

Троянские программы

Вперед



Оглавление

- 1) Определение
- 2) Маскировка
- 3) Виды
- 4) Описания
- 5) Глоссарий

Назад

Вперед

- Троянская программа – вредоносная программа, выполняющая несанкционированную пользователем передачу управления компьютером (администрирование) удаленному пользователю, а также действия по удалению, модификации, сбору информации третьим лицам.



- Большая часть троянских программ маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере. Именно поэтому их называют троянцами по аналогии с легендой о троянском коне.

Назад

Вперед

Маскировка

- Троянская программа может имитировать или даже полноценно выполнять задачу какой либо программы (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Trojan.Winlock

ВИДЫ:

Trojan-PSW —
воровство паролей

Trojan-Notifier —
оповещение об
успешной атаке

Trojan-Clicker —
Интернет - кликеры

Trojan-Proxy —
тройские прокси -
сервера

Trojan-Downloader —
доставка прочих
вредоносных
программ

Backdoor — тройские
утилиты удаленного
администрирования

Trojan-Spy —
шпионские
программы

ArcBomb — «бомбы»
в архивах

Trojan-Dropper —
инсталляторы
прочих вредоносных
программ

Trojan — прочие
тройские
программы

Назад

Вперед

Backdoor

- Троянские программы этого класса являются **утилитами удаленного администрирования** компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов.
- Считаются вирусами, так как пользователь не знает об их существовании – отсутствует предупреждения об инсталляции и запуске; процессы бэкдоров не отображаются в диспетчере задач. Пользователь не догадывается, что его **компьютер открыт для управления злоумышленником**.

Trojan-PSW

- **Похитители паролей (Trojan-PSW)** - трояны, предназначенные для получения паролей и прочей конфиденциальной информации, но не использующие слежение за клавиатурой. Обычно в таких троянах реализованы способы извлечения паролей из файлов, в которых эти пароли хранятся различными приложениями.

Trojan-Trojan-Spy

- **Программы категории Trojan-SPY** предназначены для явного шпионажа за пользователем. Это в первую очередь клавиатурные шпионы, всевозможные системы слежения за активностью пользователя. Интересной особенностью многих программ данной категории является то, что они зачастую вполне легально распространяются и продаются, снабжены подробной документацией и инсталлятором. Однако решаемые ими задачи (скрытный сбор информации, скрытная отправка собранной информации в соответствии с настройками) не оставляет сомнений в вредоносности данных программ.

Trojan-Downloader

- Вредоносные программы категории Trojan-Downloader предназначены для скрытной загрузки на пораженный компьютер постороннего программного обеспечения и его последующей регистрацией в реестре или запуском. В некоторых случаях Trojan-Downloader может выступать в роли "первой ступени" почтового вируса - в этом случае с зараженного ПК ведется рассылка не писем с вирусом, а писем с Trojan-Downloader небольшого размера, который в случае запуска загружает основное тело вируса.



- "Следует признать тот факт, что хакеры, как никогда ранее, активны в написании новых вирусов и становятся все более агрессивны в своих попытках отследить новые компьютеры с целью получения полного контроля над ними. Если подключить к Интернету новый компьютер, не защищенный патчами, межсетевым экраном и самым современным антивирусным ПО, он может попасть под контроль хакеров уже через 10 минут", - Грэм Клули, антивирусный аналитик.

Назад

Вперед

Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

t7580620000 на номер 3649

введите полученный код

Активация

для разблокировки у вас есть

02:59:41

*попытка переустановить систему может привести к потере важной информации и нарушениям работы компьютера.

- Блокирует работу операционной системы Windows. Троянец требует отправить СМС или переслать деньги на электронный кошелек и в ответном сообщении или прямо на чеке из платежного терминала получить код разблокировки.

Это следует сделать:

- 1) Воспользоваться онлайн-сервисами подбора кода разблокировки на сайтах производителей антивирусного ПО
- 2) Произвести полное сканирование компьютера антивирусной утилитой со свежими обновлениями антивирусной базы

Этого нельзя делать:

Выполнять требования злоумышленников. Так Вы не будете спонсировать деятельность хакеров. К тому же, в большинстве случаев, вы не получаете код после снятия денежных средств с Вашего баланса.

