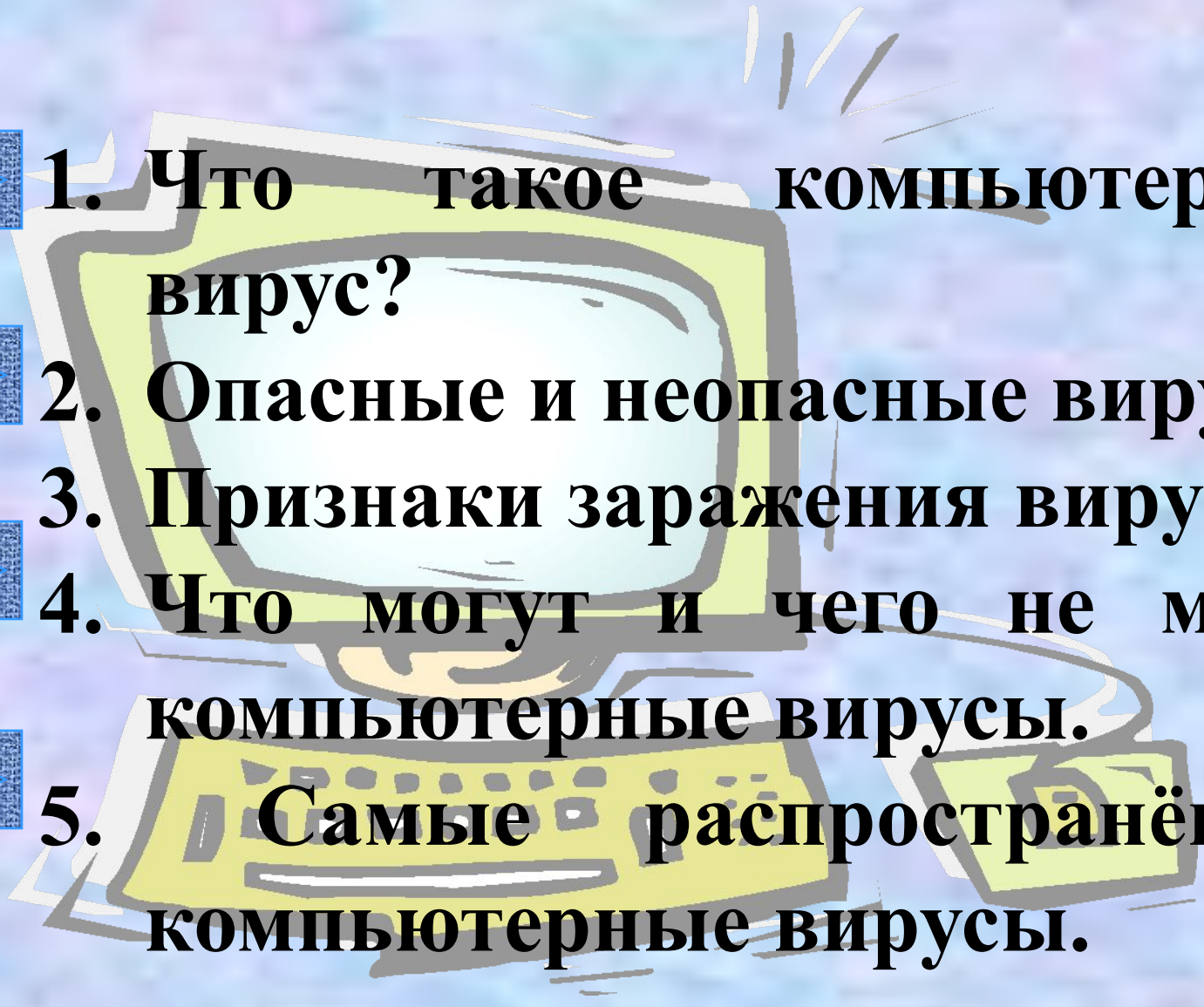
Компьютерные вирусы



1. Что такое компьютерный вирус?
2. Опасные и неопасные вирусы.
3. Признаки заражения вирусом.
4. Что могут и чего не могут компьютерные вирусы.
5. Самые распространённые компьютерные вирусы.

