УДК 004.49

магистр Л.Е. Пека
ГВУЗ «Национальный горный университет»

ВРАЖДЕБНЫЕ JAVA - АППЛЕТЫ

В данной статье исследованы враждебные Java-апплеты, описан их принцип действия и возможные угрозы. Предложены возможные пути решения указанных проблем.

Приложения на основе мобильных кодов, реализуемые в виде Java-апплетов, управляющих элементов ActiveX, сценариев JavaScript и других самоисполняемых приложений, могут быть мощным средством распространения информации. Но вместе с нарастанием их мощи возрастает и потенциал их использования в злонамеренных целях.

Злонамеренные мобильные коды все еще мало известны широкому кругу пользователей, поскольку они фундаментально отличаются от более распространенных вирусов, заражающих системы, или непосредственных хакерских атак, способных повредить сеть. Враждебные апплеты не воспроизводят себя или просто повреждают данные, как это делают вирусы, вместо этого они чаще всего осуществляют специфические атаки, направленные на похищение данных или вывод системы из строя.

Java – это язык программирования, разработанный Sun Microsystems для того, чтобы был механизм, позволяющий загружать по Интернету программы и выполнять их на большом числе рабочих станций и персональных компьютеров. Java является интерпретируемым при выполнении, и на самом деле выполняется при помощи программы, называемой виртуальная машина Java(JVM). JVM имеется для Unix, Windows, Macintosh и ряда других ОС, что позволяет выполнять апплеты Java в гетерогенной компьютерной среде.

Модель безопасности Java – строгий контроль среды, в которой выполняются апплеты, с помощью создания безопасной отдельной среды выполнения для работы апплета. Апплеты могут взаимодействовать только с сервером, с которого они были загружены, и им запрещено обращаться к локальным дискам и устанавливать сетевые соединения. Но в Java было обнаружено много ошибок, которые позволяют профессионалам создавать апплеты, легко обходящие ограничения безопасной среды. Sun ответил на это,

сделав "стенки" безопасной среды выше, но и после этого регулярно обнаруживаются новые уязвимые места.

Ни одна из моделей безопасности не является совершенной. Подход Java ограничивает разрушения, которые может вызвать враждебный апплет – если будут найдены и исправлены все ошибки в Java. Некоторые производители брандмауэров поддерживают блокирование и аутентификацию апплетов на своих брандмауэрах.

Следует отметить, что пользователь может и не подозревать, что он загрузил апплет и этот апплет выполнился на его компьютере. Поэтому должны быть предприняты такие меры безопасности:

– Пользователи должны быть проинформированы о рисках интерактивных программ, и о том, как сконфигурировать свои браузеры так, чтобы предотвратить загрузку апплетов.

– Пользователи должны сконфигурировать свои браузеры так, чтобы загрузка апплетов была возможна только из надежных источников. Если это невозможно, то браузеры следует сконфигурировать так, чтобы загрузка апплетов была запрещена.

Подводя итог, можно констатировать, что по мере возрастания масштабов использования мобильных кодов все больше внимания будет уделяться и атакам на основе злонамеренных апплетов.

Перечень литературы:

1. Компьютерные вирусы: Скрипт-вирусы / Script virus / Электронный ресурс / URL доступ http://help-antivirus.ru/drweb_virus_script.php

2. Информационная безопасность: ISSP \ Домен 09. Безопасность приложений. Часть 9 / Электронный ресурс / URL доступ http://dorlov.blogspot.com/2011/04/issp-09-9.html