Назад

Вперед

Борьба с троянцами.

Большинство антивирусных программ эффективно защищают от данных вирусов. Рекомендуется скачивать программы с официальных сайтов издателей.

После удаления вирусов следует исправить записи системного реестра, в который троянские программы могли внести изменения. Это можно сделать с помощью программы CCleaner.

Детальное описание скриншота: Окно «Подробный отчет» в Windows Security Center. В левом меню выделена «Защита от сетевых атак». Основная панель отображает «Защита от сетевых атак» за сегодня, 27.09.2011. Таблица логов показывает четыре события: три запуска задачи Kaspersky Internet Security и одно событие «Неизвестно» с результатом «Запрещено: Intr...». Внизу уведомление о заблокированной сетевой атаке с деталями: время 19:58:14, программа «Неизвестно», объект «UDP от 219.148.1.91 на локальный порт 1434», результат «Запрещено: Intrusion.Win.MSSQL.worm.Helkern».

Время	Программа	Результат
Дата: Сегодня (4)		
27.09.2011 13:44:04	Kaspersky Internet Security	Задача запущена
27.09.2011 15:53:55	Kaspersky Internet Security	Задача запущена
27.09.2011 18:54:45	Kaspersky Internet Security	Задача запущена
27.09.2011 19:58:14	Неизвестно	Запрещено: Intr...

Сетевая атака заблокирована

Время: 27.09.2011 19:58:14
Программа: Неизвестно
Объект: UDP от 219.148.1.91 на локальный порт 1434
Результат: Запрещено: Intrusion.Win.MSSQL.worm.Helkern

Назад

Вперед

Глоссарий

Троянец:

Синонимы: Троянская программа

- В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.
- Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для распределенных DoS-атак на удаленные ресурсы сети).

Шпионская программа

Синонимы: Spyware

- Под определение "spyware" ("шпионские программы") подпадают программы, скрытно собирающие различную информацию о пользователе компьютера и затем отправляющие её своему автору.
- Эти программы иногда проникают на компьютер под видом adware-компонентов других программ и не имеют возможности деинсталляции пользователем без нарушения функционирования использующей их программы. Иногда spyware-компоненты обнаруживаются в весьма распространенных программных продуктах известных на рынке производителей.
- Шпионские программы, проникающие на компьютер пользователя при помощи интернет-червей, троянских программ или при атаках хакерами уязвимостей в установленных программных продуктах, в классификации "Лаборатории Касперского" были отнесены к категории TrojanSpy.

Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которых является способность к **размножению (саморепликация)**. В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.

Неспециалисты ошибочно относят к компьютерным вирусам и другие виды вредоносных программ - программы-шпионы и даже спам. Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру.

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273).

Согласно доктрине информационной безопасности РФ, в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами и обеспечению информационной безопасности в сетях ЭВМ.

Топ 20 вредоносных программ в интернете

<u>Вредоносная программа</u>	<u>Позиция</u>
AdWare.Win32.FunWeb.kd	1
Trojan-Downloader.JS.Agent.fxq	2
AdWare.Win32.FunWeb.jp	3
Trojan.JS.Popupper.aw	4
Trojan.JS.Redirector.pz	5
Trojan.HTML.Iframe.dl	6
Trojan.JS.Redirector.qa	7
Trojan.JS.Redirector.py	8
Trojan.JS.Redirector.qb	9
Exploit.HTML.CVE-2010-4452.bc	10
Trojan-Downloader.JS.Agent.gbj	11
Trojan-Downloader.JS.Agent.fzn	12
Trojan-Downloader.JS.Agent.gay	13
Trojan-Downloader.JS.Iframe.cfw	14
Trojan.JS.Iframe.tm	15
Exploit.JS.Pdfka.dyi	16
Exploit.JS.Pdfka.duj	17
Trojan-Ransom.JS.SMSer.id	18
Trojan-Downloader.JS.Agent.gaf	19
Hoax.Win32.Screensaver.b	20

Назад

Вперед

Назад