Компьютерный вирус

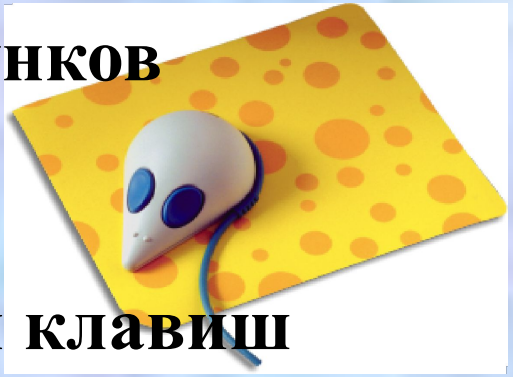
– это специально написанная, как правило небольшая по размерам программа, которая может записывать свои копии в компьютерные программы, расположенные в исполняемых файлах, системных областях диска, драйверах, документах, причем эти копии сохраняют возможность к размножению.

Функционирование вируса.

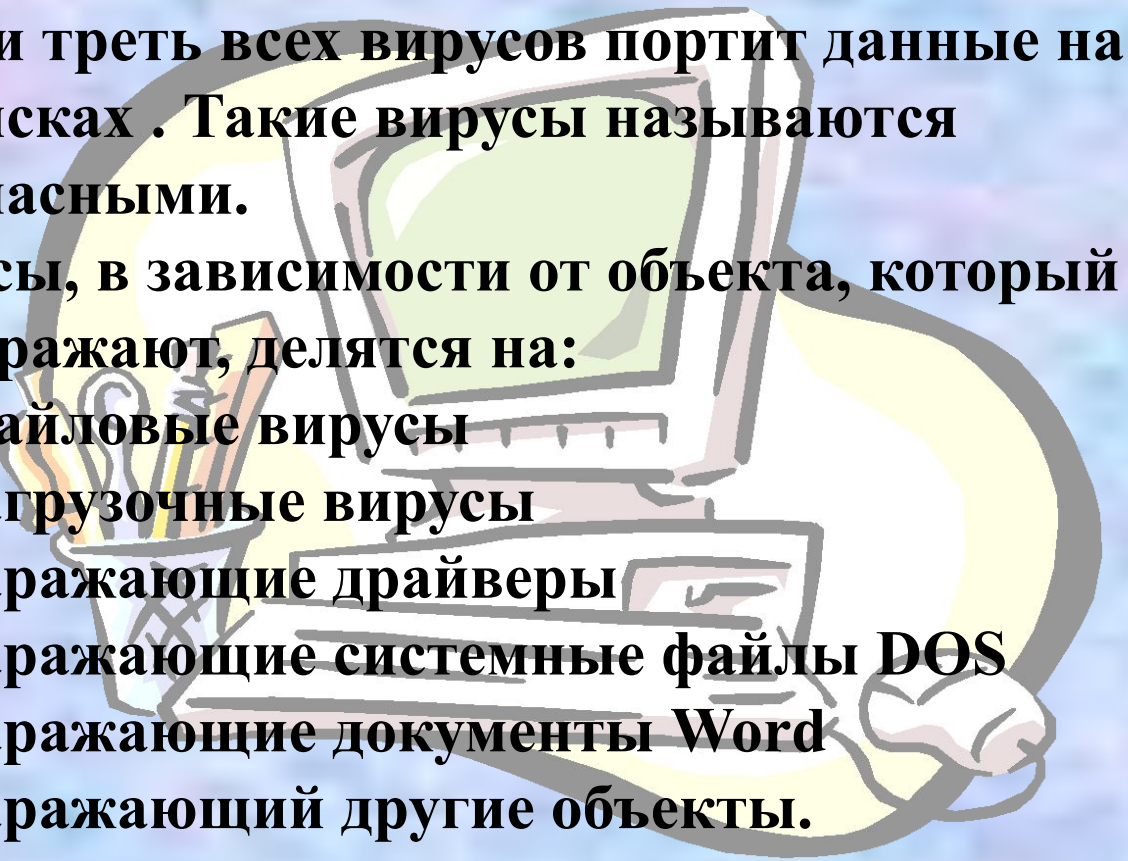
- **Вирус получает управление в момент начала работы зараженной программы.**
- **Вирус находит и «заражает» другие программы, объекты или выполняют вредные действия.**
- **Вирус передает управление той программе, в которой он находится.**

