

**Лабораторная работа №1 «Изучение путей распространения и форм проявления компьютерных вирусов»**

**Выполнил:**

студент группы 2ИСП11-18

Порядный Д.А.

**Проверил**: преподаватель Возвахов Д. А.

Москва

2022

**Цель работы и содержание:** изучить пути распространения и формы проявление компьютерных вирусов.

Троян: Trojan.AndroidOS.Hiddad

Классификация

Класс: Trojan

Тип: Троян

Платформа: Android

Псевдоним: Hiddad

Информация

Вредоносные программы этого семейства используют рекламу в качестве основного средства монетизации. Их цель – доставить пользователю как можно больше рекламы различными способами, в том числе за счет установки новых скрытых рекламных программ. Используют права суперпользователя для того, чтобы скрыться в системной папке, откуда удалить их будет очень сложно.

Технические детали

Рекламное ПО может проникнуть в систему двумя способами. В первом случае Вы загружаете бесплатную или условно-бесплатную программу, которая незаметно устанавливает рекламное ПО без Вашего ведома или разрешения. Это происходит потому, что авторы программы сотрудничают с производителями рекламного ПО. Почему? Потому что доход от показа рекламы позволяет распространять программу бесплатно (при этом даже платные приложения, полученные из ненадежных источников, могут распространять рекламное ПО). После этого рекламное ПО запускает свои вредоносные алгоритмы – и пользователь понимает, что у "бесплатного" приложения тоже есть своя цена.

Причины возникновения вируса на ПК

Рекламное ПО приносит доход своим разработчикам, автоматически отображая в пользовательском интерфейсе программ или в отдельном окне, которое появляется перед глазами пользователя во время установки того или иного приложения, загружаемые из Интернета рекламные сообщения.

Кого атакует рекламное ПО?

Согласно устоявшемуся представлению основными жертвами рекламного ПО являются частные пользователи, а не предприятия. Рекламное ПО подстерегает пользователей всегда и повсеместно – от компьютеров под управлением Windows или Mac OS, до мобильных телефонов и практически всех типов браузеров. Злоумышленники изобретают все новые мошеннические схемы: предлагают новые игры, фильмы или специальные скидки, завлекают потенциальных жертв якобы полезным бесплатным продуктом, который слишком хорош, чтобы быть правдой.

|  |  |
| --- | --- |
| Название вируса | HIDDAD |
| Тип угрозы | Вирус рекламного ПО |
| Названия обнаружения | BitDefender (TROJAN.ANDROIDOS.HIDDAD), ESET-NOD32 (Script.Generic.Miner.Gen), Kaspersky (Downloader.AndroidOS.Agent) |
| Симптомы | Всплывающие окна, баннеры, появляющиеся справа и слева, и другой навязчивый контент, который не только мешает работать, но даже перенаправляет Вас на неизвестные веб-сайты. |
| Методы распространения | Носители, загрузка приложений со сторонних источников. |
| Ущерб | Трата времени на закрытие рекламы, нагрузка на ПК. |
| Рекомендации по удалению | Соблюдайте меры предосторожности при работе с компьютером. Это означает, что лучше подумать дважды, прежде чем загружать и устанавливать новую программу, особенно если она бесплатна. Перед тем как принимать условия и положения использования, прочитайте их так, как это сделал бы юрист, и немедленно прерывайте процесс загрузки, если возникнет что-либо подозрительное, похожее на разрешение загрузить рекламное ПО. |

Майнер: Trojan.BtcMine.218

Классификация

Категория: Майнер

Тип: Майнерское вредоносное ПО

Платформа: W32

Псевдоним: MinerBTC

Информация

**Тип вируса — майнер, предназначенный для добычи криптовалюты на ПК за счет его ресурсов.**

Технические детали

Работает под процессом NsCpuCNMiner32.exe.

Причины возникновения вируса на ПК

Делается это тремя нехитрыми способами:

1. С помощью программы, установленной на устройство без ведома его владельца либо его собственными руками, но под видом вполне благонадежного софта.
2. С применением браузерных расширений.
3. Посредством зараженного сайта. Вот сидите вы себе спокойно на The Pirate Bay или на сайте Хабаровской городской администрации, а злоумышленники тем временем используют мощности вашего ПК для добычи Monero или другой крипты с повышенной анонимностью.

## Trojan.BtcMine — как удалить?

Данный майнер [обнаруживается в базе](https://vms.drweb.ru/virus/?i=7301756&lng=ru) Доктора Веба. Дата обнаружения — 2015 год. Поэтому можно сделать вывод, что их утилита скорее всего сможет удалить Trojan.BtcMine.

Однако рекомендовано проверить ПК дополнительными утилитами против потенциально опасных модулей.

