого обнаружения выдает ложные срабатывания на безопасные программы.

Bitdefender Antivirus Free Edition - бесплатный антивирус, использующий вирусные сигнатуры и проактивные технологии Bitdefender для защиты от новых и неизвестных угроз в режиме реального времени. Функциональность и эффективность полноценных платных решений позволяет надежно защищать компьютер от вредоносных программ, сетевых угроз, мошеннических и фишинговых веб-сайтов.

Основные возможности антивируса:

- Защита в режиме реального времени;
- Облачные технологии;
- Активный вирусный контроль;
- HTTP-сканирование;
- Антируткит;
- Периодическое обновление;
- Раннее сканирование при загрузке системы;
- Сканирование во время простоя;
- Технология Smart Scan.

Недостатком является отсутствие всех функций платного продукта, за исключением антивирусной защиты.

AVG AntiVirus free - не замедляющая работу системы базовая защита компьютера Windows.

Основные возможности антивируса:

- Защита компьютера в режиме реального времени;
- Веб-защита и защита электронной почты;

Уровни защиты антивируса:

- Сигнатурная система обнаружения – сравнивает файлы с известными вирусными определениями, после чего выполняет детальный анализ для выявления типа заражения.

- Полиморфная система обнаружения – используется для обнаружения новых вариантов известного вируса. Данный метод эффективен при обнаружении макровирусов и скрипт-вирусов.
- Эврестическая система анализа – осуществляет мониторинг поведения объектов для выявления их вредоносной природы. Данный уровень защиты позволяет выявить вредоносные программы, которые не содержатся в базе данных сигнатур.
- Поведенческая система анализа – наблюдает за поведением программ и выявляет признаки вредоносного поведения, после чего предотвращает дальнейшее исполнение объекта.
- Обнаружение активных вредоносных вспышек – облачная система обнаружения распространенных заражений.
- CyberCapture – облачная технология интеллектуального сканирования, которая позволяет снизить время обнаружения при изоляции и анализе неизвестных файлов в режиме реального времени.CyberCapture изолирует неизвестные файлы в облачную среду для глубокого анализа и автоматически устанавливает двухканальное соединение с центром AVG Threat Labs для ускоренного обнаружения.

Avast Free Antivirus – ультралегкая и современная защита с минимальной нагрузкой на системные ресурсы.

Бесплатный антивирус Avast был усовершенствован с целью повышения эффективности и снижения нагрузки на системные ресурсы компьютера.

Он включает в себя уникальную технологию CyberCapture собственной разработки, которая автоматически детектирует и отправляет неизвестные файлы в лабораторию онлайн-угроз для анализа в режиме реального времени; кроме того, был усовершенствован компонент Wi-Fi Inspector, который способен обнаружить еще больше типов уязвимостей роутеров.

Он также включает в себя усиленный Игровой режим, отключающий выполняемые в фоновом режиме процессы, гарантируя максимальное удовольствие от игры.

Основные компоненты антивируса:

- Антивирус и антишпион;
- CyberCapture;
- Экран поведения;
- Проверка Wi-Fi;
- Очистка браузера;
- Обновление приложений;
- Подлинность сайтов;
- Интеграция с MyAvast;
- Менеджер паролей;
- Игровой режим;
- Аварийный диск;
- Online Security.

Основные функции антивируса:

1. Защита компьютера:
   - Интеллектуальное сканирование;
   - Антивирус;
   - Анализ поведения;
   - CyberCapture;
   - Режим игры.
2. Защита за пределами компьютера:
   - Анализ сети;
   - Обновление программ;
   - Менеджер паролей;
   - Диск аварийного восстановления.

Мы рассмотрели результаты тестирования двух независимых источников. На основе их результатов, я протестирую три антивируса, наиболее подходящих для коммерческой организации.

Таблица 5

	Kaspersky	Avira	Avast
Общий рейтинг	4,37	4.19	4,17
Стоимость	10 660 р	21 490 р	15 130 р
Версия Windows	10,8,7,Vista,XP	10,8,7	10,8,7,XP
Защита от программ-шпионов	+	+	+
Защита от фишинга	+	+	+
Защита от программ-вымогателей	+	+	+
Защита от спама	+	+	+
Безопасный банкинг	+		
Тонкая настройка	+	+	+
Защита почтового клиента	+	+	+
Менеджер паролей	+	+	+
Создание загрузочного диска	+		

В таблице №5, мы видим, что лидером стал Антивирус Касперского. Общий рейтинг этого антивируса выше, чем у остальных. Следует отметить, что у Kaspersky есть функция безопасного банкинга.

2.3. Стоимость услуг

В настоящее время руководители организаций понимают необходимость антивирусной защиты.

Организация антивирусной защиты небольшого и крупного предприятия отличаются друг от друга. Для сегмента крупного бизнеса более характерно внедрение отдельного продукта для решения конкретной задачи. Для малого бизнеса производители антивирусного ПО, на которых приходится основная

доля рынка, пошли намного дальше антивируса в традиционном его понимании и предлагают пакеты «все в одном», куда могут входить:

- Антивирус. Обеспечивает защиту от вредоносного ПО. В зависимости от производителя и от продукта различаются базы данных вирусов, способы борьбы с вирусами и способы обнаружения вирусов.
- Брандмауэр. Позволяет контролировать активность сотрудников в интернете, запрещать или ограничивать доступ сотрудников к конкретным веб-сайтам или категориям.
- Контроль устройств. С помощью этого механизма можно запретить сотрудникам использовать флеш-карты, разрешить использовать только корпоративные флешнакопители и жесткие диски, или ограничить доступ к сетевому принтеру.
- Контроль работающих в корпоративной сети программ.
- Управление мобильными устройствами. Позволяет контролировать мобильные устройства, подключаемые к корпоративной сети, обеспечивая безопасность данных при работе с такими устройствами.
- Шифрование данных в корпоративной сети, в том числе для передачи файлов по почте.
- Антиспам. Обеспечивает сканирование почты на наличие вирусов, спама, фишинговых писем и других угроз.
- Консоль управления. Дает возможность централизованно управлять всеми компонентами антивирусного ПО.

