ПРОЕКТ ПО ИНФОРМАТИКЕ ТЕМА”БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ”

Работу выполнил: ученик 9Б класса Морозов Илья

Работу приняла: Сизова М.Ю.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Интернет-безопасность — это отрасль компьютерной безопасности, связанная специальным образом не только с Интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом.

ИНТЕРНЕТ – ЭТО ОБЪЕДИНЕННЫЕ МЕЖДУ СОБОЙ КОМПЬЮТЕРНЫЕ СЕТИ, ГЛОБАЛЬНАЯ МИРОВАЯ СИСТЕМА ПЕРЕДАЧИ ИНФОРМАЦИИ С ПОМОЩЬЮ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ.

Опасные угрозы в сети Интернет:

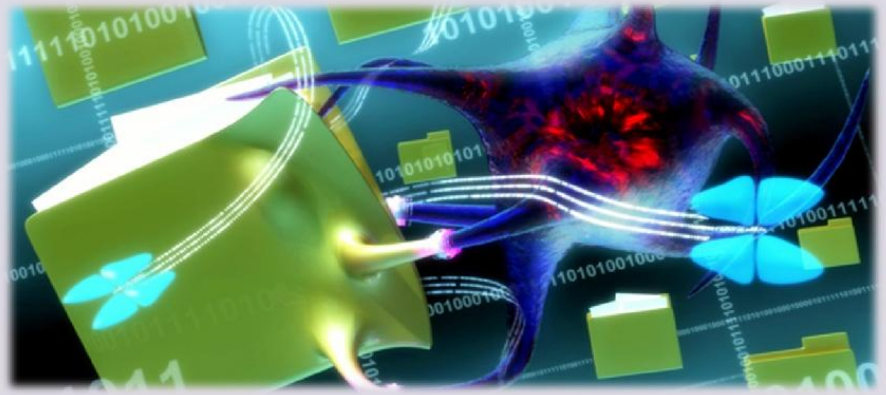
- Угроза заражения вредоносным программным обеспечением (ПО);
- доступ к нежелательному содержимому;
- контакты с незнакомыми людьми с помощью чатов или электронной почты;
- поиск развлечений (например, игр) в Интернете;
- неконтролируемые покупки.

ВИРУС

- ***Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).***

ФАЙЛОВЫЕ ВИРУСЫ

- Файловые вирусы – внедряются в файлы, имеющие расширение COM и EXE



- Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность.

МАКРОВИРУСЫ

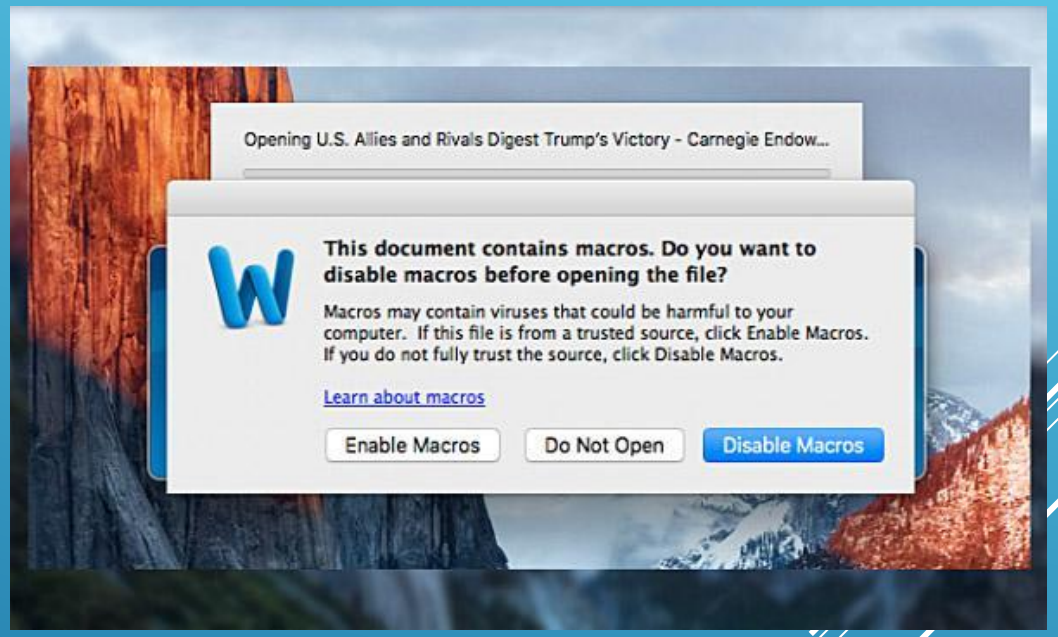
- *Это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.*

