ОНЛАЙН-ОБРАЗОВАНИЕ

# Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

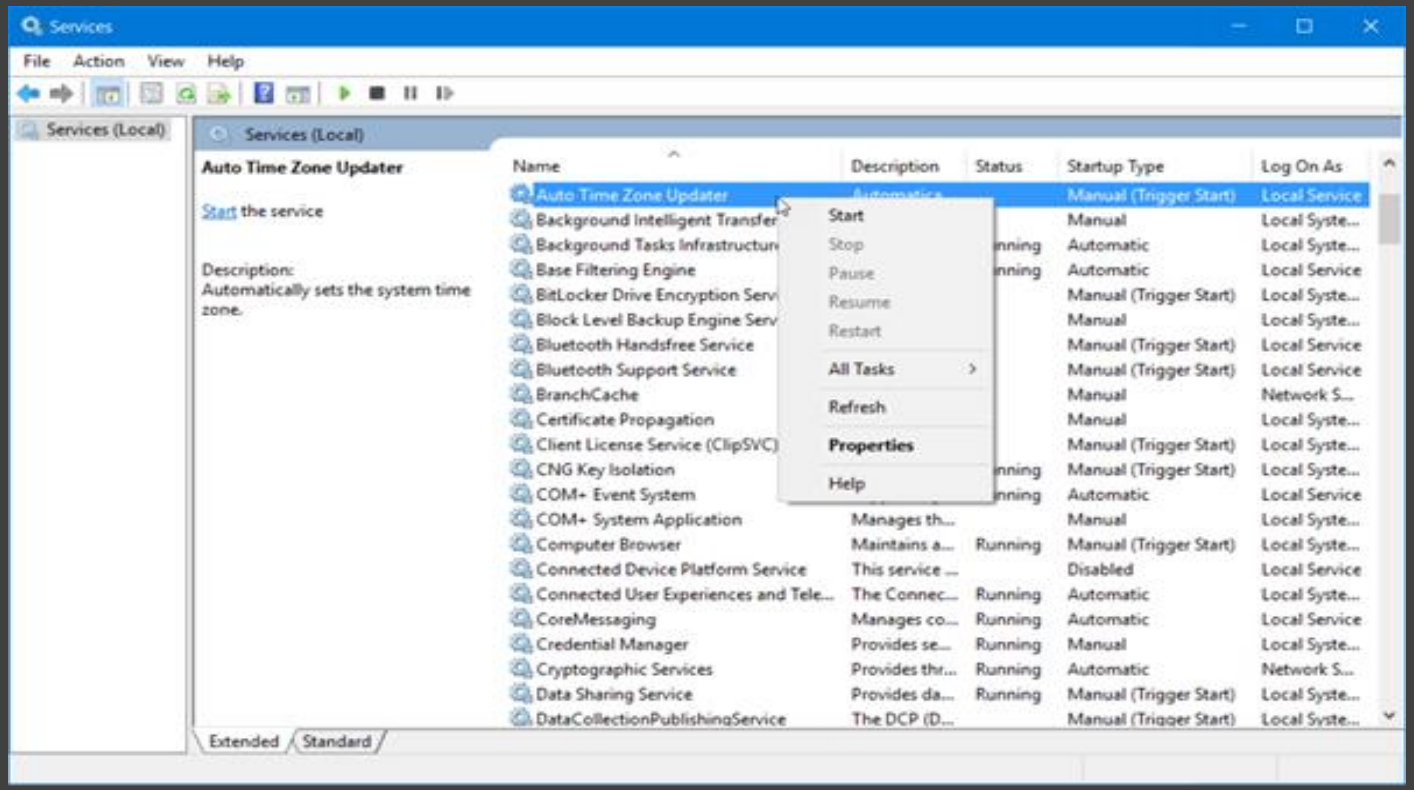
OTUS

# Программирование служб

Пакулов Артур

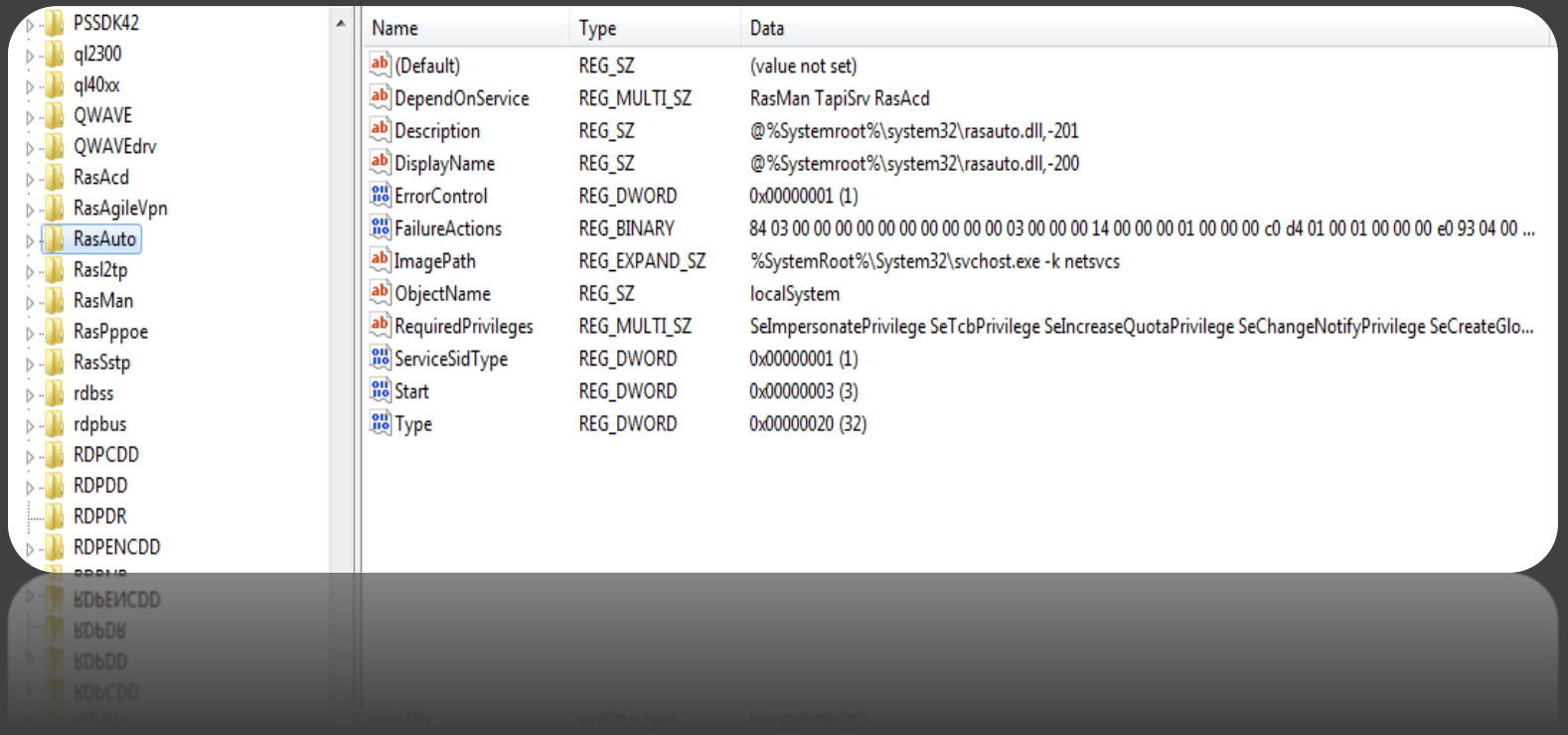
# Что такое службы?

Службы (Services) - это процессы пользовательского