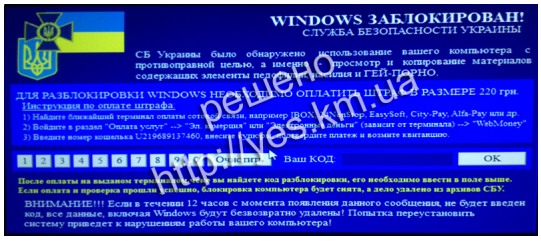
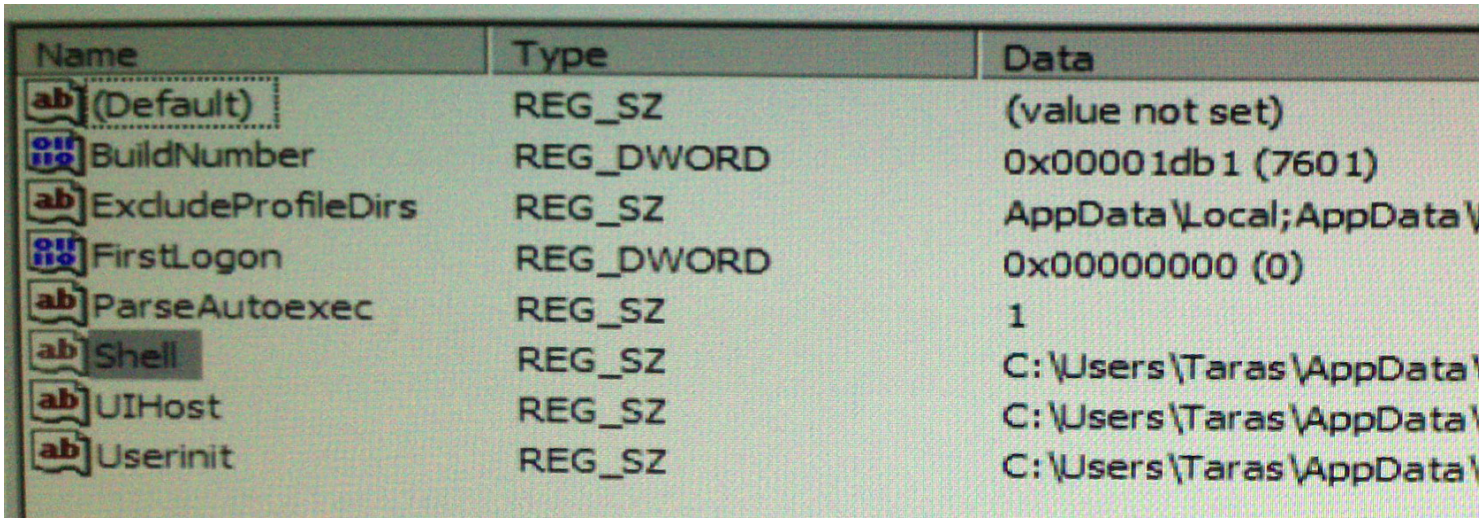
# Вирус-вымогатель. Пополнить кошелек U219689137460

Автор: Administrator
14.02.2013 16:54 -




Windows-блокер якобы от имени Службы Безопасности Украины сообщает о просмотре и копировании на Вашем компьютере порнографических видео-материалов. Через терминал предлагается пополнить кошелек WebMoney **U219689137460** на 220 грн. Вирус надежно прописывается в реестре:




Для удаления указанного вируса необходимо:

1. Загрузится с загрузочного диска.
2. Подключится к реестру установленной ОС.
3. Восстановить значения реестра на:
 [HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionWinlogon]
ключ "Shell"="Explorer.exe"

ключ "Userinit"="C:WINDOWSsystem32userinit.exe,"
ключ "UIHost"="logonui.exe"
4. Файловым менеджером очистить папку Temp.

После перезагрузки ОС не подключаясь к интернету полностью деинсталировать браузер, который использовался последним и установить его заново. (В нашем случае это была Opera. И несмотря на то, что был почищен кеш и закрыты закладки при следующей работе в браузере вирус подгружался снова. Возможно, он прописывался в плагины).