МАКРОВИРУС ЧЕРЕЗ ФИШИНГОВЫЕ САЙТЫ

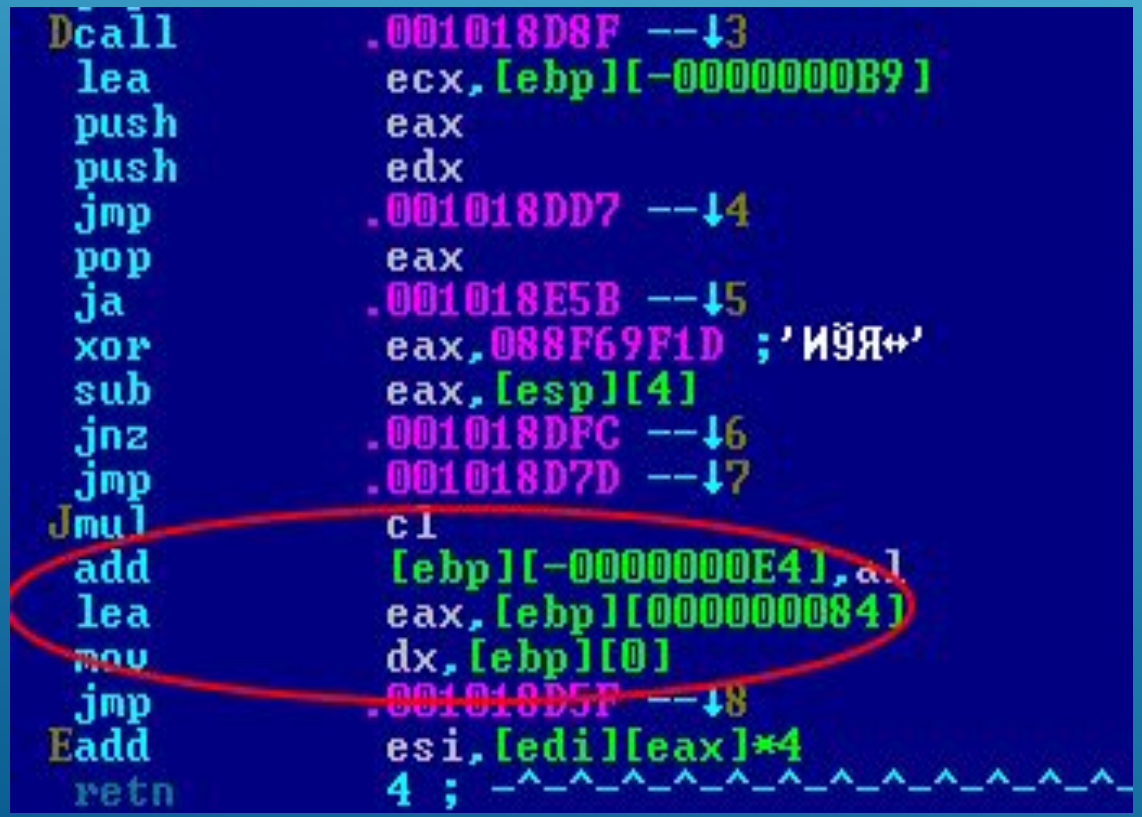
- *Недавно исследователи натолкнулись на рекламную кампанию, в рамках которой злоумышленники пытались заразить пользователей, зарегистрированных на некоторых интернет-ресурсах, и предлагала некую работу, с подробностями которой можно было ознакомиться во вложенном файле. Это был обычный документ Word, а не исполняемый .exe-файл, что и притупило бдительность некоторых жертв. Ведь что может быть не так с обычным документом Microsoft Office?А может быть вот что: в офисных документах могут содержаться макровирусы — зловреды, скрывающиеся в макросах. Макровирусы, как следует из их названия, предназначены для добавления вредоносного кода к макросам электронных документов. Подавляющее большинство макровирусов написаны для файлов Microsoft Office (Word, Excel, Access, PowerPoint и Project) как для Windows, так и для macOS.Если открыть такой документ, он потребует разрешение на выполнение макроса, которое некоторые пользователи ему благополучно выдают. После этого программа устанавливает на устройство жертвы клавиатурный шпион (кейлоггер) или троян удаленного доступа.Когда ваш компьютер заражен подобным зловредом, преступники могут видеть любой текст, который вы набираете, включая логины и пароли. То есть, по сути, могут красть ваши учетные записи и деньги.*