режима, для запуска и функционирования которых, регистрация интерактивного пользователя в системе не требуется



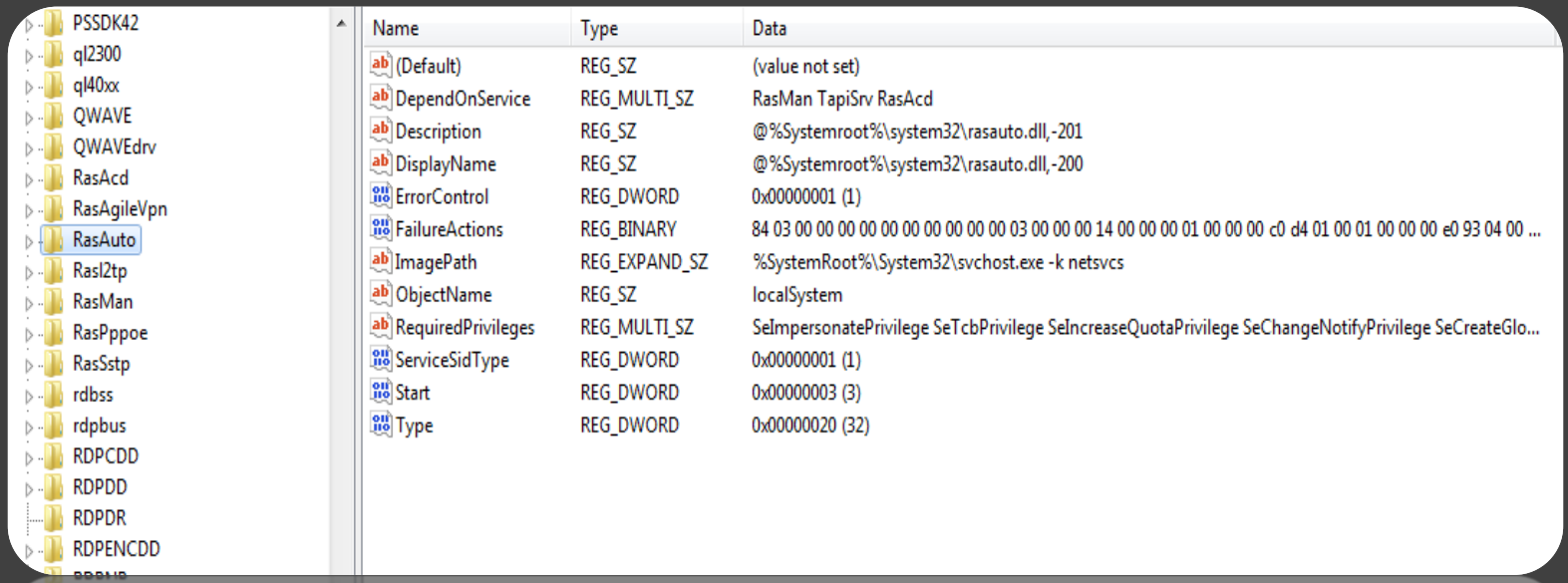
# База данных служб

Вся информация о службах хранится в реестре по адресу HKLM\System\CurrentControlSet\Services