Неопасные вирусы.

- Заражение других программ, дисков
- Выдача каких-либо сообщений, рисунков
- Игра музыки
- Перезагрузка компьютера
- Блокировка или изменение функций клавиш клавиатуры
- Замедление работы компьютера
- Создание видео эффектов



Опасные и очень опасные вирусы.



Почти треть всех вирусов портит данные на дисках . Такие вирусы называются опасными.

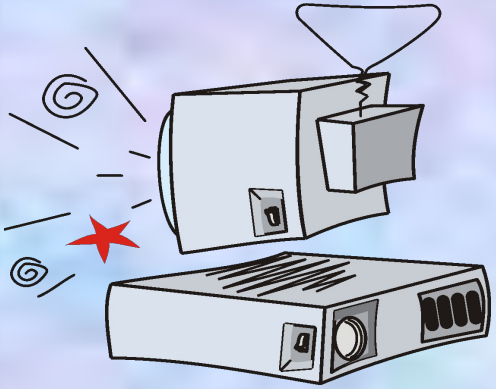
Вирусы, в зависимости от объекта, который они заражают, делятся на:

1. **Файловые вирусы**
2. **Загрузочные вирусы**
3. **Заражающие драйверы**
4. **Заражающие системные файлы DOS**
5. **Заражающие документы Word**
6. **Заражающий другие объекты.**

Возможные признаки заражения вирусом

1. Антивирусная программа сообщает об обнаружении известного вируса
2. На экран или принтер начинают выводиться посторонние сообщения, символы
3. Некоторые файлы оказываются испорченными
4. Некоторые программы перестают работать или начинают работать неправильно
5. Работа на компьютере существенно замедляется

Что могут компьютерные вирусы



1. Обманывать антивирусные программы
2. Выживать при перезагрузке, выключении и включении компьютера
3. Заражать файлы в архивах
4. Бороться с антивирусными программами, уничтожая их файлы или портя базу данных
5. Активизироваться в определенное время после заражения компьютера
6. Шифровать системные области дисков или данные на диске.

Чего вирусы не могут

1. Заражать графические файлы (.bmp, .pcx, .gif.)
2. Заражать текстовые файлы, файлы баз данных
3. Заражать оборудование
4. Заражать или изменять данные, находящиеся на дискетах с установленной защитой от записи.

Классификация компьютерных вирусов

- По способу заражения файлов вирусы делятся на "overwriting", паразитические ("parasitic"), компаньон-вирусы ("companion"), "link"-вирусы, вирусы-черви и вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.
- Подробнее

Прочие вредоносные программы

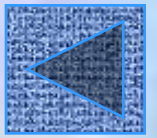
- К "вредным программам", помимо вирусов, относятся также троянские кони (логические бомбы), intended-вирусы, конструкторы вирусов и полиморфик-генераторы.
- Подробнее

Некоторые компьютерные вирусы

- Trojan-Downloader.Win32.Small.dex
- Trojan.Win32.DNSChanger.ih
- Backdoor.Win32.Frauder.aoy
- Worm.Win32.Feebs
- Backdoor.Win32.Haxdoor.gu
- Backdoor.Win32.Padodor.ax