МАКРОВИРУС ЧЕРЕЗ ФИШИНГОВЫЕ ПИСЬМА

- *Часто хакеры используют следующую технику – отправляют жертве фишинговое письмо с прикрепленным документом, содержащим макрос с вредоносным кодом.*
- *Если жертва пытается открыть документ, появляется диалоговое окно с уведомлением о необходимости активировать макросы, чтобы просмотреть его содержимое. Когда макросы включены, выполняется загрузка дополнительного ПО с подконтрольного злоумышленникам сайта.*
- *Специалисты обнаружили вредоносный документ Word, содержавший макрос со скриптом на Python. На начальном этапе макрос определяет, какая операционная система (Windows или macOS) установлена на компьютере, а затем загружает соответствующие версии вредоносного скрипта.*



ПОЛИМОРФНЫЙ ВИРУС



- Вирус,использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации,используемой для получения новых копий шифратора также может быть зашифрована. Например,вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора,но и сам алгоритм.

РУТКИТ

РУТКИТЫ

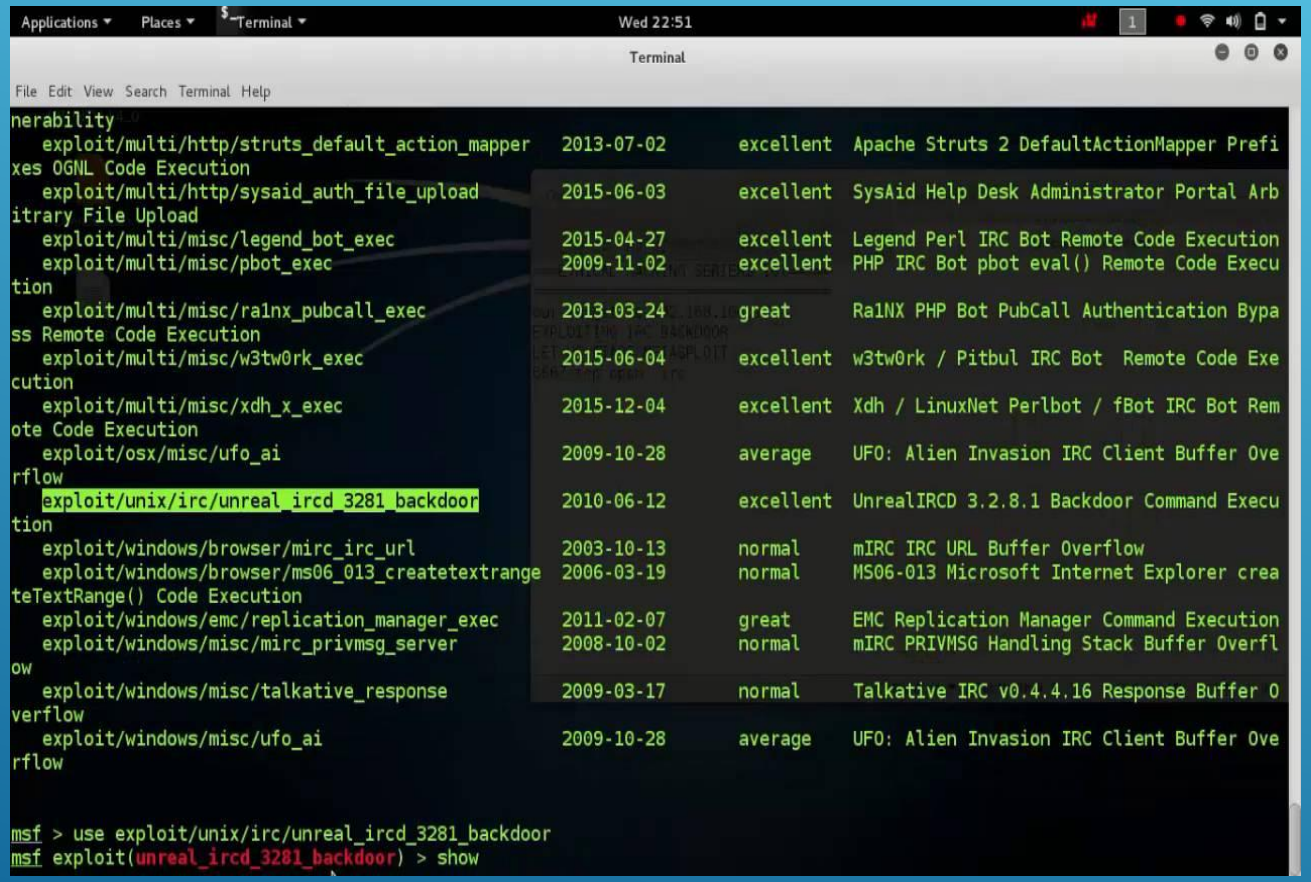
Руткит *(от англ. root kit - «набор для получения прав root»)* - программа или набор программ для скрытного взятия под контроль «взломанной» системы.

В операционной системе Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции.