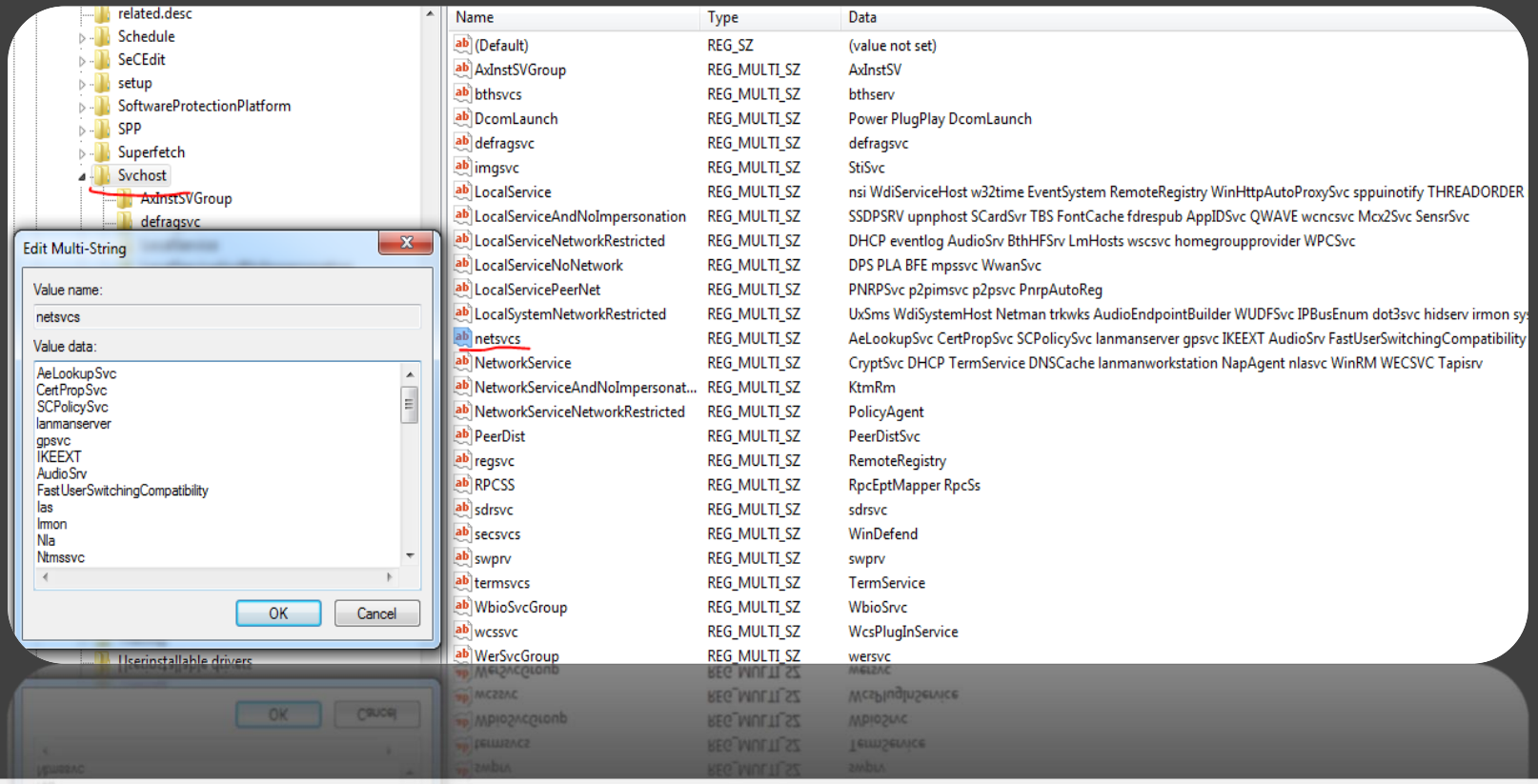
# База данных служб

Значение imagePath:
%SystemRoot%\System32\svchost.exe -k netsvcs
говорит, что службы из группы netsvcs нужно загрузить в контексте процесса svchost.exe



