СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ИММУНИЗАЦИИ ОТ ЧЕРВЕЙ

Ливандовский В.В., Губенко Н.Е.
Донецкий национальный технический университет

Обстановку в современной сети Интернет иначе как «криминогенной» назвать нельзя. Постоянные вирусные и троянские атаки терроризируют практически всех пользователей Интернета — домашних пользователей, небольшие и средние компании, глобальные корпорации и государственные структуры. О причинах подобной криминализации сети говорилось и говорится довольно много — это корыстный интерес.[2]

По данным «Лаборатории Касперского» наиболее активными среди вирусов являются сетевые черви.

К категории червей относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

· проникновения на удаленные компьютеры;
· запуска своей копии на удаленном компьютере;
· дальнейшего распространения на другие компьютеры в сети.[1] Основным признаком, по которому типы червей различаются между собой,

является способ распространения червя — каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам). Email-worm - почтовые черви.

К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте).

В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространенными из них считают: прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку; использование сервисов MS Outlook; использование функций Windows MAPI.

P2P-worm - черви для файлообменных сетей.

Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

IRC-worm - черви в IRC-каналах.

У данного типа червей, как и у почтовых червей, существуют два способа распространения червя по IRC-каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю

сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение). Net-worm - прочие сетевые черви.

Существуют прочие способы заражения удаленных компьютеров, например:

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.[1]

Единственный способ противостоять вирусам - увеличить защищенность своего узла. Для этого можно использовать следующие мероприятия:

- резервное копирование: наличие резервной копии позволяет быстро " подняться" после любого сбоя, к минимуму сводя убытки от потерянной информации;
- переход на более защищенные операционные системы;
- уменьшение привилегий пользователей до минимума: запрет на модификацию исполняемых файлов делает распространение большинства вирусов просто невозможным. Для сетевых червей политика разграничения доступа к файлам документов сведет последствия деструктивных действий вируса к минимуму;
- сокращение избыточной функциональности программ;
- мониторинг изменения файлов: периодический контроль целостности существующих файлов и отслеживание появления новых;
- контроль за обращениям к файлам;
- анализ полученных из сети файлов.

Однако если вы заметили, что ваш компьютер ведет себя некорректно, то есть проявляет признаки зараженности вирусом, то следует отключить компьютер от Интернета и от локальной сети, если он к ней был подключен. Прежде чем предпринимать какие-либо действия, провести резервное копирование вашей работы на внешний носитель (дискету, CD-диск, флэш-карту и пр.). В случае заражения известными вирусами, можно прибегнуть к помощи антивирусов, однако существует весьма высокая вероятность столкнуться с некорректным удалением вируса из файлов, в результате чего система либо полностью теряет свою работоспособность, либо вирус остается не долеченным и "выживает", и зачастую после этого уже не детектируется антивирусом. Лучше просто удалить зараженный файл, восстановив его с резервной копии. Конечно, это не гарантирует того, что в системе не осталось компонентов, скрыто внедренных вирусом.

Поэтому, более надежен следующий путь: загрузившись с заведомо стерильного CD-диска (или дискеты), удаляются папки Windows (WINNT) и Program Files, а затем начисто переустанавливается операционная система вместе со всеми приложениями. Конечно, это медленно, но ничего более лучшего предложить, по-видимому, просто невозможно.[2]

Литература

[1] http://www.kaspersky.ru/ - 18 ноября
[2] http://www. security. strongdisk.ru/ - 20 ноября