Многие rootkit устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

ВРЕДОНОСНЫЕ ФУНКЦИОНАЛЬНОСТИ

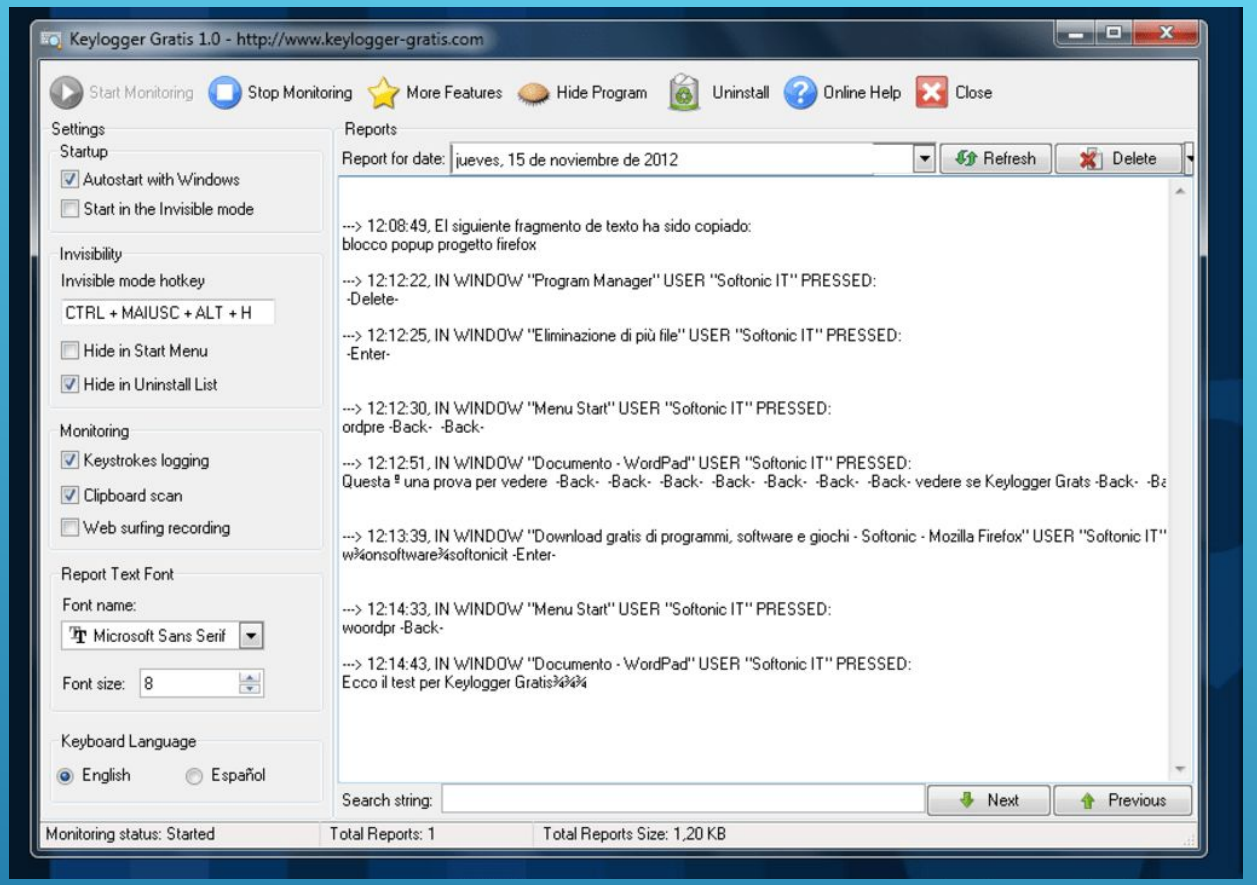
БЭКДОРЫ



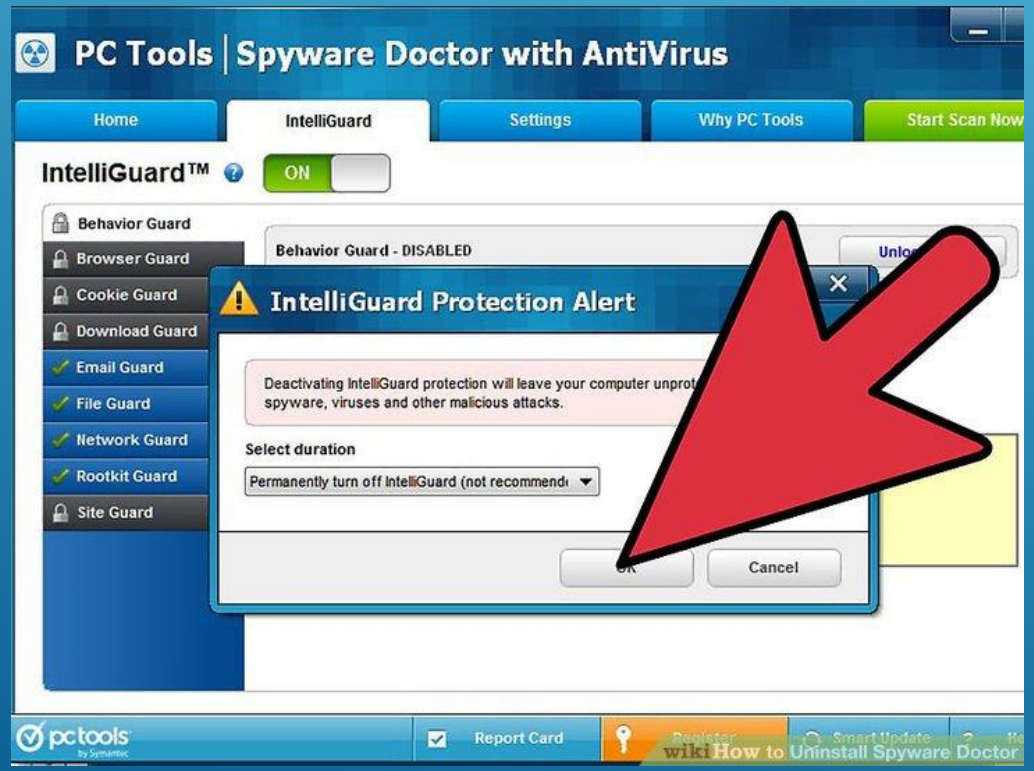
- Backdoor - программная или аппаратная уязвимость, позволяющая получить доступ неавторизованных лиц для кражи данных или управлению ОС.
- Бэкдор устанавливается на компьютер пользователя скрыто, не выдает при этом никаких сообщений, он также может отсутствовать в списке активных приложений.
- Бэкдор позволяет злоумышленникам копировать файлы с зараженного компьютера, а также передавать файлы и программы на зараженный компьютер, получить удаленный доступ к реестру, выполнять системные операции (перезагружать компьютер, создавать новые сетевые ресурсы). Мошенники используют бэкдоры для получения и передачи конфиденциальных данных пользователей, для запуска вредоносных программ, уничтожения информации и пр.
- Обнаружить установленный Backdoor можно при помощи обычного антивирусного сканера или посредством установки межсетевого экрана и контроля за использованием портов компьютера.

КЕЙЛОГГЕРЫ

- Кейлоггером является любой компонент программного обеспечения или оборудования, который умеет перехватывать и записывать все манипуляции с клавиатурой компьютера. Нередко кейлоггер находится между клавиатурой и операционной системой и перехватывает все действия пользователя. Этот инструмент либо хранит перехваченную информацию на зараженном компьютере, либо, если является частью более крупной атаки, все данные сразу передаются на удаленный компьютер организаторов атаки. Хотя термином «кейлоггер» обычно называют вредоносные программы, но порой его используют и правоохранительные органы.