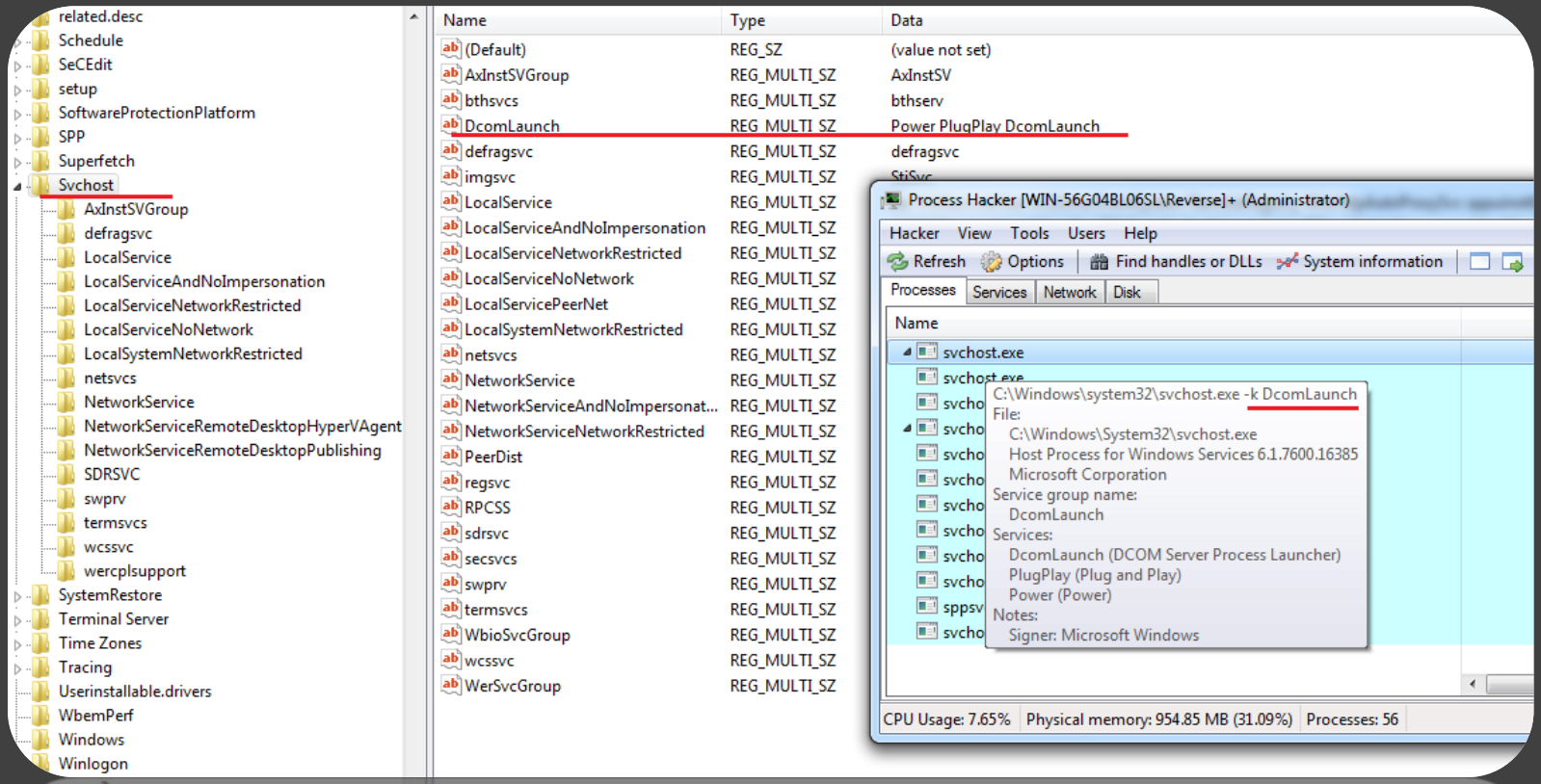
# База данных служб

Информация о группах тут:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\SvcHost



