

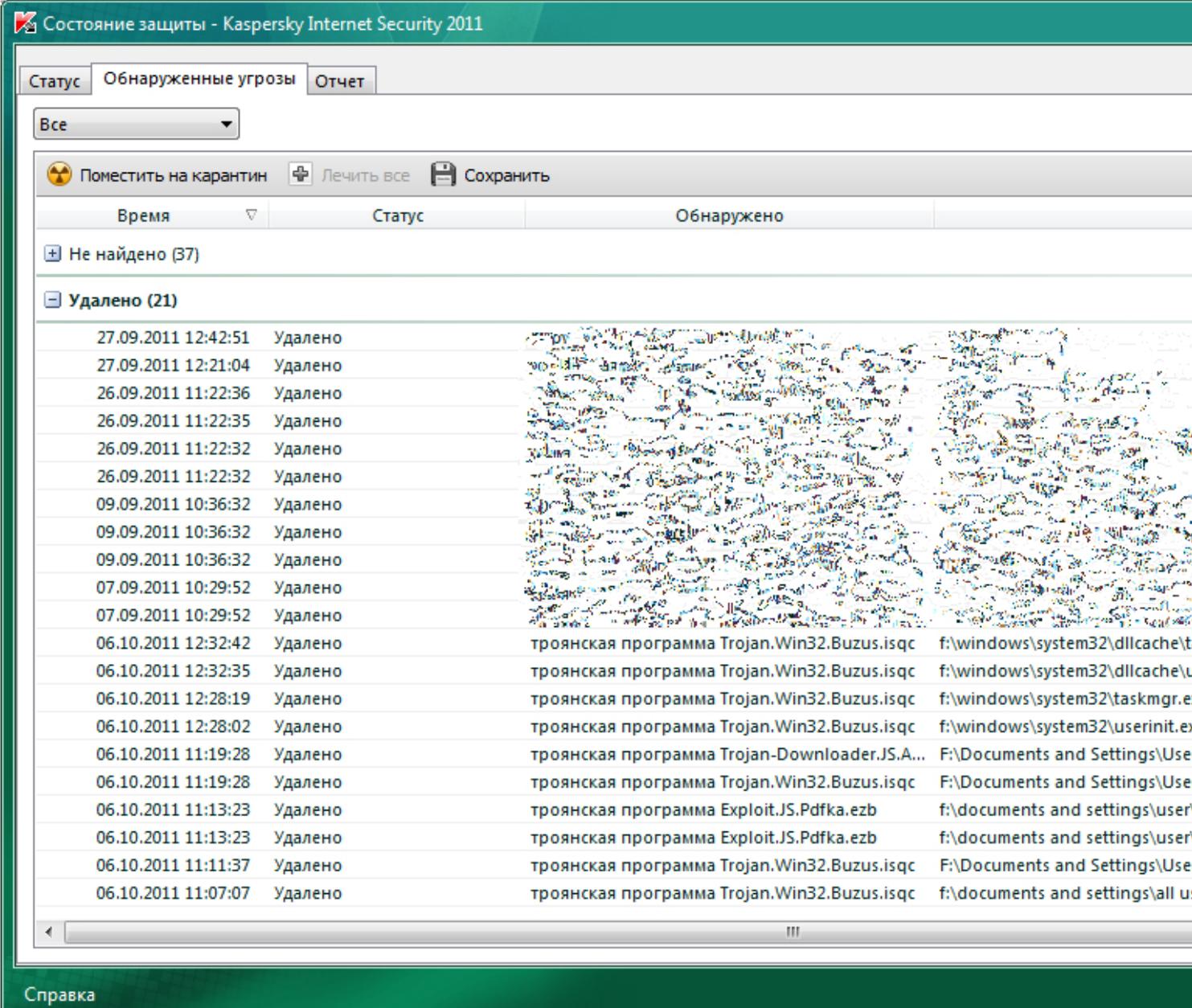
## Windows заблокирован. Пополнение счета webmoney

Автор: Administrator

06.10.2011 13:35 - Обновлено 31.10.2012 17:10

Очередной **блокер-вымогатель**. Проблема: после старта **Windows** XP всплывает баннер с требованием оплатить разблокировку.