Используйте следующие утилиты:

* [Dr.Web CureIt!](https://free.drweb.ru/cureit/) — одна из лучших утилит против опасных вирусов, троянов, майнеров, ботнетов. Способна удалить серьезные опасные вирусы. Загружается уже с антивирусными базами, может весить около 100 мб. Длительность проверки зависит от количества файлов на диске.
* [AdwCleaner](https://www.malwarebytes.com/adwcleaner/) и [HitmanPro](https://www.hitmanpro.com/en-us/hmp.aspx" \t "_blank) — утилиты против рекламного/шпионского ПО. Отлично удаляют левые программы, которые вы не устанавливали, а также убирает рекламу с ПК. Проверяют: автозагрузку, реестр, планировщик задач, ярлыки браузеров и их профильные папки и многое другое. Утилиты направлены на удаление одной категории угроз, однако используют разные алгоритмы работы, поэтому рекомендуется проверить обоими, по очереди.

|  |  |
| --- | --- |
| Название вируса | MinerBTC |
| Тип угрозы | Майнер, |
| Ссылки обнаружения | NsCpuCNMiner32.exe |
| Симптомы | Повышенная нагрузка в диспетчере задач. Компьютер зависает. |
| Методы распространения | Сайты, загрузка пиратского контента |
| Ущерб | Ухудшение работоспособности ПК.  Повышенная нагрузка на комплектующие ПК. |
| Рекомендации по удалению | Чтобы удалить вирус нужно воспользоваться антивирусом. |

Ботнет: **Зомби (Zombie) вирус**

Классификация

Категория: Вредоносное ПО

Тип: проведение атак типа Denial Of Service

Платформа: W32

Псевдоним: BotNet

Информация

**Зомби (Zombie)**- это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы.

Технические детали

Если у вас не очень хорошо работает спам-фильтр, то вы прекрасно представляете себе, сколько мусорных писем может прийти на самый обычный электронный адрес. Но далеко не все в курсе, что за большинством спам-рассылок также стоят зомби-сети, ведь провайдеры и специальные агентства жестко преследуют спамеров, блокируя не только их почтовые аккаунты, с которых осуществляется рассылка, но и IP-адреса.

Поэтому злоумышленники для рассылки спама прикрываются адресами компьютеров из ботнета — их подставить не жалко. Кроме рассылок нежелательных писем зомби-сети выполняют и обратную задачу — крадут с зараженных компьютеров адрес почты владельцев, а также все электронные адреса, которые удастся вытащить из списка контактов. Потом эти украденные адреса пополняют спам-базы для рассылок, и круг замыкается.

Причины возникновения вируса на ПК

Когда на электронную почту приходит письмо от неизвестного пользователя, не опытный User может открыть его и занести на компьютер вирус.

Как защититься

Однако совсем отчаиваться не стоит. Есть ряд несложных мер, которые точно помогут снизить риск заражения вашей техники.

1. Не отмахивайтесь от предупреждений файервола о подозрительной сетевой активности установленных приложений, в особенности если установленная программа не подразумевает работы в Интернете.

2. Поменяйте пароли по умолчанию в роутерах, веб-камерах, принтерах, Wi-Fi-холодильниках и во всех остальных устройствах, подключенных к Интернету. Вообще любое устройство с подключением к Сети имеет смысл проверить на возможность установки и смены пароля.

3. Всегда устанавливайте обновления безопасности — и для самой операционной системы, и для остальных программ.

|  |  |
| --- | --- |
| Название вируса | BotNet |
| Тип угрозы | Проведение атак типа Denial Of Service |
| Названия обнаружения | Storm  SpyEye  Sality |
| Симптомы | Компьютер использует бóльшую часть интернет-трафика. ПК зависает. |
| Методы распространения | Ботнеты используются для поиска уязвимостей в еще не зараженных устройствах, установки новых копий самих себя, а также как транспортная сеть для доставки сторонних вирусов, троянов— загрузчиков других зомби-сетей. |
| Ущерб | Снижение скорости интернета. «Лаги» на компьютере. |
| Рекомендации по удалению | Чтобы удалить вирус нужно воспользоваться антивирусом. |

**Контрольные вопросы**

1. Взять описание работы компьютерных вирусов можно с этих сайтов:

* [www.sut.ru](http://www.sut.ru)
* [www.nkj.ru](http://www.nkj.ru)
* habr.com

1. Интернет и носители информации – главные распространители компьютерных вирусов
2. Осложнение загрузки ОС, медленная работа ПК, исчезновение файлов и каталогов или искажение их содержимого и прекращение работы ранее успешно функционировавших программ.
3. Наиболее незаметными проявлениями компьютерных вирусов для пользователя являются использование компьютера пользователя для организации ДДОС- аттак, фишинги, майнеры.