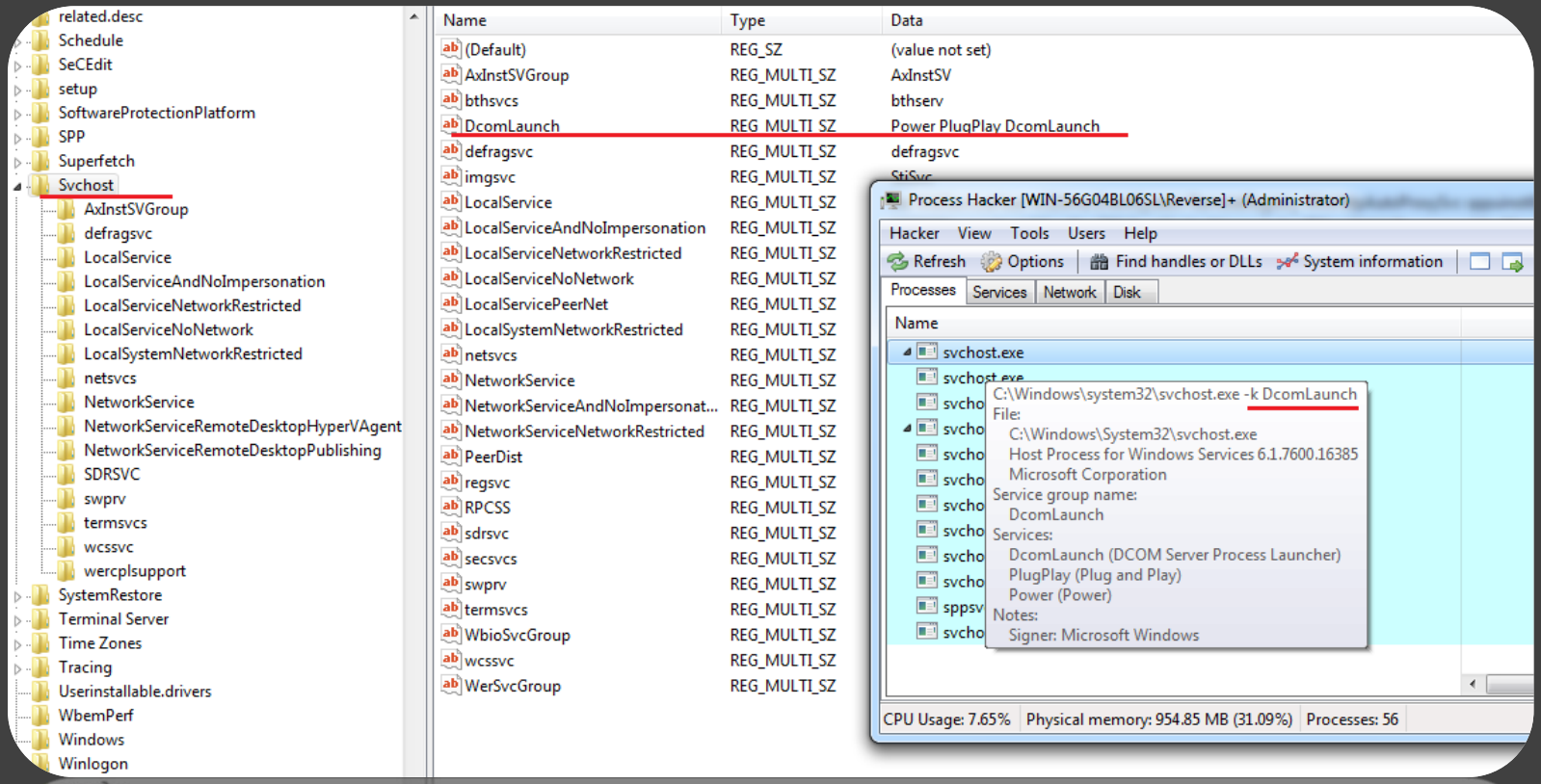
# Процесс svchost

Каждая группа загружается в контексте отдельного процесса svchost.exe



# Процесс svchost

Внимание!
Легитимный svchost.exe всегда является дочерним процессом services.exe



2

# Пример

# Регистрируем службу в реестре

Создаём ключ с именем службы тут:

HKLM\SYSTEM\CurrentControlSet\Services\SvcHostDemo

```
wsprintf(szRegPath, L"SYSTEM\\CurrentControlSet\\Services\\%s", szServiceName);
wsprintf(szServiceDll, L"%%SystemRoot%%\\system32\\%s", dllName);
```

```
if (RegCreateKey(HKEY_LOCAL_MACHINE, szRegPath, &hKey) == ERROR_SUCCESS)
{
    RegSetValueEx(hKey, L"Description", 0, REG_SZ, (BYTE*)szDescription, lstrlen(szDescription));
    if (RegCreateKey(hKey, L"Parameters", &hParKey) == ERROR_SUCCESS)
    {
        if (RegSetValueEx(hParKey, L"ServiceDll", 0, REG_EXPAND_SZ, (BYTE*)szServiceDll, lstrlen(szServiceDll)*2) == ERROR_SUCCESS)
            result = TRUE;
        RegCloseKey(hParKey);
    }
    RegCloseKey(hKey);
}
return result;
```

