# СКРЫТЫЕ СЛУЖБЫ WINDOWS

*П. Г. Шаламов*
(Курган, КГУ, nekkuro1@gmail.com)

Службы Windows (Windows Service) – это особый класс приложений, запускающийся автоматически при запуске системы и не зависящий от статуса пользователя. Как правило, службы не имеют GUI, вследствие чего их обычная работа не заметна для пользователя.

При стандартной установке Windows XP в систему инсталлируется порядка 80 разнообразных служб. Нередко вместе с установкой стороннего программного обеспечения устанавливаются и дополнительные службы.

Важно отметить, что по умолчанию службы запускаются от имени пользователя «LocalSystem». Этот пользователь обладает полными правами внутри системы, его права превосходят даже учетную запись «Administrator».

При таких условиях работы службы являются отличным местом для хранения и сокрытия вредоносного кода. Ситуацию облегчает лишь то, что список служб не является скрытым и легко просматривается стандартными средствами системы (рис. 1).

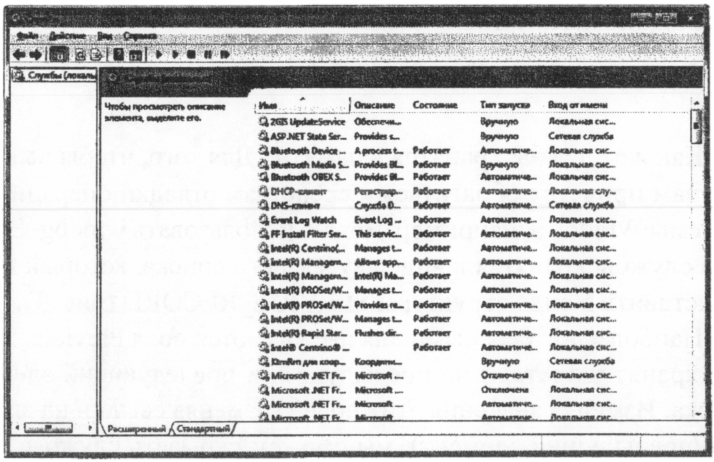


Рис. 1. Список служб

Однако что произойдет, если скрыть службу? Для начала стоит разобраться, возможно ли это сделать в принципе, и как вообще службы хранятся в системе?

Можно выделить два места хранения служб: реестр и ядро. Найти службы в реестре несложно, все они хранятся в ветке «HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services» (рис. 2). Реестр представляет такие же возможности работы со службами, как и стандартные утилиты Windows (например, services.msc), а значит, не позволит нам скрыть службу или обнаружить скрытую.

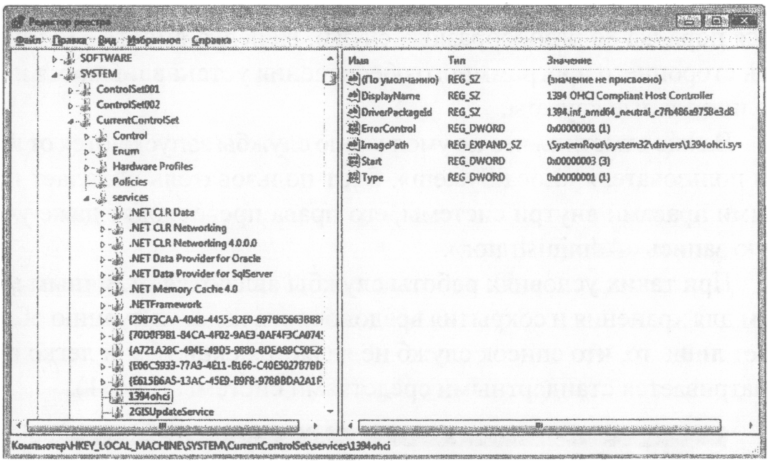


Рис. 2. Службы в реестре

Как же службы хранятся в памяти? Для того, чтобы выяснить это, нам придется обратиться к средствам отладки операционной системы Windows, например, можно использовать windbg. Внутри ядра службы хранятся в виде двусвязного списка, который можно представить в виде структуры SERVICE_RECORD (рис. 3).

Наиболее интересными для нас являются поля Previous, Next – они хранят указатели на предыдущий и последующий элементы списка. Изменяя значения этих полей (изменяя ссылки на следующий/предыдущий элемент), мы сможем скрывать службы, а впоследствии, зная размер этой структуры, искать скрытые службы.

```
typedef struct _SC_SERVICE_RECORD
{
    PSC_SERVICE_RECORD Previous;
    PSC_SERVICE_RECORD Next;
    WCHAR *ServiceName;
    WCHAR *DisplayName;
    DWORD Index;
    DWORD Unknow0;
    DWORD sErv;
    DWORD ControlCount;
    DWORD Unknow1;
    PSC_SERVICE_PROCESS Process;
    SERVICE_STATUS Status;
    DWORD StartType;
    DWORD ErrorControl;
    DWORD TagId;
    PSC_DEPEND_SERVICE DependOn;
    PSC_DEPEND_SERVICE Depended;
}
```

Рис. 3. Описание структуры SERVICE_RECORD

Допустим, мы хотим скрыть службу с номером (в списке) N, для этого нам надо у службы с номером N – 1 в поле Next поставить ссылку на службу с номером N + 1, а у N + 1 аналогичным образом изменить поле Previous. Для нахождения скрытой службы достаточно идти от начала списка и отслеживать значение указателя там, где значение превышает размер структуры, явно прослеживаются изменения списка.

Чтобы не выполнять подобные операции каждый раз в ядре, можно разработать программу. Алгоритм ее работы будет следующий:

1. Найти ID процесса «services.exe».
2. Перейти в рабочее пространство процесса «services.exe».
3. По метке «sErv» найти начало списка служб.
4. Пройти по списку, ища скрытые службы.
5. Сигнализировать о найденных службах.

Данный алгоритм позволяет без труда как скрывать службы, так и обнаруживать ранее скрытые, что может в некоторых случаях существенно повысить надежность системы.