Решение проблемы. Подключаем HDD к другому компьютеру с установленным KIS2011. Делаем проверку диска. Получаем результат:



The screenshot shows the 'Состояние защиты - Kaspersky Internet Security 2011' window. The 'Обнаруженные угрозы' (Detected threats) tab is active. A dropdown menu is set to 'Все' (All). Below the menu are buttons for 'Поместить на карантин' (Quarantine), 'Лечить все' (Treat all), and 'Сохранить' (Save). The main area displays a table of detected threats. The first row shows 'Не найдено (37)' (Not found (37)). The second row shows 'Удалено (21)' (Deleted (21)). The table lists 21 deleted threats with columns for 'Время' (Time), 'Статус' (Status), and 'Обнаружено' (Detected). The 'Обнаружено' column contains two columns of text, likely representing the threat name and the file path.

Время	Статус	Обнаружено
+ Не найдено (37)		
- Удалено (21)		
27.09.2011 12:42:51	Удалено	
27.09.2011 12:21:04	Удалено	
26.09.2011 11:22:36	Удалено	
26.09.2011 11:22:35	Удалено	
26.09.2011 11:22:32	Удалено	
26.09.2011 11:22:32	Удалено	
09.09.2011 10:36:32	Удалено	
09.09.2011 10:36:32	Удалено	
09.09.2011 10:36:32	Удалено	
07.09.2011 10:29:52	Удалено	
07.09.2011 10:29:52	Удалено	
06.10.2011 12:32:42	Удалено	тройная программа Trojan.Win32.Buzus.isqc f:\windows\system32\dllcache\t
06.10.2011 12:32:35	Удалено	тройная программа Trojan.Win32.Buzus.isqc f:\windows\system32\dllcache\U
06.10.2011 12:28:19	Удалено	тройная программа Trojan.Win32.Buzus.isqc f:\windows\system32\taskmgr.e
06.10.2011 12:28:02	Удалено	тройная программа Trojan.Win32.Buzus.isqc f:\windows\system32\userinit.ex
06.10.2011 11:19:28	Удалено	тройная программа Trojan-Downloader.JS.A... F:\Documents and Settings\User
06.10.2011 11:19:28	Удалено	тройная программа Trojan.Win32.Buzus.isqc F:\Documents and Settings\User
06.10.2011 11:13:23	Удалено	тройная программа Exploit.JS.Pdfka.ezb f:\documents and settings\user
06.10.2011 11:13:23	Удалено	тройная программа Exploit.JS.Pdfka.ezb f:\documents and settings\user
06.10.2011 11:11:37	Удалено	тройная программа Trojan.Win32.Buzus.isqc F:\Documents and Settings\User
06.10.2011 11:07:07	Удалено	тройная программа Trojan.Win32.Buzus.isqc f:\documents and settings\all u

Справка

## Windows заблокирован. Пополнение счета webmoney

Автор: Administrator

06.10.2011 13:35 - Обновлено 31.10.2012 17:10

---

Касперский идентифицирует системные файлы **taskmgr.exe** и **userinit.exe** как троянские программы

**Buzus.isqc**

а так же файлы

**wpbt0.dll**

и

**22co6c32.exe**

и удаляет их. Просмотрев лог можно предположить, что пользователь загрузил файл

**calc[1].exe**

, который создал файл со случайным именем

**22co6c32.exe**

и изменил системные файлы.

После проведенной процедуры запускаем Windows на вылеченном компьютере. Винда доходит до окна выбора пользователя. При попытке войти в учетную запись любого пользователя система завершает его сеанс. Это понятно - у нас не хватает системных файлов. Мы их подкидываем с рабочей копии винды. В реестре HKEY\_LOCAL\_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionWinlogon исправляем Shell (который был изменен зловредом на **22co6c32.exe**).

[Скачать &nbsp; taskmgr.exe&nbsp; userinit.exe](#)

Список статей: [Разблокировать Windows](#)