УРОКИ ДОКТОРА ВЕБА

ПРОЛОГ

В конце минувшего года редакционные компьютеры подверглись вирусной атаке. Нельзя сказать, что подобное случилось впервые, однако бедствий такого масштаба ранее не было. Первой жертвой стали самые эксплуатируемые, уязвимые и незащищенные — компьютеры бюро набора текстов. Результат — безвозвратно утеряны несколько тысяч файлов, в том числе почти все свежие материалы очередного номера журнала "Радио".

После приличествующих случаю стенаний и проклятий неизвестному врагу к работе приступила срочно созданная бригада спасателей. Из имеющихся в редакции антивирусов имя злодея назвал только один — приобретенный в "ДиалогНауке" Doctor Web. Злоумышленником оказался не самый новый, но зато один из наиболее массовых макровирусов — WM.Cap, написанный еще в 1996 г. 15-летним венесуэльским мальчиком. Прятался он не в исполняемых файлах, к чему все привыкли, а в текстовых, формата Word for Windows. Специфика же редакционной кухни такова, что простои недопустимы, основная информация содержится именно в текстовых файлах, и они беспрерывно циркулируют по компьютерам, а вместе с ними — и незваный венесуэлец. Одним словом, более благодатного места для размножения и подрывной работы WM.Cap, наверное, найти не смог.

И развернулось сражение. Doctor Web и редакция, с одной стороны, а с другой — WM.Cap и компьютеры с их винчестерами и дискетами, ставшие невольными пособниками врага. Попутно заметим (может, кому пригодится), что рекомендованные зарубежными и отечественными "вирусологами" методы борьбы со злодеем к требуемому результату не привели. Все советы специалистов по борьбе с вирусами сводились к простому лечению зараженных файлов и шаблонов Word, в крайнем случае, к уничтожению (стиранию) шаблона Normal.dot (при очередном запуске редактора он автоматически восстанавливается со значениями по умолчанию). Ничего другого не предлагалось. А в некоторых рекомендациях (см., например, http://virus.komi.ru/wmcap.htm) в ответ на вопрос о целесообразности переустановки редактора Word (что в общем-то напрашивается) прямо говорится: "Переустанавливать Word ни в коем случае не надо".

Опуская подробности, скажем, что практика (а она, как-никак, критерий истины) эту рекомендацию отвергла. До тех пор, пока лечение зараженных файлов не было дополнено искоренением, а затем новой установкой Word, истребить вездесущий WM.Cap нам не удалось. Казалось, окончательно и бесповоротно истребленный вирус после более или менее продолжительного молчания вновь проявлял себя, и ... все начиналось сначала.

В этой тяжелой борьбе, растянувшейся более чем на месяц, с самой лучшей стороны показал себя Doctor Web. Размышляя в перерывах между "боями" о превратностях компьютерного прогресса, мы вспомнили о статье "Антивирусная система Spider's Web" ("Радио", 1994, № 1, с. 21, 22), в которой рассказывалось и о вирусах, и об антивирусном пакете Spider's Web, предшественнике Doctor Web, и о его авторе Игоре Анатольевиче Данилове. Невольно возникла идея вернуться к этой публикации, посмотреть, что

нового в антивирусном мире, побеседовать с И. Даниловым, рассказать о его творческих планах и т. д.

НЕМНОГО О ВИРУСАХ И АНТИВИРУСНЫХ ПРОГРАММАХ

Вообще говоря, за прошедшие со времени публикации четыре года в принципиальном плане мало что изменилось. Компьютеры становятся все сложнее, используются все более совершенные технологии, как аппаратные, так и программные. Число вирусов, увы, не убавилось, а "вредность" их растет вместе с совершенствованием антивирусов, иногда опережая их, иногда отставая. Возбудители компьютерных заболеваний "научились" заражать загрузочные сектора дисков, файлы всех операционных систем, умело "прятаться", стали мутантами (полиморфными).