# Регистрируем службу в реестре

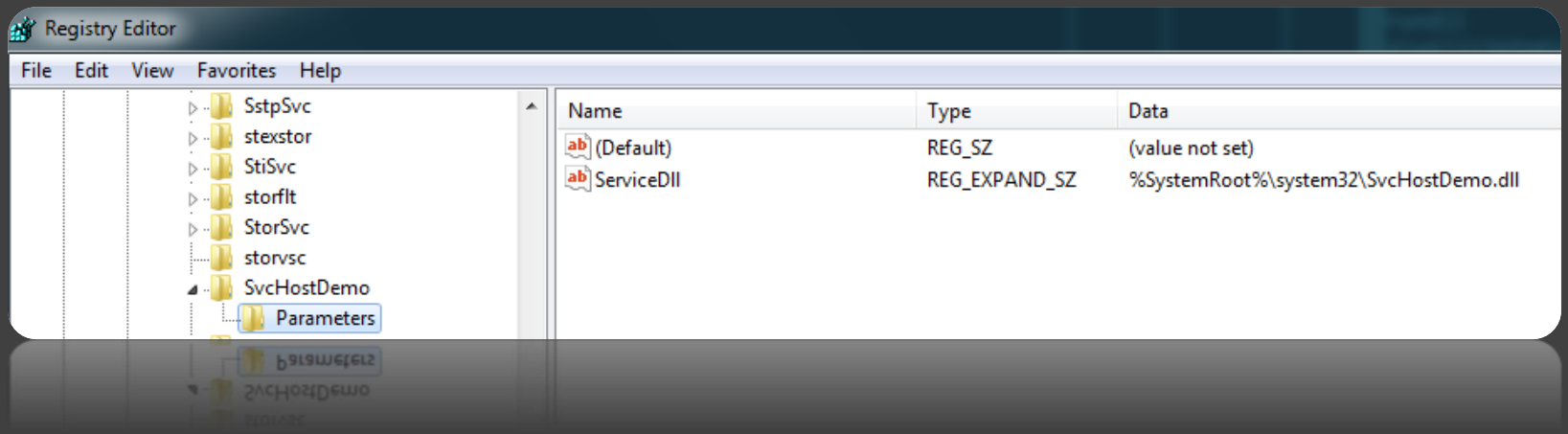
Затем создаём параметр «Description» и подключ «Parameters» с значением «ServiceDll»

```
wsprintf(szRegPath, L"SYSTEM\\CurrentControlSet\\Services\\%s", szServiceName);
wsprintf(szServiceDll, L"%%SystemRoot%%\\system32\\%s", dllName);
```

```
if (RegCreateKey(HKEY_LOCAL_MACHINE, szRegPath, &hKey) == ERROR_SUCCESS)
{
    RegSetValueEx(hKey, L"Description", 0, REG_SZ, (BYTE*)szDescription, lstrlen(szDescription));
    if (RegCreateKey(hKey, L"Parameters", &hParKey) == ERROR_SUCCESS)
    {
        if (RegSetValueEx(hParKey, L"ServiceDll", 0, REG_EXPAND_SZ, (BYTE*)szServiceDll, lstrlen(szServiceDll)*2) == ERROR_SUCCESS)
            result = TRUE;
        RegCloseKey(hParKey);
    }
    RegCloseKey(hKey);
}
return result;
```

# Регестрируем службу в реестре

Затем создаём параметр «Description» и подключ «Parameters» с значением «ServiceDll»



# Регистрируем службу в реестре

OTUS

Добавляем нашу службу в группу netsvcs

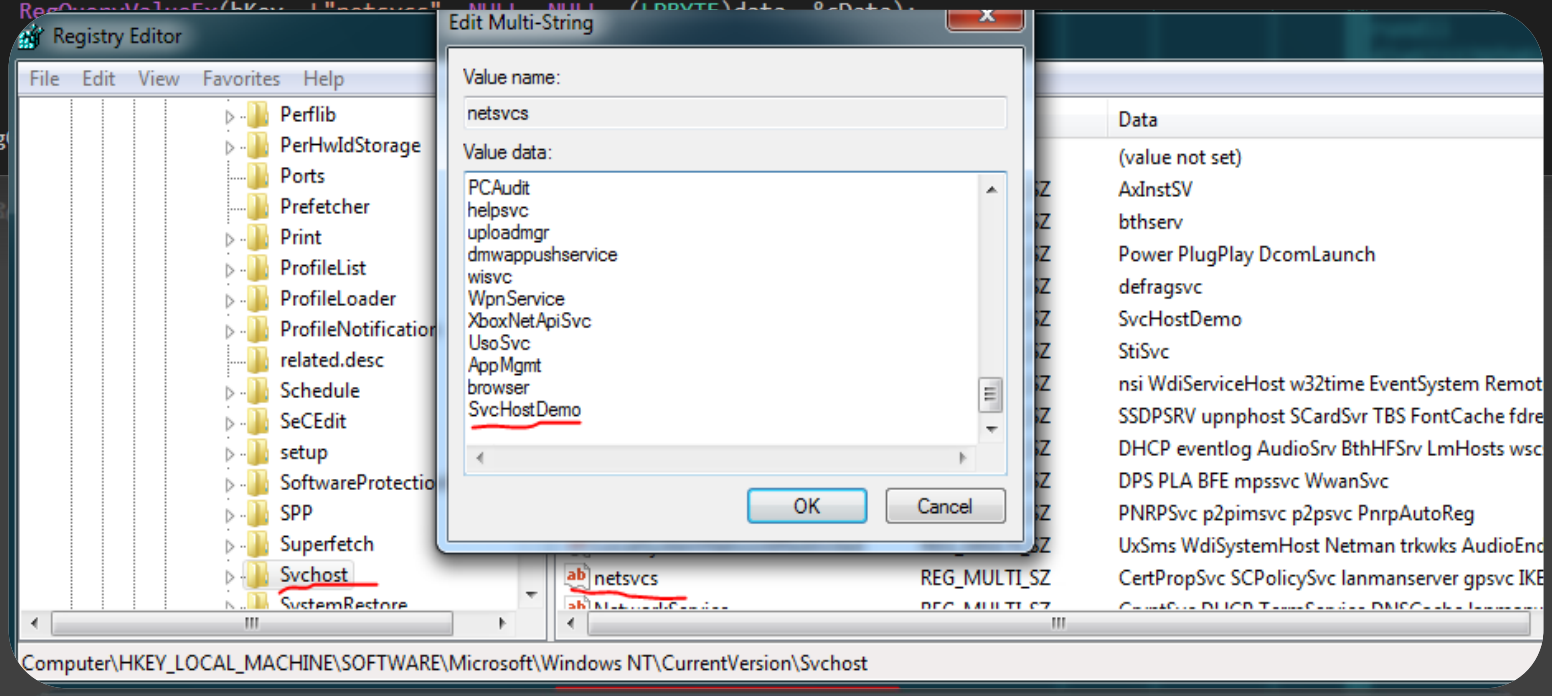
```
wsprintf(szRegPath, L"SYSTEM\\CurrentControlSet\\Services\\%s", szServiceName);
wsprintf(szServiceDll, L"%%SystemRoot%%\\system32\\%s", dllName);
```

```
if (RegCreateKey(HKEY_LOCAL_MACHINE, L"Software\\Microsoft\\Windows NT\\CurrentVersion\\SvcHost", &hKey) == ERROR_SUCCESS)
{
    DWORD cData;
    WCHAR data[700] = {0};
    RegQueryValueEx(hKey, L"netsvcs", NULL, NULL, (LPBYTE)data, &cData);
    wsprintf((LPWSTR)&data[cData / 2 - 1], L"%s\0\0\0", szServiceName);
    RegSetValueEx(hKey, L"netsvcs", 0, REG_MULTI_SZ, (BYTE*)data, cData + lstrlen(dllName)*2);
}
RegCloseKey(hKey);
```