Самые распространённые вирусы

- I) **Trojan-Downloader.Win32.Small.dex**
- Rootkit: НетВидимые проявления: Блокировка диспетчера задач
  Появление множества посторонних процессовСинонимы: Trojan.DownLoader.14760 (DrWeb)
- Троянский загрузчик, 8749 байта размером, сжат FSG. В случае запуска скрытно выполняет следующие операции:
  1. Блокирует запуск диспетчера задач
  2. Модифицирует настройки встроенного Firewall Windows, регистрируя свое приложение в качестве доверенного при помощи команды «netsh firewall set allowedprogram».
  3. Производится скрытную загрузку ряда исполняемых файлов с сайта dfgdfgfdg.biz, причем загруженные файлы сначала сохраняются в папке программы во временных файлах, а затем переименовываются в WINDOWS\system32\z11.exe … WINDOWS\system32\z16.exe.
  4. Производится запуск загруженных файлов.
  Загруженные файлы являются троянскими программами различных типов – на момент исследования загружаемые файлы являлись вредоносными программами Trojan-Dropper.Win32.Small.atd, Trojan-Downloader.Win32.Tibs.jy, Trojan-Downloader.Win32.Tiny.bm, Trojan-Downloader.Win32.Agent.bdr.



Самые распространённые вирусы

- II) **Trojan.Win32.DNSChanger.ih**
- Rootkit: Да
- Троянская программа, исполняемый файл имеет размер 63455 байта, машинный код зашифрован. В случае запуска скрытно выполняет следующие операции:
  1. Проверяет ключ реестра Control Panel\International\Geo, анализируя параметр Nation. Проверка применяется для определения локализации операционной системы, на русскоязычной XP данная вредоносная программа не работает.
  2. Создает на диске файл WINDOWS\system32\kdeiy.exe
  3. Создает в ключе реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon параметр System = kdeiy.exe
  4. Осуществляет построение списка процессов. В памяти системного процесса csrss.exe создает троянский поток
  5. Запускает системный процесс WINDOWS\explorer.exe, внедряет в его память троянский код и запускает его методом подмены контекста
  6. Завершает работу. Внедренный ранее в системные процессы троянский код уничтожает исполняемый файл трояна на исходном месте

  Исполняемый файл system32\kdeiy.exe маскируется на диске по руткит-технологии, за счет перехвата ряда функций в UserMode.
  Ключ автозапуска Winlogon\System в реестре агрессивно защищается, попытка удаления ключа приводит к его немедленному пересозданию. Троянские функции данной программы сводятся к перенаправлению пользователя на посторонние WEB сайты. AVZ успешно нейтрализует перехваты, что позволяет обнаружить маскирующийся файл и удалить его отложенным удалением.