Разработанное специально для небольших компаний с числом сотрудников до 25, решение Kaspersky Small Office Security просто в установке и управлении.

Стоимость такого решения от Kaspersky – 10 660 руб. в год на 10 ПК.

Возможности Kaspersky Small Office Security:

- Поддержка различных платформ;
- Защита от шифровальщика – в случае атаки автоматически создает резервную копию файла до его зашифровки вредоносным ПО;

- Безопасность ценных данных – шифрование ценных данных и резервное копирование обеспечивают сохранность важной информации в случае потери, кражи или повреждения устройства;
- Безопасная работа в интернете – защита от эксплойтов, фишинговых ссылок при просмотре веб-сайтов и электронной почты;
- Защита финансовой информации – обеспечивает защиту финансовых операций онлайн, а безопасная виртуальная клавиатура предотвращает перехват паролей.
- Производительность – ускорен процесс загрузки установочного пакета программы и пакетов обновлений;
- Менеджер паролей – создание надежных, устойчивых ко взлому паролей.

ЗАКЛЮЧЕНИЕ

Целью данной дипломной работы являлось ознакомление с разновидностями компьютерных вирусов, изучение механизмов их работы, а также борьба с ними с помощью антивирусного программного обеспечения.

Для достижения цели, я определила понятие компьютерного вируса, рассмотрела их классификацию и структуру, также рассмотрела типы вредоносного ПО. Для обеспечения защиты в коммерческой организации я изучила результаты тестирований антивирусов, а также протестировала три

наиболее подходящих антивируса, выбрала самый оптимальный и рассчитала стоимость на комплект персональных компьютеров.

Так как объектом исследования была коммерческая организация, я уделила больше внимания вирусам и вредоносным ПО, которые с наибольшей вероятностью могли появиться на компьютерах организации.

Для обеспечения информационной безопасности, я применяла комплексную антивирусную защиту.

В результате проведенной работы было определено, что существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере.

Во время проведения итогового тестирования антивирусных программ, я столкнулась с трудностями, так как в настоящее время существует большое разнообразие антивирусного программного обеспечения, и выбрать один – было весьма трудно.

Также хотелось бы отметить, что киберпреступность возрастает с каждым годом, поэтому при создании систем безопасности в коммерческих организациях в последние годы особое внимание уделяется вопросам антивирусной защиты.

В заключении данной дипломной работы отмечу, что тема “Организация комплексной антивирусной защиты в коммерческой организации” носит весьма актуальный характер на нынешнем этапе развития вредоносного программного обеспечения.

СПИСОК ИСТОЧНИКОВ

1. https://www.kaspersky.ru/resource-center/threats/malware-classifications [1]
2. https://hi-news.ru/computers/sotrudniki-laboratorii-kasperskogo-nashli-neubivaemyj-kompyuternyj-virus.html [2]
3. https://cyberstat.kaspersky.com/ru/ [3]
4. http://www.2-delete-spyware.com/ru/udalit-trojan-js-miner-m/ [4]
5. https://threats.kaspersky.com/ru/threat/Trojan.Script.Miner/ [5]

6. https://xakep.ru/2018/02/21/tesla-mining/ [6]
7. https://securelist.ru/it-threat-evolution-q1-2018/89800/ [7]
8. http://www.tadviser.ru/index.php/Статья:Вредоносная_программа. [8]
9. http://salamnews.org/ru/news/read/313691 [9]
10. https://securelist.ru/spam-and-phishing-in-2017/88630/ [10]
11. https://www.recoverymaster.ru/algoritm-raboty-kompyuternyx-virusov.html
12. http://life-prog.ru/1_12112_virusi-i-antivirusnie-sredstva.html
13. www.yaklass.ru/materiali
14. https://vms.drweb.ru/virustypes/
15. https://vms.drweb.ru/classification/
16. https://multiurok.ru/files/issliedovatiel-skaia-rabota-komp-iutiernyie-virusy-i-antivirusnyie-proghrammy.html
17. http://www.tadviser.ru/index.php/Статья:Компьютерный_вирус
18. http://www.home-engineer.ru/interesnoe-i-poleznoe-pro-computers/vidy-kompyuternyx-virusov/
19. https://progress.online/bezopasnost/1716-vidy-kompyuternyh-virusov
20. http://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html
21. http://www.globalit.ru/articles/secutiry/view-of-computer-threatening.html
22. http://winlined.ru/articles/Bannernye_virusy_obshchaya_informatsiya.php
23. https://it-sektor.ru
24. https://regnum.ru/news/2415651.html
25. https://hitech.vesti.ru/article/633942/
26. http://www.banki.ru/news/daytheme/?id=9647705
27. https://www.kaspersky.ru/small-business-security/small-office-security
28. https://www.comss.ru