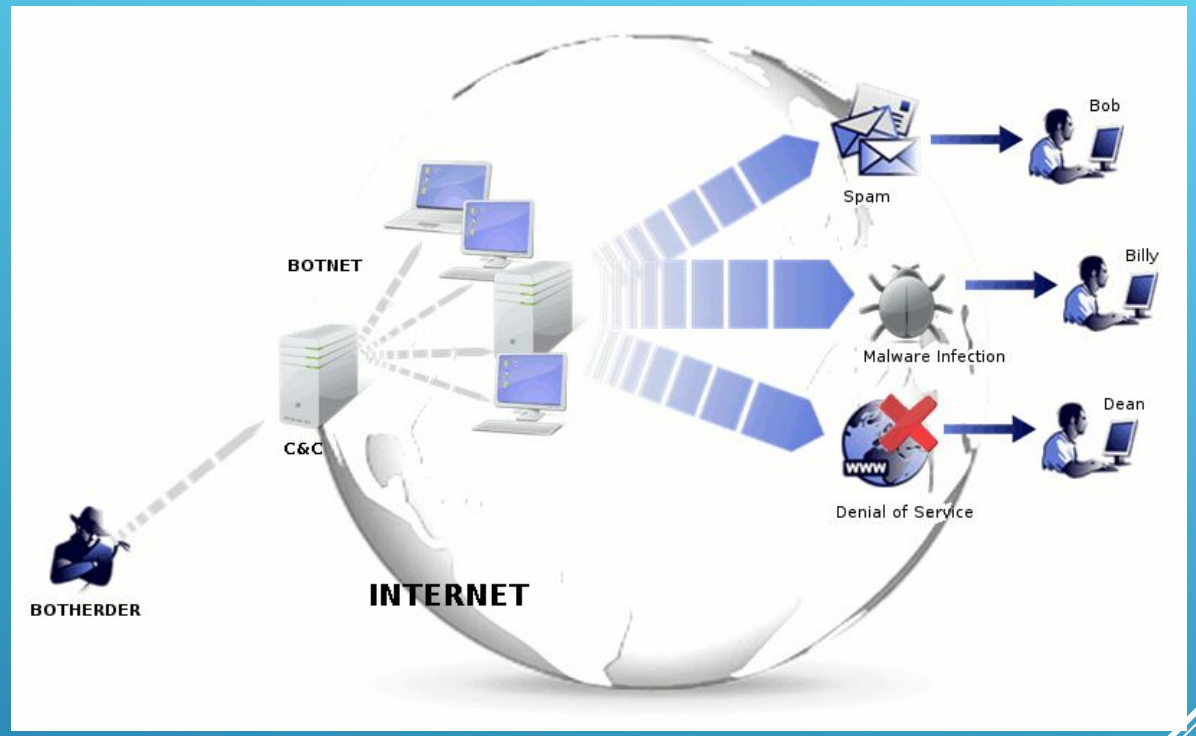
ШПИОНЫ



- Spyware – небольшая шпионская программа - вредитель. Такие программки создаются не простыми людьми, а высококлассными специалистами и способны незаметно внедрится в компьютер с целью: сбора информации о конфигурации компьютера, пользователей или для изменения настроек или установки программ без вашего ведома.

БОТНЕТЫ

- Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.
- Это компьютерная сеть, в которой каждое устройство с доступом в интернет заражено вредоносной программой и управляется бот-мастером. Первые ботнеты начали появляться в 2000-х, и с каждым годом их количество стремительно росло.



БОРЬБА С СЕТЕВЫМИ УГРОЗАМИ

УСТАНОВИТЕ КОМПЛЕКСНУЮ СИСТЕМУ ЗАЩИТЫ!

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам – фильтр и еще пару – тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление.

БУДЬТЕ ОСТОРОЖНЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ!

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlooku Windows Mail помогают блокировать потенциально опасные вложения.

ПОЛЬЗУЙТЕСЬ БРАУЗЕРАМИ MOZILLA FIREFOX, GOOGLE CHROME И APPLE SAFARI!

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. IE до сих пор удерживает первую строчку в рейтинге популярности, но лишь потому, что он встроен в Windows. Opera очень популярна в России из-за ее призрачного удобства и реально большого числа настроек. Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше им и не пользоваться вовсе.

ОБНОВЛЯЙТЕ ОПЕРАЦИОННУЮ СИСТЕМУ WINDOWS!

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

НЕ ОТПРАВЛЯЙТЕ SMS-СООБЩЕНИЯ!

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS. При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус. Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

ПОЛЬЗУЙТЕСЬ ЛИЦЕНЗИОННЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ!

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность. Лицензионные программы избавят Вас от подобной угрозы!

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ!