Самые распространённые вирусы

- **III) Backdoor.Win32.Frauder.aoy**
- Троянская программа, предоставляющая злоумышленнику удаленный доступ к зараженному компьютеру. Является приложением Windows (PE-EXE файл). Имеет размер 19456 байт. Написана на C++.
- Деструктивная активность
- После запуска, для контроля уникальности своего процесса в системе троянец создает уникальный идентификатор с именем: XXX5 Внедряет в адресное пространство процесса "WINLOGON.EXE" исполняемый код, обеспечивающий злоумышленнику возможность удаленного управления зараженным компьютером посредством посылки IRC-команд. Добавляет процесс с внедренным кодом в список доверенных приложений Windows Firewall: [HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List] "\\??\\%System%\\winlogon.exe"="\\??\\%System%\\winlogon.exe:*:enabled:@shell32.dll,-1" Отключает функцию восстановления системных файлов. Пытается подключиться к следующим IRC-серверам: irc***ef.pl pro***ircgalaxy.pl если это удается, то он получает ссылки на вредоносные файлы предназначенные для загрузки. На момент создания описания список получаемых ссылок был следующим: http://***mash.cn/oc/box.txt http://***stiya.cn/sp/me.txt http://***stiya.cn/sp/me2.txt http://www.***s.pl/EvID4226Patch.exe Троянец загружает файлы по указанным URL адресам и сохраняет во временный каталог Windows под именами: %WinDir%\TEMP\VRT1.tmp Данный файл имеет размер 11264 байта и детектируется Антивирусом Касперского как Backdoor.Win32.SdBot.pcx. %WinDir%\TEMP\VRT2.tmp Данный файл имеет размер 53248 байт и детектируется Антивирусом Касперского как Trojan-Downloader.Win32.Genome.sas. %WinDir%\TEMP\VRT3.tmp Данный файл имеет размер 59392 байта и детектируется Антивирусом Касперского как Worm.Win32.Agent.zl. %WinDir%\TEMP\VRT4.tmp Данный файл имеет размер 39936 байт. Распространение Внедряет свой код в адресное пространство всех запущенных в системе процессов. Внедренный код перехватывает следующие системные функции в библиотеке ntdll.dll: NtCreateFile NtCreateProcess NtCreateProcessEx NtOpenFile NtQueryInformationProcess при помощи которых следит за открываемыми файлами и запускаемыми приложениями. При обнаружении запуска нового процесса или открытии исполняемого файла производит его заражение. Заражаются файлы с расширениями .EXE и .SCR, которые являются приложениями Windows (PE-EXE). Не заражает файлы, которые содержат в своем имени следующие строки : "WINC", "WCUN", "WC32". При заражении расширяет последнюю PE-секцию заражаемого файла. Зараженные файлы детектируются как Virus.Win32.Virut.ce.

Самые распространённые вирусы

- **IV) Worm.Win32.Feebs**

- Анализ перехваченных функций показывает, что червь может маскировать свой процесс, маскировать файлы на диске, фильтровать обращения к реестру. Кроме того, он перехватывает функции, отвечающие за работой в Интернет.
Интересен перехватчик OpenProcess - при обнаружении попытки открытия маскируемого руткитом процесса перехватчик червя убивает "любопытный" процесс - тем самым существенно затрудняется применение против червя всевозможных менеджеров процессов.
Программный код червя размещен в DLL, которая как правило называется ms*32.dll (известны варианты названия msss32.dll, msgf32.dll).
На эту DLL реагирует искатель кейлоггеров и троянских DLL AVZ:
- Сам DLL файл имеет размер около 54 кб (последний изученный образец имел размер 54697) и запакован UPack.
Червь маскирует один процесс - это процесс svchost.exe, это системный компонент, DLL червя загружена в его адресное пространство.
Распространение червя ведется по электронной почте, письмо имеет вид:

- You have received Protected Message from MSN.com user.
This e-mail is addressed personally to you.
To decrypt the e-mail take advantage of following data:
Subject: happy new year
ID: 18695
Password: wsxoomdxi
Keep your password in a safe place and under no circumstances give it to ANYONE.
Protected Message and instruction is attached.
Thank you,
Secure E-mail System,
MSN.com

К письму приаттачен HTA файл, типичное имя - Encrypted Html File.hta или Secure Mail File.hta, его запуск и приводит к инсталляции червя (при этом имитируется вывод окна запроса пароля, что соответствует контексту письма). Второй вариант - это письмо с ZIP-архивом, который в свою очередь содержит HTA файл. Третий вариант - инсталлятор червя в виде небольшого исполняемого файла размером около 55 кб, один из вариантов имени - webinstall.exe.
Согласно отчетам пользователей в ряде случаев на зараженной машине наблюдается побочный эффект - перестает переключаться раскладка клавиатуры.
Изученная разновидность червя регистрирует CLSID 95BC0491-2934-6105-856B-193602DCEB1F и прописывает себя на автозапуск при помощи ShellServiceObjectDelayLoad (в котором собственно идет ссылка на CLSID червя).
На зараженном компьютере можно обнаружить инсталлятор червя. Он имеет имя ms*.exe (например, mshq.exe) и размер около 55 кб.

Самые распространённые вирусы

Червь создает в реестре ключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSxx, в которо хранит различную информацию. В частности, раздел DAT этого ключа хранит найденные на компьютере email адреса.