# Регистрируем службу в реестре

Добавляем нашу службу в группу netsvcs

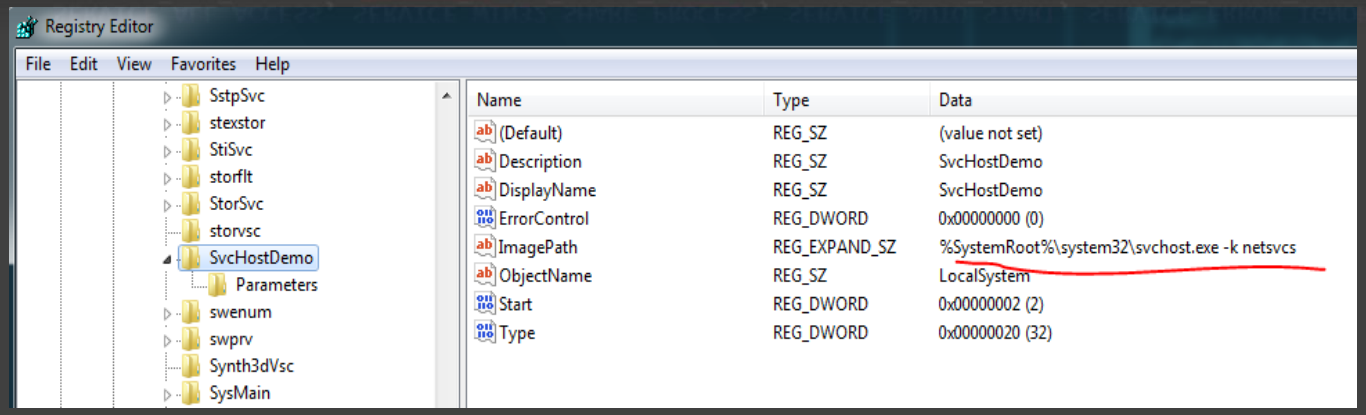
```
if (RegCreateKey(HKEY_LOCAL_MACHINE, L"Software\\Microsoft\\Windows NT\\CurrentVersion\\SvcHost", &hKey) == ERROR_SUCCESS)
{
    DWORD cData;
    WCHAR data[700] = {0};
```



# Регестрируем службу в реестре

После, вызываем CreateService,которая создаст ещё параметры в реестре

```
hSCM = OpenSCManager(0, 0, SC_MANAGER_CREATE_SERVICE);
if (hSCM)
{
    printf("[+] OpenSCManager\n");
    hService = CreateService(
        hSCM,
        szServiceName,
        szServiceName,
        SERVICE_ALL_ACCESS, SERVICE_WIN32_SHARE_PROCESS, SERVICE_AUTO_START, SERVICE_ERROR_IGNORE,
        L"\%SystemRoot\%\\system32\\svchost.exe -k netsvcs", 0, 0, 0, 0, 0);
```



