

Dr.Web не был установлен на компьютере. Но помог обнаружить вирусы на нем!

И в этом нет ничего фантастического. Ведь речь идет об интернет-сервисе Dr.Web AV-Desk, чьи средства позволяют удаленно наблюдать за вирусной обстановкой в сети, в которой антивирусом Dr.Web оснащены хотя бы несколько компьютеров.

Этот случай произошел в одной из средних школ города Бердска, участвующей в программе по бесплатному подключению к услуге «Антивирус Dr.Web» школ Новосибирской области. В рамках этой программы в школах региона проходит внедрение интернет-сервиса **Dr.Web AV-Desk**, позволяющего установить на школьных компьютерах средства антивирусной защиты с функцией Родительского контроля.

Все началось с того, что через консоль **Dr.Web AV-Desk** нашими специалистами была замечена резко возросшая вирусная активность в школьной сети. За три дня антивирусный монитор **SpIDer Guard** нейтрализовал порядка 400 экземпляров вредоносных программ. При ближайшем рассмотрении выяснилось, что они распространялись по сети с одного зараженного компьютера.

Специалисты «Доктор Веб» выехали на место происшествия. Компьютер – источник «заразы» оказался не защищен антивирусом и заражен сетевым червем Win32.HLLW.Shadow.based (известным также под именем Conficker). Исходящий паразитный трафик стремился заразить все компьютеры домена с целью превращения их в ботнет. Многие сайты, в том числе www.drweb.com и www.freedrweb.com с этого компьютера не открывались, что не позволяло скачать средство для лечения непосредственно с серверов «Доктор Веб».

Вирус распространялся по сети с правами администратора, так что **SpIDer Guard** мог «прибить» зараженные файлы только в момент попытки их выполнения на других компьютерах. Пароль администратора на незащищенном компьютере, в свою очередь, был скомпрометирован. Попытки его изменить ни к чему не привели – он тут же сбрасывался. Тогда специалисты «Доктор Веб» изменили алгоритм шифрования пароля в домене и задали более жесткие правила безопасности.

Когда мятежный компьютер был укрощен, оставалось раз и навсегда вылечить другие машины в сети. Для этой цели как нельзя лучше подошел новый продукт «Доктор Веб» – сетевая лечащая утилита **Dr.Web CureNet!**, позволяющая централизованно просканировать сеть и ликвидировать последствия заражения. Сканирование всех компьютеров и сервера в классе выявило 207 зараженных объектов. С «заразой» было покончено.

Таким образом, услуга «**Антивирус Dr.Web**» помогла выявить проблему на компьютере, который даже не был защищен ПО услуги. В другой ситуации эта проблема еще долгое время могла оставаться неразрешенной. Возможность централизованного наблюдения за вирусной активностью позволила быстро «напасть на след» вредоносной программы и в кратчайшие сроки ликвидировать ее. **Dr.Web CureNet!**, в свою очередь, помог закрепить успех, продемонстрировав свои возможности по лечению компьютеров и серверов в сети.

О компании «Доктор Веб»

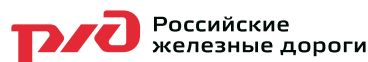
«Доктор Веб» – российский разработчик средств информационной безопасности и лидер российского рынка интернет-сервисов безопасности для провайдеров IT-услуг. «Доктор Веб» стала первой компанией, предложившей на российском рынке инновационную модель потребления антивируса в качестве услуги сервис-провайдеров.

Интернет-сервис Dr.Web AV-Desk создан специалистами компании «Доктор Веб» в 2007 году. На сегодняшний день установку Dr.Web AV-Desk осуществили более 100 провайдеров из более чем 30 регионов России, а также Украины, Казахстана, Киргизии, Болгарии и Эстонии. По итогам 2007 года Dr.Web AV-Desk был признан лучшим «продуктом-услугой» русской версией журнала PC Magazine. В сентябре 2008 года Dr.Web AV-Desk получил Большую Золотую Медаль «Сибирской ярмарки» в номинации «Оригинальное научно-техническое решение в технике связи».

Антивирусные продукты Dr.Web разрабатываются с 1992 года. Обширная география пользователей и многочисленные сертификаты и награды свидетельствуют о степени исключительного доверия к продуктам компании.

Опыт крупных проектов

Среди клиентов «Доктор Веб» – крупные компании с мировым именем, российские и международные банки, государственные организации, учебные заведения и научно-исследовательские институты, сети которых насчитывают десятки тысяч компьютеров. Антивирусным решениям «Доктор Веб» доверяют высшие органы государственной и исполнительной власти России, компании топливно-энергетического сектора.



Dr.Web является зарегистрированной торговой маркой ООО «Доктор Веб»



© ООО «Доктор Веб», 2003–2009

125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп. 12а

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

www.drweb.com

www.freedrweb.com

www.av-desk.com