- Побочным эффектом работы червя является удаление всех сохраненных на компьютере cookies.
-
- **Анализ HTA файлов, которые применяются для закачки червя.**

HTA файл содержит скрипт, часть которого зашифрована. Шифровка многоступенчатая:
1. В скрипте имеется несколько строковых переменных с несмысловыми именами, которые содержат текст фанкции-дешифратора. Данные в переменных представлены в формате %XX, где XX - код символа. Собственно "дешифрация" сводится к конкантенации строк и обработке содержащейся в ней информации при помощи unescape (в частности, в исследуемом образце это выглядело как "unescape(eb+lc+aqe+iao+hrb);". В результате получается текст функции, который выполняется с помощью eval (побочный эффект - функция становится доступной для последующего кода). Данная функция-дешифратор на входе получат строку, раскодирует ее и выводит в документ при помощи document.write
2. Производится вызов функции-дешифратора. Код
i("T'mmsZF,mvF'jKw"9Z'x$ sZ= .... в скрипте на первый взгляд является мусором, но это не так - это вызов функции с именем "i" (эта функция получается на шаге 1), а бредовые на первый взгляд данные - это зашифрованный скрипт).
3. Функция-дешифратор помещает расшифрованный скрипт в документ, и он исполняется.
Размещенный в документе на шаге 3 скрипт собсвенно и делает всю работу. Его можно классифицировать как Trojan-Downloader. В теле скрипта имеется массив из нескольких адресов, с которых производится загрузка файла. Загрузка оригинальна - загружаемый файл текстовый, поэтому просто производится навигация на один из URL загрузки, а затем полученный текст считывается из Document.Body.InnerText. В моем случае файл сохранялся в папке C:\Recycled\userinit.exe, причем в скрипте предусмотрена проверка наличия там этого файла. В случае отсутствия файла он создается и заполняется результатми расшифровки.
Примечательно, что в скрипте содержится адрес, на который был прислан скрипт - этот адрес сохраняется в реестре.
Второй особенностью скрипт является попытка удаления в реестре сервисов pcipim, pcIPPsC, RapDrv, FirePM, KmxFile. Если хотя-бы одна из попыток удаления оказывается успешной, то скрипт определяет через реестр путь к папке автозапуска и копирует туда загруженный/расшифрованный EXE файл. Если удаление было неспешным (т.е. предполагается, что таких сервисов в реестре не зарегистрировано), то происходит запуска загруженного файла.
Кроме того, в скрипте есть код для прописывания a Active Setup\Installed Components\{CLSID вируса} параметра Stubpath, указывающего на загруженный файл.
Загруженный EXE файл является дроппером DLL, которая собственно и является вирусом.

Самые распространённые вирусы

- **V) Backdoor.Win32.Haxdoor.gu**
- Rootkit: Да
- Haxdoor устанавливается при помощи инсталлятора небольшого размера (55-60 кб), инсталлятор может внедряться на компьютер любым способом, например при помощи эксплоита.
- После установки в системе образуется два файла:
- skyu16.dll, qz.dll - 44034 байта, сжат UPX (заголовки с копирайтами UPX из файла удалены). Прописывается как раширение Winlogon, защищается от анализа путем монопольного открытия файла
- skyu24.sys, qz.sys - драйвер, размер 21904 байта, устанавливается в папку System32 и регистрируется в реесте. Перехватывает ряд функций режима ядра:
  ZwCreateProcess
  ZwCreateProcessEx
  ZwOpenProcess
  ZwOpenThread
  ZwQueryDirectoryFile
  ZwQuerySystemInformation
- Как видно из набора перехваченных функций, руткит может маскировть файлы на диске, искажать системную информацию (в частности список процессов и DLL), отслеживать открытие и создание процессов.
- Haxdoor выполняет маскировку процесса explorer.exe
- В UserMode перехватываются две функции: ntdll.dll:LdrLoadDll и wininet.dll:InternetConnectA, обе подменой первых байт машинного кода на команду JMP.
- Для реализации Backdoor-функций прослушивается порт 16661 TCP
- В папке System32 можно найти файл ps2.a3d - в него в текстовом виде записываются найденные пароли.