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

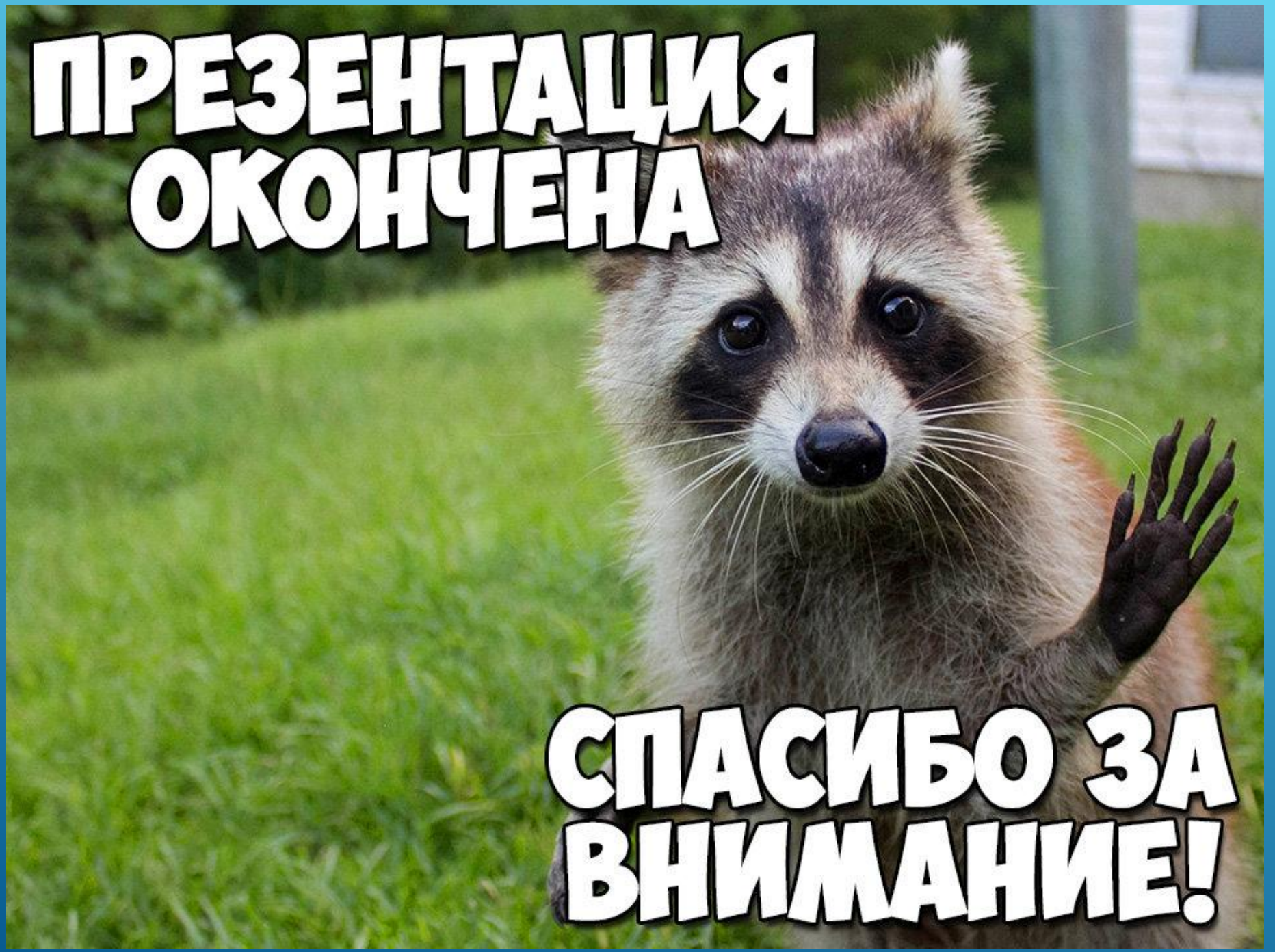
ДЕЛАЙТЕ РЕЗЕРВНЫЕ КОПИИ!

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве –флеш-карте, оптическом диске, переносном жестком диске.


ВЫХОД

ФУНКЦИЯ «РОДИТЕЛЬСКИЙ КОНТРОЛЬ» ОБЕЗОПАСИТ ВАС!

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников. Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.


ПРЕЗЕНТАЦИЯ
ОКОНЧЕНА
СПАСИБО ЗА
ВНИМАНИЕ!