В КОНТАКТЕ С ВИРУСОМ

В МАЕ В РОССИИ БЫЛА ЗАРЕГИСТРИРОВАНА ПЕРВАЯ ЭПИДЕМИЯ КОМПЬЮТЕРНОГО ВИРУСА, РАСПРОСТРАНЯЮЩЕГОСЯ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ. ЧЕРВЬ WIN32.HLLW.ANTIDUROV ЗАРАЗИЛ, ПО ЭКСПЕРТНЫМ ОЦЕНКАМ, ДО СОТЕН ТЫСЯЧ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ СЕТИ «ВКОНТАКТЕ.РУ». СЛЕДОМ АНАЛОГИЧНЫЙ ВИРУС ПОЯВИЛСЯ И В СЕТИ «ОДНОКЛАССНИКИ.РУ». СПЕЦИАЛИСТЫ ОТМЕЧАЮТ, ЧТО СОЦИАЛЬНЫЕ СЕТИ ЯВЛЯЮТСЯ ИДЕАЛЬНЫМ ИНСТРУМЕНТОМ ДЛЯ РАСПРОСТРАНЕНИЯ ВИРУСОВ, ПОСКОЛЬКУ ПОЛЬЗОВАТЕЛИ ДОВЕРЯЮТ РАЗМЕЩЕННОМУ ТАМ СОДЕРЖИМОМУ. ДЕНИС ЗЕНКИН

СОЦИАЛИЗАЦИЯ ВИРУСОВ Главная тенденция последних пяти лет развития интернета заключается в бурном росте социальных сетей — виртуальных объединений пользователей по интересам. По данным аналитической компании comScore за июнь, в глобальном масштабе аудитория этих сетей составляла более 580 млн человек. У каждой из наиболее популярных сетей — Facebook и MySpace — число пользователей превысило сотню миллионов. По числу активных пользователей социальных сетей на первом месте страны Азии (200 млн человек), затем Европа (165 млн) и Северная Америка (130 млн).

Неудивительно, что социальные сети оказались благодатной средой для распространения вредоносных программ, а также различных видов мошенничества. Во многом это связано с доверчивостью пользователей, к тому же разработчики, несмотря на предостережения антивирусных компаний, заверяли аудиторию в полной безопасности своих ресурсов.

Первыми от действий мошенников пострадали пользователи западных социальных сетей, таких как MySpace и Facebook. 4 октября 2005 года в течение 20 часов компьютеры более миллиона пользователей MySpace заразились сетевым червем Samy. К счастью, он оказался обычным «хулиганом»: его единственным проявлением была незначительная модификация профилей учетных записей. Тем не менее автор червя Сами Камкар был арестован и приговорен к исправительным работам с трехлетним испытательным сроком.

Позднее вирусные эпидемии стали распространяться и на другие социальные сети и веб-сервисы. Черви атаковали пользователей Gaia Online, Orkut, Yahoo!, Twitter и даже китайский клон Facebook под названием Xiaonei. В 2008 году началась тотальная эпидемия в социальных сетях: за лето было обнаружено почти два десятка вирусов для MySpace и Facebook, при этом вирусологи наблюдали их бурный качественный рост. В «Лаборатории Касперского» выделили шесть поколений, каждое из которых использовало все более совершенные способы распространения и маскировки.

Российские пользователи также оказались абсолютно не готовы к внезапной атаке со стороны сетевых мошенников. Утром 16 мая СМИ сообщили о появлении червя Rovud — первой в своем роде вредоносной программы, распространявшейся в сети «ВКонтакте.ру». Этот вирус рассылал с инфицированных машин другим пользователям сети ссылку на картинку в формате .jpeg, ведущую на ресурс злоумышленника. Реально же сервер отдавал по этой ссылке исполняемый файл deti.scr, который и является сетевым червем. Запущенный без ведома пользователя файл сохранял на диске саму картинку и запускал приложение для просмотра файлов .jpeg. Таким образом, пользователь видел то, что ожидал увидеть, не подозревая, что в его компьютере поселился вирус. Скопировав себя в одну из системных папок под именем svc.exe, червь устанавливался в систему в качестве сервиса Durov VKontakte Service и находил пароль к «ВКонтакте.ру». Если пароль находился, то червь получал доступ ко всем контактам своей жертвы в данной сети и рассылал по этим контактам все ту же ссылку. Деструктивная функция червя заключалась в том, что 25-го числа каждого месяца в 10.00 начиналось удаление с диска C всех файлов.

Эта проба пера вирусописателей опровергла расхожее представление о том, что «первый блин комом». Rovud на деле доказал свою работоспособность, а его жертвами стали десятки тысяч пользователей. Двумя месяцами позже по сети «ВКонтакте.ру» ураганом прошлась новая рассылка вредоносной программы. На этот раз под видом порноролика распространялась троянская программа Crypt, подчинявшая зараженный компьютер полному контролю злоумышленников. Несмотря на примитивную приманку, «троянец» все же смог поразить более 4 тыс. участников сети.

АНДРЕЙ МАХОНИН

«ОДНОКЛАССНИКИ» И «В КОНТАКТЕ» ПРЕВРАТИЛИСЬ В РАССАДНИКИ ВИРУСОВ

ПРИНЦИПЫ РАБОТЫ Можно выделить три основных метода распространения вредоносных программ через социальные сети. Первый метод заключается в использовании уязвимостей программного обеспечения, которые позволяют заражать компьютеры незаметно для его владельца. Опыт червя Samy показал, что таким способом можно добиться исключительных результатов. Опасность этого метода заключается в том, что жертвами могут стать даже грамотные пользователи, строго соблюдающие правила безопасности в сети. Другими словами, не всегда спасает регулярное скачивание обновлений и наличие антивируса: до момента обнаружения угрозы и распространения «лекарства» проходит какое-то время. Его бывает достаточно, чтобы вирус заразил сотни тысяч ПК.

Второй метод основан на применении методов социального инжиниринга. Различными ухищрениями пользователя вынуждают зайти на специальную страницу в интернете и запустить файл с вирусом. В ход идут испытанные уловки: порноролики, шокирующие подробности об артистах, новые программы — все, что может заинтересовать человека.

Третий способ заключается в использовании учетных записей (и, соответственно, базы контактов) пользователей в качестве платформы для запуска вирусов. В этом случае под прицел попадают пользователи коммуникационных приложений (например, ICQ) и пользователи социальных сетей: им приходят ссылки на зараженные страницы и файлы, якобы присланные друзьями.

Цели создания этих специфических вирусов весьма разнообразны. В целом же вирусописатели пытаются заработать на невнимательности пользователей. Например, «троянец» Agent превращал компьютеры участников сети «Одноклассники.ру» в зомби-машины. С их помощью можно было рассылать спам, проводить хакерские атаки, следить за активностью пользователя, похищать персональные данные. Проникнув в корпоративную сеть, такой вирус мог украсть конфиденциальную информацию, подорвать конкурентоспособность организации, нанести ущерб имиджу. «Мы настоятельно рекомендуем нашим заказчикам отключать доступ к любым социальным сетям. Кроме снижения производительности труда это и серьезная угроза: всего одна успешная атака может стоить компании бизнеса,— говорит Евгений Преображенский, генеральный директор компании Perimetrix.— На фоне быстрого роста количества специфических вирусов доступ к таким сетям из офиса представляется нам неоправданной роскошью».

Популярностью социальных сетей не брезгуют в политических и имиджевых целях. Например, упомянутый выше Rovud перед уничтожением данных выводил на экран оскорбительный текст, якобы написанный основателем «ВКонтакте.ру» Павлом Дуровым. А в начале сентября День города в Москве в сети SecondLife был отмечен выходкой неизвестных персонажей, заполонивших Красную площадь грузинскими флагами.

Вирусные эпидемии этого года вызвали недвусмысленную реакцию антивирусной индустрии. По мнению директора по маркетингу ESET Анны Александровой, прошедшая волна эпидемий лишь предвестник будущих потрясений: «Атаки на российские социальные сети были эффектны, но неэффективны, поскольку антивирусные компании смогли оперативно их локализовать. Очевидно, следует ожидать появления в социальных сетях угроз, приносящих авторам серьезную финансовую выгоду. Для вирусописателей открываются широкие возможности как для банального шантажа владельцев соцсетей, так и для хищения паролей и платежной информации непосредственно с компьютеров пользователей».

МЕТОДЫ ЗАЩИТЫ Существует несколько способов защиты от угроз, исходящих от социальных сетей. Лучший пассивный метод — использование антивирусной программы. Такие продукты установлены практически на каждом компьютере и защищают от вирусов вне зависимости от их источника. Однако антивирус должен регулярно обновляться, а на время между появлением угрозы и выпуском обновления компьютер может оказаться уязвимым. Поэтому важно наличие проактивных методов защиты. Они с достаточной вероятностью смогут обнаружить вредоносный код, который еще не добавлен в антивирусную базу данных. Существенным дополнением к проактивным технологиям является межсетевой экран (МСЭ), который можно приобрести отдельно или в составе комплексных пакетов класса Internet Security. МСЭ позволяет анализировать сетевую активность, выявлять и блокировать потенциально опасные действия.

Несмотря на торжество антивирусных технологий, основой защиты компьютера все равно остается человеческий фактор. Пользователю необходимо знакомиться с новостями, следовать советам специалистов, соблюдать правила компьютерной гигиены. Важным дополнением к этому является отношение к любой сетевой активности (даже знакомых людей) как к потенциальной угрозе и принятие мер предосторожности. Все большую популярность приобретает техника разделения браузеров. Например, для интернет-банкинга используется Opera, для социальных сетей — Firefox, для других случаев — Internet Explorer. Это сокращает шансы успешной атаки и изолирует приложения по функциональному признаку.

История свидетельствует о том, что вирусы не могут остановить развитие сетевых технологий, хотя они сопровождают каждый новый шаг человечества в интернете. Пользователи накапливают опыт, специалисты по информационной безопасности находят приемлемые способы защиты. Не помешают вирусы и пользоваться социальными сетями — не отвадили же они нас от электронной почты и интернет-пейджеров. ■

> DDOS В СОЦСЕТЯХ

В сентябре 2007 года ученые из греческого Института компьютерных наук продемонстрировали новый способ проведения DDoS-атак. В этом методе используются взломанные программы для социальных сетей (например, программа для Facebook под названием Super Wall). Испытания показали, что даже небольшая аудитория размером в 1 тыс. компьютеров способна остановить работу средней руки веб-сайта. При этом утилитой Super Wall, к примеру, пользуются около 20 млн человек.

В середине 2007 года итальянский исследователь Розарио Валотта опубликовал концепцию Nduja Connection. Согласно концепции, вредоносные программы способны распространяться сразу в нескольких социальных сетях. Специалисты по безопасности пришли к выводу, что практическая реализация такой угрозы способна привести к крупнейшей в истории интернета эпидемии.

АУДИТОРИЯ САМЫХ ПОПУЛЯРНЫХ СОЦИАЛЬНЫХ СЕТЕЙ

НАЗВАНИЕ СЕТИ	КОЛИЧЕСТВО ПОСЕТИТЕЛЕЙ (ТЫС. ЧЕЛ.)		ИЗМЕНЕНИЕ
	ИЮНЬ 2007 ГОДА	ИЮНЬ 2008 ГОДА	
FACEBOOK.COM	52,167	132,105	153%
MYSPACE.COM	114,147	117,582	3%
HI5.COM	28,174	56,367	100%
FRIENDSTER.COM	24,675	37,08	50%
ORKUT	24,12	34,028	41%
BEBO.COM	18,2	24,017	32%
SKYROCK NETWORK	17,638	21,041	19%
ВСЕГО	464,437	580,51	25%

ИСТОЧНИК: COMSCORE.