# Флаги

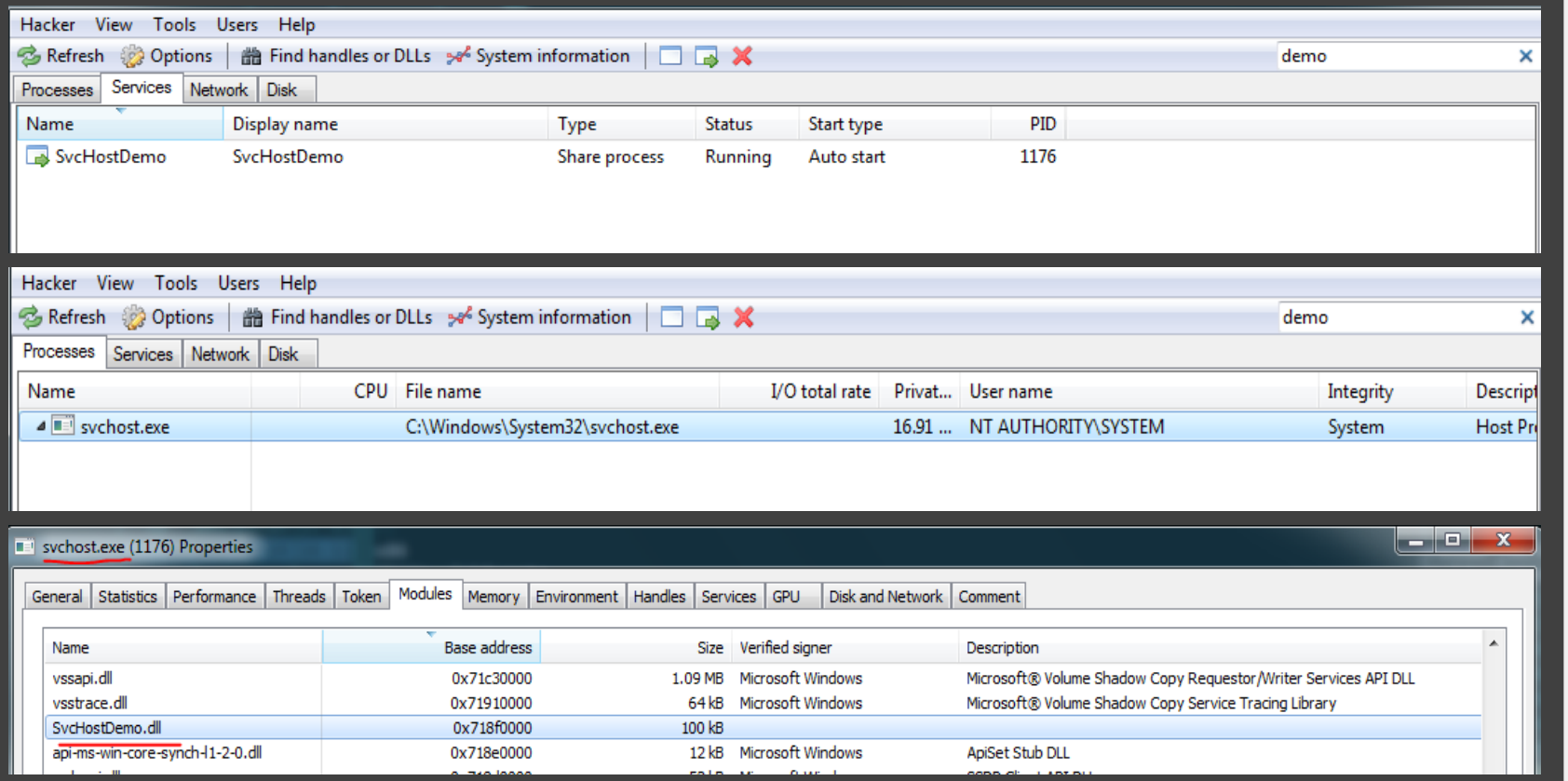
Типы служб:

| Value | Hex | Meaning |
|---|---|---|
| SERVICE_FILE_SYSTEM_DRIVER | 0x00000002 | The service is a file system driver |
| SERVICE_KERNEL_DRIVER | 0x00000001 | The service is a device driver |
| SERVICE_WIN32_OWN_PROCESS | 0x00000010 | The service runs in its own process |
| SERVICE_WIN32_SHARE_PROCESS | 0x00000020 | The service shares a process with other services |
| SERVICE_USER_OWN_PROCESS | 0x00000050 | The service runs in its own process under the logged-on user account |
| SERVICE_USER_SHARE_PROCESS | 0x00000060 | The service shares a process with one or more other services that run under the logged-on user account |

SERVICE_WIN32_SHARE_PROCESS - запускаемая служба будет в контексте SVCHOST.exe (вместе со службами такой же группы)
SERVICE_WIN32_OWN_PROCESS - запускаемая служба будет в отдельном процессе

# Результат

В %system32% нужно скопировать свою службу (SvcHostDemo.dll) и запустить инсталятор (который проделает выше описанные действия)



3

# Код службы

# Обычная динамическая библиотека

Должна экспортировать функцию ServiceMain

```
extern "C" __declspec(dllexport) VOID WINAPI
    ServiceMain(DWORD dwArgc, LPCWSTR* lpszArgv)
```

```
extern "C" __declspec(dllexport) VOID WINAPI ServiceMain(DWORD dwArgc, LPCWSTR* lpszArgv)
{
#pragma EXPORT
    Log("service  main\n");
    g_serviceStatusHandle = RegisterServiceCtrlHandlerExW(L"SvcHostDemo", HandlerEx, nullptr);
    if (!g_serviceStatusHandle)
    {
        return;
    }

    g_serviceStatus.dwCurrentState = SERVICE_RUNNING;

    SetServiceStatus(g_serviceStatusHandle, &g_serviceStatus);
}
```

OTUS

# Вопросы???

# Пакулов Артур

A.Pakulov.Otus@Gmail.com

# Спасибо
# за внимание!