УДК 004:065.012.8

СЕТЕВАЯ УГРОЗА ТИПА ЧЕРВЬ

Руй С.С., Мешков В.И.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, rui1990@mail.ru

В данной работе рассмотрена вредоносная программа типа «Сетевой Червь», а также методы её роспространения в сети

Ключовые слова – Сетевой Червь, сетевые угрозы;

ВВЕДЕНИЕ

Сетевые черви – это программы, которые основаны с внутренним механизмом распространения по локальным и глобальным компьютерным сетям с определенными целями.

Данными целями являются:

- проникновение на удаленные компьютеры с частичным или полным перехватом управления ими (скрытым от пользователя- хозяина этого компьютера разумеется);
- запуск своей копии на компьютере;
- дальнейшее распространение по всем доступным сетям, как локальным, так и глобальным.

Многие сетевые черви распространяются не только как файлы, а и в виде сетевых пакетов. Таких сетевых червей называются бес файловыми или пакетными, вычислить их достаточно сложно, еще труднее противостоять их попаданию на компьютер, так как вы, реально ничего не скачивая и не запуская никаких файлов, получите себе сетевого червя, просто перейдя на какую-либо Интернет ссылке. Подобные сетевые черви, используя ошибки в программном обеспечении операционных систем, попадают прямо в ОЗУ компьютера и там независимо активизируют свой код.

Сетевые черви также распространяются в сети многими способами. Во первых, конечно, электронная почта, различные программы мгновенного обмена сообщений , файл обменные ресурсы, локальные сети, сети обмена между мобильными устройствами.

Имеются разнообразные виды сетевых червей. В первую очередь нужно упомянуть ОЗУ-резидентных червей, которые располагаются в оперативной памяти компьютера, не затрагивая файлов на жестком диске. Избавиться от таких компьютерных червей достаточно просто – нужно перезапустить операционную систему, при этом произойдет сброс данных, находящихся в ОЗУ, соответственно, сотрется и червь. ОЗУ-резидентные вирусы состоят из двух частей: шелл-кода с помощью которого они проникают на компьютер, и самого тела червя.

Отдельные сетевые черви имеют также свойствами остальных разновидностей вредоносного программного обеспечения. Например, он может содержать троянские функции или также заражают реализовываемые файлы на локальном диске, имеют свойства троянской программы или компьютерного вируса.

Компания Eset в 2010 году обнародовала рейтинг распространенных Интернет-угроз, выявленных специалистами вирусной лаборатории компании в марте 2010 года. В марте текущего года рейтинг мировых угроз в очередной раз возглавил червь Win32/Conficker с показателем в 10,32%. По-прежнему высокий уровень распространения у данной угрозы на Украине – 19,68%, в Германии – 10,09%, в ОАЭ – 9,93%, в Финляндии – 9,65%, в Великобритании – 7,92%.

В первом квартале 2011 были отмечены компьютерные черви Worm.Conficker.Win32, Worm.Palevo.Win32 и Worm.AutoRun.Win32, составляя в сумме более 6% от всех зафиксированных инцидентов. Примечательно, что все эти черви перемещаются при помощи съёмных накопителей (как правило, flash-накопителей), и для червей Worm.Palevo.Win32 и Worm.AutoRun.Win32 «флэшки» являются основным способом распространения от одного компьютера к другому.

В 2012 году специалисты по вирусной безопасности обнаружили настоящий очаг необычной вирусной инфекции в Перу. Новый вирус-червь, получивший название ACAD/Medre.A по классификации компании ESET, похищал различные файлы, включая чертежи и проекты, созданные в популярном пакете AutoCAD, а также почтовые архивы пакета Outlook 11/12, отправляя их неизвестным адресатам в Китае. Стоит заметить, что Перу стала не единственной страной, пострадавшей от вируса ACAD/Medre.A, однако, именно там на данный момент отмечено подавляющее большинство случаев заражения.

Один из самых разрушительных сетевых червей это Червь Морриса он был зафиксирован в 1988 году.Он нанес убытка 96 миллионов долларов. Он парализовал роботу компьютеров своим хаотичным и бесконтрольным размножениям.

Что бы уменьшить риск заражения компьютера сетевыми червями, нужно выполнять некоторые требования:

- не переходить по неизвестным ссылкам;
- не скачивать подозрительные файлы;
- что бы был правильно настроен антивирус, браузер.

ВЫВОД

Для того чтобы не стать жертвой сетевых червей, нужно использовать доверенные сайты, проверять съемные носители.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Независимый информационно-аналитический центр(Электрон. ресурс) /Способ доступа: URL: http://www.anti-malware.ru/worms

2. Википедия (Электрон. ресурс) /Способ доступа: URL: http://ru.wikipedia.org/wiki/Сетевой_червь
3. Сетевые черви (Электрон. ресурс) /Способ доступа: URL: http://www.anvir.net/setevyie-chervi.htm
4. Сетевые черви (Электрон. ресурс) /Способ доступа: URL: http://thelocalhost.ru/setevye-chervi