Самые распространённые вирусы

- **VI) Backdoor.Win32.Padodor.ax**
-
- Rootkit: Да. Видимые проявления: UserMode перехваты
  Маскировка процесса Okchadpn.exeСинонимы: Backdoor.Win32.Padodor.ax
- Backdoor.Win32.Padodor.ax обнаружен в "живой природе" 25.06.2005, для маскировки применяет классический встроенный RootKit
- Сам Backdoor размещается в файле с имененм Oqjanjpa.exe размером 24167 байта, упакован ASPack. После запуска он перехватывает ряд функций UserMode, фрагмент протокола AVZ:
- 1. Поиск RootKit и программ, перехватывающих функции API >> Опасно ! Обнаружена маскировка процессов >>>> Обнаружена маскировка процесса 1456 Okchadpn.exe 1.1 Поиск перехватчиков API, работающих в UserMode Анализ kernel32.dll, таблица экспорта найдена в секции .text Функция kernel32.dll:FindNextFileW (219) перехвачена, метод APICodeHijack.JmpTo Функция kernel32.dll:Process32Next (647) перехвачена, метод APICodeHijack.JmpTo Анализ ntdll.dll, таблица экспорта найдена в секции .text Функция ntdll.dll:NtQuerySystemInformation (263) перехвачена, метод APICodeHijack.JmpTo Функция ntdll.dll:RtlGetNativeSystemInformation (609) перехвачена, метод APICodeHijack.JmpTo Функция ntdll.dll:ZwQuerySystemInformation (1072) перехвачена, метод APICodeHijack.JmpTo Анализ user32.dll, таблица экспорта найдена в секции .text Анализ advapi32.dll, таблица экспорта найдена в секции .text Функция advapi32.dll:RegEnumKeyA (471) перехвачена, метод APICodeHijack.JmpTo Функция advapi32.dll:RegEnumKeyExA (472) перехвачена, метод APICodeHijack.JmpTo Функция advapi32.dll:RegEnumKeyExW (473) перехвачена, метод APICodeHijack.JmpTo Функция advapi32.dll:RegEnumKeyW (474) перехвачена, метод APICodeHijack.JmpTo Функция advapi32.dll:RegEnumValueA (475) перехвачена, метод APICodeHijack.JmpTo Функция advapi32.dll:RegEnumValueW (476) перехвачена, метод APICodeHijack.JmpTo Как видно по протоколу, этот Backdoor динамически меняет свое имя, перехват функции kernel32.dll:FindNextFileW позволяет ему замаскировать свои файлы, а kernel32.dll:Process32Next - процессы. Кроме того, имеется перехват функций:
  ntdll.dll:NtQuerySystemInformation,
  ntdll.dll:RtlGetNativeSystemInformation,
  ntdll.dll:ZwQuerySystemInformation
  позвляющий реализовать маскировку процессов от утилит, работающих с NativeAPI (перехват на уровне kernel32 наводит на мысль о работоспособности данного зверя в Windows 9x)
  Перехват функций advapi32.dll:Reg**** позволяет замаскировать от обнаружения ключи реестра.

- Автозапуск оригинален. Кроме exe в системе создается \WINDOWS\system32\Npploclm.dll (Backdoor.Win32.Padodor.gen), который прописывается на автозапуск через ключ реестра ShellServiceObjectDelayLoad, имя параметра - "Internet Explorer". Библиотека эта имеет размер 6 кб и решает единственную задачу - запуск программы "Okchadpn" при помощи API функции WinExec (файл этот ищется в системной папке, которая определяется через GetSystemDirectoryA).

-
- **Лечение**
- Нейтрализация перехватов при помощи антируткита AVZ