Появились новые разновидности, например, макровирусы, к которым принадлежит и WM.Cap. Впервые макровирусы, атакующие файлы в формате Word for Windows, были обнаружены летом 1996 г. и наделали немало шума, так как, на первый взгляд, своим поведением опровергали устоявшиеся представления о вирусах. Оказалось, что необычность их нрава связана с тем, что они, а точнее их создатели, очень умело использовали возможности встроенного в редактор Word for Windows макроязыка и языка программирования Word Basic. Высокая совместимость последнего с основными языками программирования, наличие средств работы с файлами обеспечили "вирусописателям" благоприятную возможность для создания высокоэффективных, труднообнаруживаемых инфицирующих программ, распространяющихся с очень высокой скоростью.

Появились вирусы и для других программ, использующих макрокоманды, например, для Excell, Ami Pro и др. Есть и такие, которые разрушают информацию, уничтожают файлы и т. д. Макровирусы работают независимо от платформы, т. е. инфицирующая программа, написанная для MACINTOSH, действует и на IBM PC, и на других компьютерах. Подробнее об этих вирусах, их свойствах и особенностях можно узнать, ознакомившись со статьей В. Лутовинова, коллеги И. Данилова (см., например, http://www.admiral.ru/~sald/artic3_w.html).

Совсем недавно появился еще один новый возбудитель, который по принципу действия можно назвать "вирусом защищенного режима". До недавнего времени вирусам, а точнее их создателям, не удавалось использовать для своих грязных целей защищенный (виртуальный) режим современных процессоров. Первенец, нареченный PM.Wanderer, использует этот режим, причем корректно взаимодействует с другими программами и драйверами, также использующими его. В перспективе не исключено, что вирус сможет полностью заменить своим кодом программу-супервайзора (см., например, http://www.dials.ccas.ru/russian/inf/wanderer.htm).

Развиваются и "обычные" вирусы. Они успешно маскируются, мутируют, одним словом, делают все возможное, чтобы продолжать творить свое черное дело.

А что же антивирусы? Тоже совершенствуются, и весьма успешно. Особенно приятно, что в число лучших антивирусных программ мира в последние годы неизменно входят и российские, в первую очередь, Doctor Web АО "ДиалогНаука" (DialogueScience DrWeb) и AntiViral Toolkit Pro фирмы "Лаборатория Касперского" (KAMI AVP). Так, в июльском (1997 г.) номере известного международного журнала "Virus Bulletin" (см. в Интернет на сайте http://www.virusbtn.com) опубликованы результаты очередного сравнительного тестирования антивирусов-сканеров, работающих под операционной системой MS DOS. По результатам испытаний Doctor Web вошел в тройку лучших антивирусов мира (табл. 1): вместе с Sophos SWEEP он показал 100-процентную эффективность в самой престижной категории — по степени обнаружения полиморфных вирусов — и разделил с ней первое—второе места. С результатом 99,5 % Doctor Web разделил второе—третье места с программой McAfee VirusScan в наиболее актуальной категории — обнаружении макровирусов. По довольно условному усредненному показателю обнаружения вирусов для рассматриваемых категорий тестов Doctor Web занял третье место, пакет KAMI AVP E. Касперского — почетное восьмое.

Очередное тестирование антивирусных программ журнал "Virus Bulletin" провел в феврале 1998 г. (табл. 2). И вновь среди лучших — Doctor Web! Он показал абсолютный результат (100-процентное обнаружение!) в двух наиболее важных категориях: по степени выявления сложных полиморфных и макровирусов. Особо стоит отметить, что по первой из них такой результат отмечается в третий раз подряд. Если вновь попытаться ввести некий усредненный показатель (что-то вроде командных результатов на спортивных соревнованиях), то Doctor Web окажется на восьмом месте (табл. 3).

Отметим, что KAMI AVP E. Касперского по этому показателю занимает шестое место, показав абсолютный результат в пяти(!) категориях из шести. И это не единственный успех E. Касперского. В конце прошедшего года журнал по компьютерной безопасности "Secure Computing" провел тестирование антивирусных продуктов для Windows 95, и оказалось, что почти по всем показателям