Помогите, вирус на сайте!

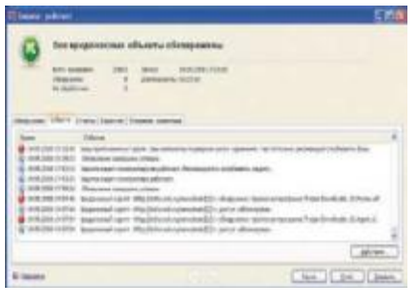
Стоило месяц назад разозлиться на медлительность «Касперского» и отключить его совсем, как на моем собственном сайте появились сразу два «новомодных» вируса: Trojan-Downloader.JS.Psyme.aml и Trojan-Clicker.HTML.IFrame.ey. Повезло еще, что случайный посетитель с антивирусным пакетом сразу заметил заразу и предупредил о ней

Анна Нартова,Алексей Набережный

Пока информационные порталы вроде веб-сайта радиостанции «Эхо Москвы» будут иметь завирусованные разделы, владельцам домашних страниц и любительских сайтов надо быть начеку.

Трояны поразили рабочий ПК сквозь очередную дыру в браузере Internet Explorer, когда в нем был открыт какой-то инфицированный сайт (вероятно, http://echo.msk.ru). Алгоритм вируса, встроенного в страницу зараженного веб-проекта, записал на клиентской машине с ОС Windows XP SP3 в папку Temporary Internet Files специальный Java-код, который еще и «прописался» на автозапуск в Реестре. После очередной перезагрузки компьютера вредоносная программа просканировала содержимое менеджера паролей FTP-клиента и взяла оттуда данные авторизации для соединения. Непростая ситуация получается с паролями: поставишь простое слово — хакеры смогут его подобрать, задашь сложное сочетание символов — придется хранить его в менеджере.

Далее вирус самостоятельно открыл FTP-сессию, получил на сервере листинг всех файлов и перезаписал ключевые файлы. Интересен критерий отбора: заражаются любые файлы, имеющие в названии слово index, например index.php, learn_course_index.php, helpindex.html и т. п. К тому же пострадали и другие важные файлы: component.php, header.php и footer.php.



В выбранных файлах на последних строках вредоносная программа вписала лишние теги <script> и </script>, а между ними — нелепую комбинацию знаков. Это дополнение сформировало html-элемент iframe, вызывающий вредоносный код со специального сервера-рассадника. Разумеется, неискушенные посетители становятся жертвами злого умысла, и если с их компьютеров управляются личные сайты по протоколу FTP, то эпидемия распространяется дальше.

Что делать? Сложно дать исчерпывающий ответ на такой вопрос, поскольку со временем появляются все новые и новые модификации вируса: механизм заражения и функционирования постоянно совершенствуется. Не исключено, что скоро следует ожидать варианты вредоносных алгоритмов, перехватывающих нажатия клавиш на пользовательских ПК и заражающих php-движки сайтов. Но пока есть пара правил, которая выручит владельцев сайтов в большинстве случаев. Во-первых, не храните даже сложные автопароли в FTP-менеджерах — лучше приклейте стикер с комбинацией символов к монитору. Во-вторых, установите надежную антивирусную программу. Например, возьмите с «Мир ПК-диска» «Антивирус Касперского 2009» и пользуйтесь им абсолютно бесплатно, ведь с каждым номером журнала мы даем читателям лицензионные ключи.

А что делать, если ваш сайт уже поражен? Мы поможем вам ответить на этот вопрос, поделившись своим опытом исцеления сайта с установленной CMS «1С:Битрикс» (Content Management System — система управления содержанием). Перво-наперво, поменяйте пароль на FTP-доступ через панель управления хостингом. Зайдите на сервер, чтобы изучить содержание таких ключевых страниц, как index.php или index.htm. Помните, в FTP-панели зараженные файлы выделяются большим размером и свежей датой модификации. Внутри html-кода удаляйте вирусные теги <script>...</script>, они располагаются либо в самом начале файла, либо в самом конце. Но встречаются и более хитрые варианты:– смотрите сразу после открывающего тега <body>. Таким образом, вы сделаете первые шаги к выздоровлению.

Если веб-сайт содержит сотни страниц, будет разумным заархивировать все содержимое в один файл и переписать его на локальный ПК. В системе «1С:Битрикс» есть удобная функция резервного копирования («Настройки»--«Резервное копирование»--«Архивировать»), после ее активации архив окажется в папке /bitrix/backup — перепишите его. Натравите «Антивирус Касперского» на архивный файл. Хотя обезвредить объект не получится, «Касперский» выдаст отчет, содержащий полный список пораженных страниц. Затем идите на сайт, чтобы избавиться от вирусных тегов в определившемся круге, и не забудьте удалить созданный ранее архив. Публичная часть сайта исцелена.

Теперь, необязательная часть работы по восстановлению ядра установленной CMS «1С:Битрикс» — расчет на вирусы будущего. Установите самые свежие обновления CMS («Настройки»-«Обновления»-«Установить рекомендуемые обновления»). Зайдите в файл include.php из папки /bitrix/modules/main и после первой строки «<?» вставьте свою «define('ENCODE','Y');». В знакомой вам вкладке «Настройки»—«Обновления» появится новая кнопка «Загрузить исходные тексты», — нажмите ее. В результате выполненных действий ядро продукта будет восстановлено, однако на вашем компьютере осталась клиентская часть вируса.

Если у вас несколько ПК с FTP-подключением к сайту, придется запрашивать лог-файлы у хостинг-провайдера и вычислять зараженный компьютер по дате и времени вирусных модификаций на сервере. По пути получите много дополнительной информации о напасти.

Как только определитесь с пораженным терминалом, приготовьтесь к заключительному этапу противостояния под кодовым названием «format c:» — шутка, но очень полезная. Дело в том, что «Антивирус Касперского» легко выявляет зараженные html-страницы, но когда дело касается исполнительного кода в пораженной системе, он спасает не всегда. Придется анализировать элементы автозагрузки в настройках системы. Нажмите кнопки «Windows»+R, в командной строке введите msconfig, откройте вкладку «Автозагрузка» и внимательно изучите ее содержимое — там спрятан след вируса. Отключите все подозрительные автозапуски, перегрузите систему и впредь в закладке «Общие» останавливайтесь на варианте «Выборочный запуск». Вот вроде бы и все. И на этот раз пронесло!

20.03.2009г.