

ЦТП "Доктор Веб"

В контакте с Trojan.Hosts.75

Компания «Доктор Веб» сообщает, что в начале июня 2009 года был обнаружен очередной троянец — Trojan.Hosts.75. Данная вредоносная программа принадлежит к семейству Trojan.Hosts и вымогает деньги у зараженных пользователей популярной социальной сети «ВКонтакте». На сегодняшний день насчитывается около сотни различных модификаций этого троянца.

Trojan.Hosts.75 перенаправляет пользователя на фишинговую страницу, оформленную в фирменном стиле социальной сети «ВКонтакте». Здесь, будто бы от лица администрации сайта, пользователю предлагается зарегистрироваться в системе при помощи SMS-активации. Объясняется это «нововведение» увеличением количества спам-рассылок.

После запуска Trojan.Hosts.75 вирус распаковывает на диск bat-файл, который, в свою очередь, модифицирует файл hosts. Прописав в файл hosts множество популярных интернет-ресурсов, киберпреступники попытались тем самым увеличить вероятность попадания жертвы на сайт вымогателей. При посещении с зараженного компьютера одного из ресурсов, указанных в модифицированном файле hosts, пользователь перенаправляется на фальшивую страницу на сервере <http://211.xx.xx.xx/index.html>.

В последнее время служба вирусного мониторинга компании «Доктор Веб» констатирует увеличение числа программ-вымогателей. Этот факт был отмечен и в нашем обзоре вирусной обстановки за май 2009 года (<http://news.drweb.com.ua/show/?i=281&c=9&p=0>).

Служба вирусного мониторинга «Доктор Веб» в очередной раз призывает пользователей не поддаваться на фишинговые провокации злоумышленников и не перечислять на их счета запрошенные суммы. Если заражение все же произошло, компания «Доктор Веб» рекомендует воспользоваться бесплатной лечащей утилитой Dr.Web CureIt! (<http://www.freedrweb.com/cureit/>). Для пользователей, защищенных антивирусными решениями Dr.Web, Trojan.Hosts.75 угрозы не представляет.

Контактная информация

Сергей Кравченко, PR- консультант ЦТП «Доктор Веб»

E-mail: sergey.kravchenko@drweb.com.ua