Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Что такое Java
- Риски при использовании Java
- Лучшие способы защиты

Java

ОБ АВТОРЕ

Автор данной статьи - независимый консультант в сфере компьютерной безопасности Арриго Триулзи. Арриго занимается информационной безопасностью более 25 лет. Он работает в Женеве, Швейцария.

ОБЗОР

Ежедневно вы устанавливаете и используете программы на своем компьютере. Примерами являются интернет браузер, текстовый процессор, клиент электронной почты, видео проигрыватель, компьютерные игры. Проблема состоит в том, что большая часть программного обеспечения написана только для определённого типа компьютеров. Так, программы для Microsoft Windows работают только на Microsoft Windows компьютерах и не совместимы с компьютерами Apple Mac. Те же программы для Apple Mac будут работать только на компьютерах Apple Mac. Отличительной особенностью программ, написанных на языке программирования Java, является то, что они могут работать на разных типах компьютеров, например, Microsoft Windows и Apple Mac. Для того, чтобы программы, написанные на языке Java, работали на вашем компьютере, необходимо установить программу Java (чаще встречается название Java Runtime Environment). В этой статье мы поговорим о рисках, связанных с наличием Java на компьютере и о способах защиты вашего компьютера.

Внимание: языки программирования Java и Javascript абсолютно разные вещи. Эта статья относится исключительно к языку программирования Java.

РИСКИ ПРИ ИСПОЛЬЗОВАНИИ JAVA

Основным способом атак, используемых кибер преступниками, является разработка специальных программ, которые находят и используют уязвимости в вашем программном обеспечении. Эти уязвимости обычно характерны для всех компьютеров одного типа. Это означает, что хакерские программы для атаки Microsoft Windows работают только на Microsoft Windows; эти программы не будут работать на других типах компьютеров, таких, как Apple Mac или наоборот. Эта особенность ограничивает возможности и сферу действия хакерских атак.

Java отличается тем, что совместима с различных типами компьютеров. Поэтому кибер преступникам достаточно создать единственную программу, которая потенциально может взломать любые компьютеры в мире, если на них установлена Java. Это и делает

Java

уязвимости Java привлекательной целью атак злоумышленников, так как есть возможность взломать большее число компьютеров с наименьшими усилиями. Следует учесть и то, что Java – сложная программа, соответственно, потенциально существует большое количество уязвимостей. Наконец, большинство людей даже не знают, что такое Java и установлена ли она на их компьютере. В результате, Java стала заманчивой целью кибер преступников.

ЛУЧШИЕ СПОСОБЫ ЗАЩИТЫ

Самый надежный способ защиты прост: если вы не используете программы, требующие Java, не устанавливайте её на компьютер. Устанавливайте Java только в случае крайней необходимости. Если вы не уверены, установлена ли Java на вашем компьютере, существует простой способ проверки. Зайдите на официальный сайт по ссылке ниже и проверьте наличие Java. Будьте осторожны, только проверьте наличие Java, не устанавливайте её.

http://www.java.com/en/download/installed.jsp

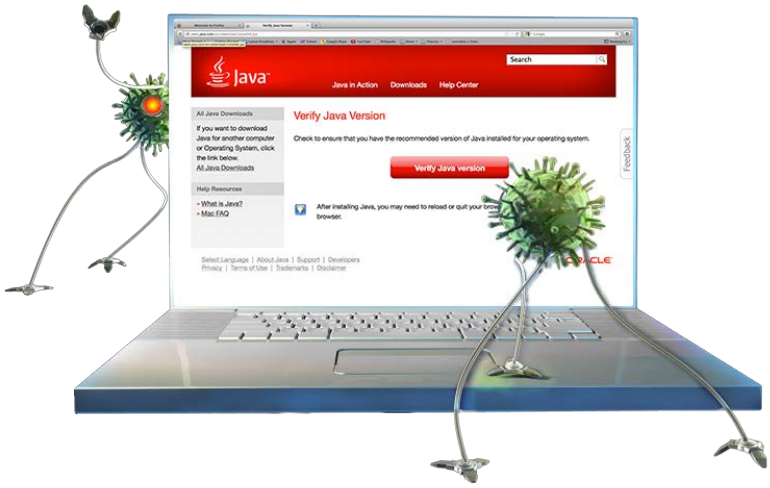
Если вы обнаружили, что Java установлена, но больше вам не нужна, удалите её с вашего компьютера.

ЕСЛИ JAVA ВАМ НЕОБХОДИМА

Если Java вам необходима, следующие советы помогут защитить ваш компьютер.

1. ВСЕГДА ИСПОЛЬЗУЙТЕ ТЕКУЩУЮ ВЕРСИЮ

Убедитесь, что на вашем компьютере установлена последняя версия Java. Устаревшая версия Java содержит множество уязвимостей, и кибер преступники легко могут взломать ваш компьютер с их помощью.



Использование Java повышает риски атак.
Если вы не используете Java, не устанавливайте её.
Если вы пользуетесь Java, работайте только с последней версией программы

Проверить, какая версия используется, и обновить Java, на компьютерах Microsoft Windows очень легко. Щелкните по иконке Java в Панели Управления и убедитесь, что установлена текущая версия Java и настроено автоматическое обновление. Если версия устарела, обновить её можно через меню Java. Для компьютеров Apple Mac опции для Java более сложны. Для лучшей защиты пользователей, Apple распространяет и обновляет собственную модификацию Java на базе версии 1.6. В процессе обновления операционной системы Mac, версия Java автоматически обновляется. Пользователи Apple также могут обновить версию Java до 1.7,

Java

загрузив её с сайта Java, однако в этом случае устанавливать и обновлять эту версию придется самостоятельно.
Будущие версии Java могут содержать дополнительные функции безопасности.

2. ОТКЛЮЧИТЕ ПЛАГИНЫ БРАУЗЕРА

Один из самых простых способов атаки на Java является ваш веб браузер. Если у вас установлена Java, вашему браузеру необходимы так называемые Java плагины, которые позволяют браузеру использовать Java. Когда вы попадаете на заражённый сайт, злоумышленники могут атаковать ваш компьютер через Java плагины. Однако очень немногие сайты требуют Java для работы. Поэтому в большинстве случаев вы можете отключить плагины Java в своем браузере. Способы отключения плагинов зависят от типа браузера. У большинства браузеров есть Предпочтения или Настройки, в которых можно отключить плагины Java. Кроме того, новые версии Java позволяют отключить плагины Java из Панели Управления Java.
Если вы зашли на сайт, который действительно требует Java для работы, то включите Java только для работы с этим сайтом, а затем отключите.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Что такое Java?:
http://preview.tinyurl.com/7l7jvb8

Удаление Java с Windows:
http://preview.tinyurl.com/4x66uco

Удаление Java 7 с Mac:
http://preview.tinyurl.com/cowkxy4

Отключение плагинов Java в веб браузере:
http://preview.tinyurl.com/cwptsxv

Проверка веб браузера Browsercheck:
http://browsercheck.qualys.com

Термины информационной безопасности:
http://preview.tinyurl.com/6wkpae5

Ежедневные советы Института SANS по информационной безопасности:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков