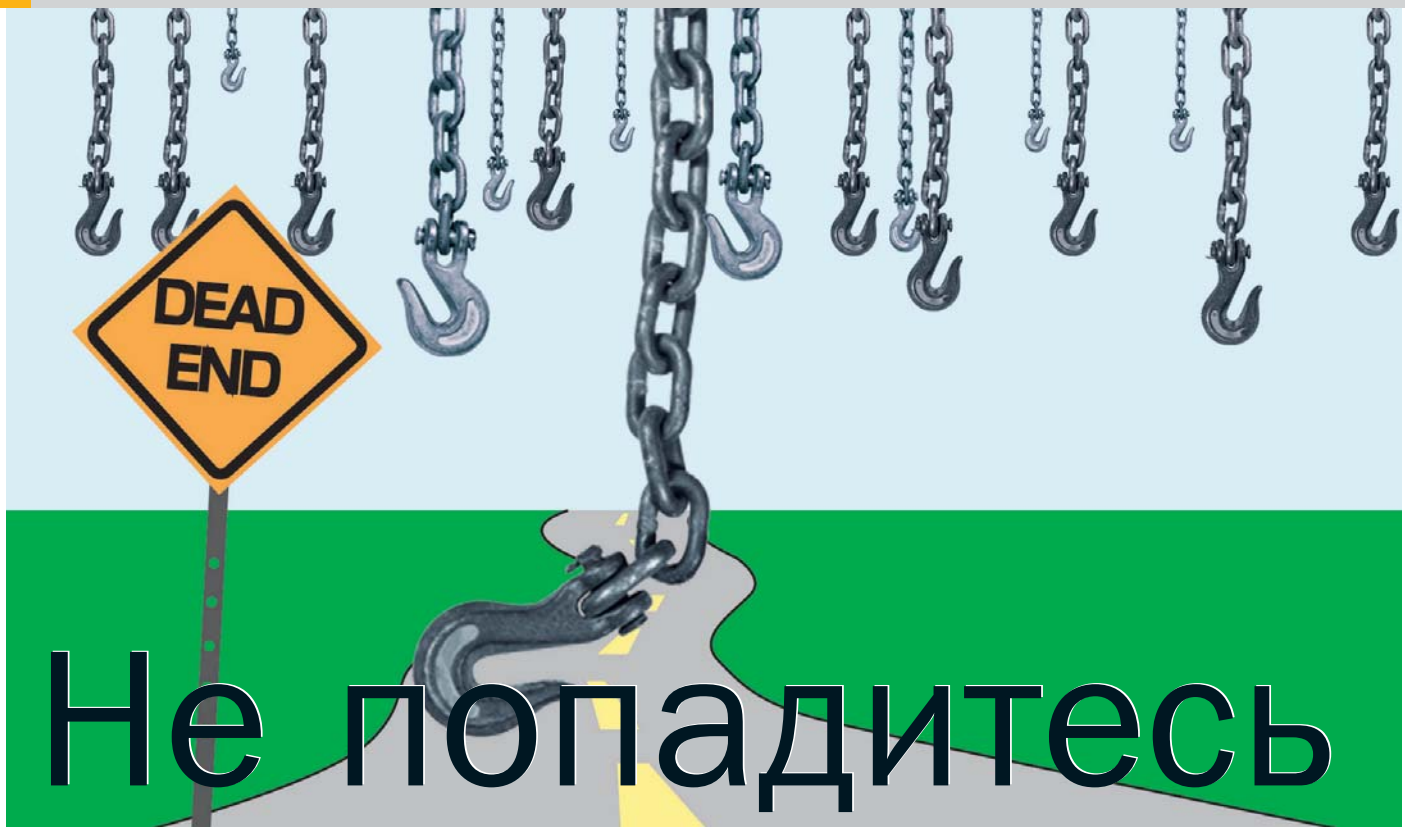


Не попадитесь на крючок

В настоящее время существует около двух десятков P2P-сетей. Стремительный рост популярности файлообменных ресурсов был вызван небывалыми возможностями этой технологии. P2P-сети представляют собой гигантские хранилища файлов. Фактически они превратились в главный источник пиратских копий музыкальных записей, компьютерных игр и, что самое страшное, вирусов.

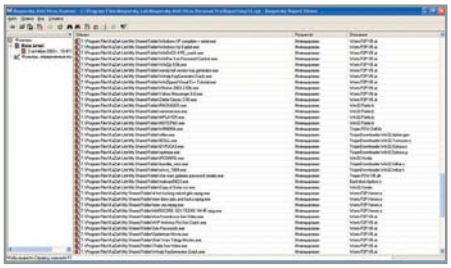
Угроза от Peer-2-Peer

Принципы работы P2P-червей

Что же собой представляет этот, наверное, самый молодой класс сетевых червей и почему с каждым днем их появляется все больше? Краткое определение можно найти в «Вирусной энциклопедии», выпущенной «Лабораторией Касперского»: «Черви, распространяющиеся по системам взаимного обмена данных, работающих по технологии Peer-to-Peer (P2P)».

Данный термин впервые появился весной 2001 года одновременно с возникновением первого P2P-червя Mandragore, распространившегося по сети Gnutella. Принцип размножения был моментально взят на вооружение вирусописателями. Когда пользователь подключается к такой системе, он должен «расшарить» (открыть для доступа извне) один из своих каталогов с файлами, которыми он хочет поделиться с другими участниками системы. Пользователь, ищущий информацию, делает запрос в поисковой системе по интересующим его словам или именам файлов, получает список тех пользователей, на компьютерах которых имеются искомые данные, после чего скачивает их к себе. Именно эту схему распространения файлов используют P2P-черви. Для запуска такого вируса достаточно создать в одном из конструкторов червя, умеющего копировать себя в нужные каталоги (а они практически всегда имеют стандартные названия вроде KaZaa\My Shared Folders) с какими-нибудь привлекательными именами файлов, например: play station emulator crack.exe, warcraft 3 crack.exe, NHL 2003 crack.exe. »

▲ Сообщение антивируса об обнаруженном в файле P2P.Worm



▲ Отчет работы антивируса о проверке каталога файлообмена

» Однако файлы — это всего лишь средство размножения подобных вирусов, которые помимо безобидной функции самораспространения могут содержать в себе и другие чрезвычайно опасные компоненты. Как правило, это процедуры, которые позволяют злоумышленнику получать удаленный доступ к управлению зараженным компьютером. Также довольно часто используются различные троянские функции класса spyware, действующие через рассылку автору информации о зараженных компьютерах. Самым свежим примером подобной функциональности можно считать случай с сетевым червем Lovesan, когда автор версии B, недавно арестованный в США, пытался распространить свою модификацию Lovesan при помощи им же написанных P2P-червей семейства Harex.

Опытным путем

Если обычные интернет-черви, распространяющиеся по электронной почте, можно перехватить при помощи сканеров, установленных на серверах провайдеров, то P2P-червя выявить и удалить можно только непосредственно после его загрузки на компьютер, и только в том случае, если данный червь уже есть в базе данных антивируса. Поэтому единственно надежным способом защиты от таких вирусов является постоянная проверка всех поступающих файлов, а также содержимого всех каталогов, которые вы открываете для доступа. Это необходимо не только вам, чтобы не стать невольным распространителем «заразы», но и всем остальным пользователям систем обмена файлами.

Нами был проведен небольшой эксперимент. В течение получаса из файлообменной сети KaZaa было скачано 37 файлов общим объемом немногим более 5 Мбайт. Затем они были проверены антивирусом с последними обновлениями. 34 файла оказались инфицированы каким-либо вирусом или червем (а иногда и двумя сразу), два файла оказались новыми вариантами различных троянских программ, и только один был полностью безопасным. Разумеется, при отборе файлов для анализа применялись специальные методы, например поиск файлов с именами, наиболее часто использующимися в названии червей. Также предпочтение отдавалось файлам размером менее 200 Кбайт, но несмотря на все эти ограничения, соотношение между чистым и зараженным софтом выглядит просто ужасающе.

Еженедельно «Лаборатория Касперского» регистрирует около десятка новых подобных червей, а ведь, кроме этого, многие современные I-Worm также имеют функцию размножения через P2P. Нетрудно сделать прогноз о том, что в будущем это число будет постоянно увеличиваться. Тем более что компания Microsoft обратила внимание на возможности P2P-сервисов и анонсировала скорый выпуск своего нового продукта — Three Degrees, который даст возможность пользователям формировать онлайновые сообщества с весьма широкими функциями — от организации привычных чатов с широким использованием смайликов и виртуальных персонажей до совместного сбора плейлистов и прослушивания музыки. Скорее всего, там будет и функция обмена файлами.

Рекомендации антивирусных экспертов

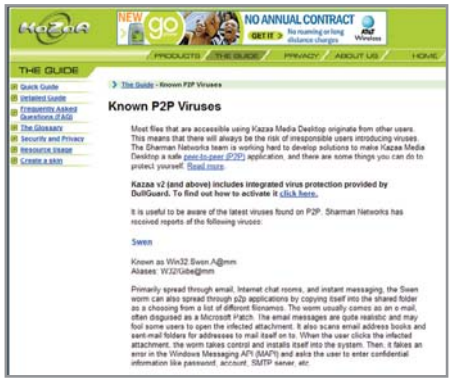
Обязательно проверяйте все полученные файлы антивирусом с самыми свежими базами. Контингент P2P-червей кардинально обновляется в течение 2–3 месяцев, а современные способы обнаружения новых вирусов довольно эффективны и позволяют оперативно вносить их в базы.

Регулярно проверяйте ваш каталог на предмет странных, неизвестных вам файлов, особенно имеющих атрибуты «скрытый» или «системный». В этой папке у вас должны лежать только те файлы, которые вы уже проверили и в содержимом которых вы уверены на все сто процентов.

Особенно подозрительно относитесь к файлам, которые вы хотите себе загрузить и которые имеют малые размеры (менее 200 Кбайт). Помните, что чем больше размер загружаемого файла, тем меньше вероятность того, что он окажется червем. Конечно, это не абсолютная закономерность, но в большинстве случаев это правило работает для всех типов вирусов-обманок.

При выборе файла для загрузки обращайте внимание на количество пользователей, у которых он уже имеется. Большое их число в совокупности с правилом о размерах файла, описанным выше, также может косвенно свидетельствовать о потенциальной опасности.

■ ■ ■ **Александр Гостев**



▲ Информация на официальном сайте KaZaa о P2P-червях и встроенной системе антивирусной защиты

▲ Двадцатка самых популярных вирусов. Выделен червь, распространяющийся через сети P2P