



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



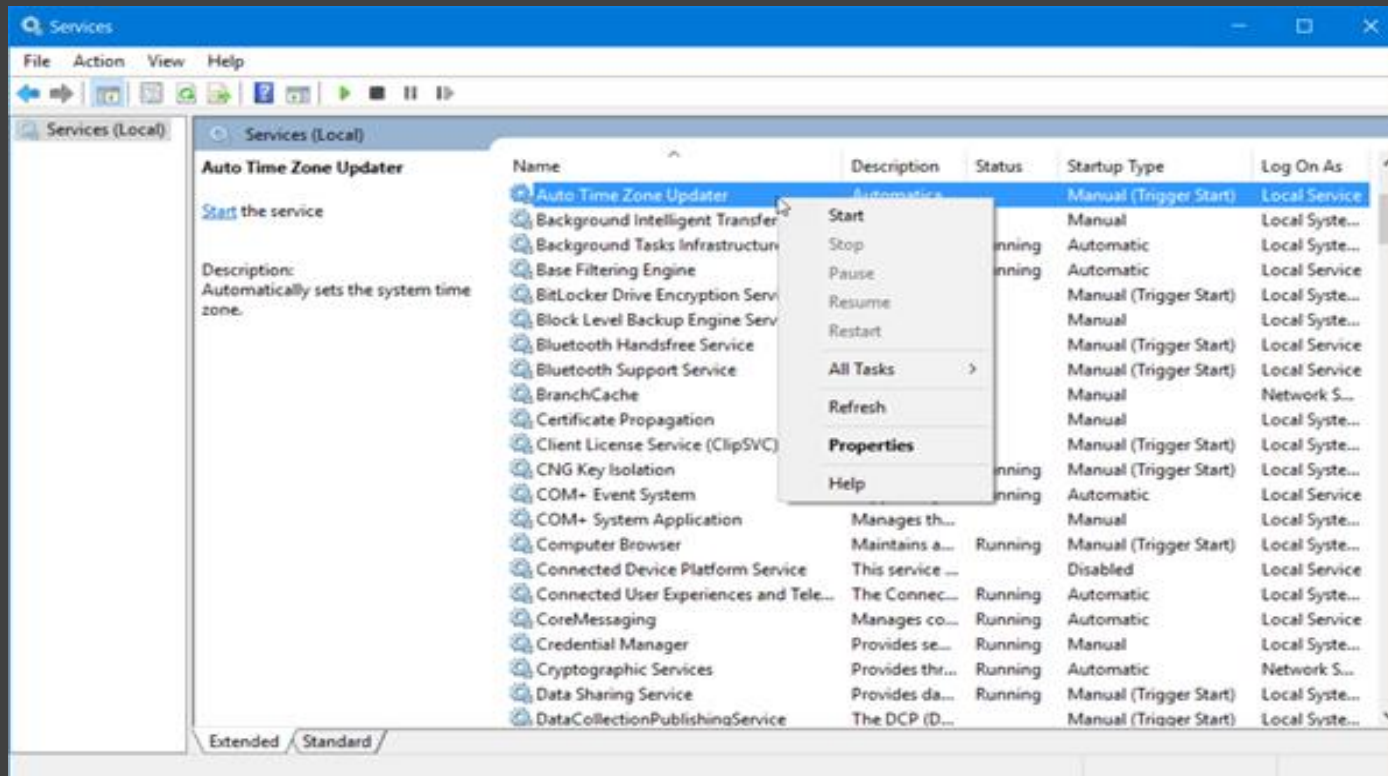
Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Программирование служб



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



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

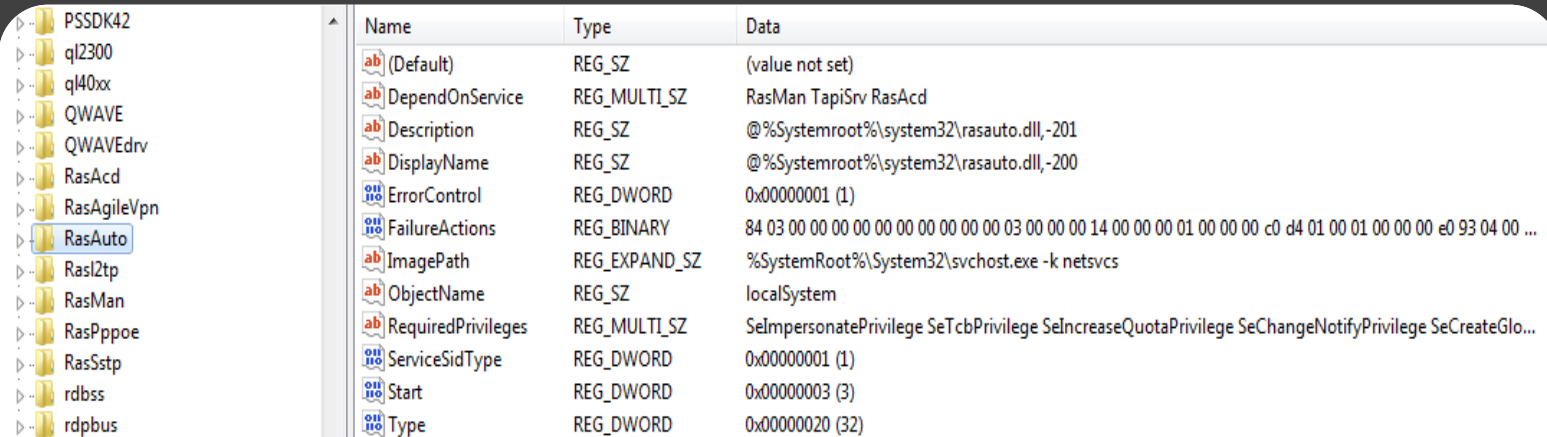
The screenshot shows the Windows Registry Editor with the path `HKLM\System\CurrentControlSet\Services` selected. The left pane shows a list of services, with `RasAuto` selected. The right pane displays the registry values for `RasAuto`.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RasMan TapiSrv RasAcid
Description	REG_SZ	@%Systemroot%\system32\rasauto.dll,-201
DisplayName	REG_SZ	@%Systemroot%\system32\rasauto.dll,-200
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	84 03 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 c0 d4 01 00 01 00 00 00 e0 93 04 00 ...
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k netsvcs
ObjectName	REG_SZ	localSystem
RequiredPrivileges	REG_MULTI_SZ	SeImpersonatePrivilege SeTcbPrivilege SeIncreaseQuotaPrivilege SeChangeNotifyPrivilege SeCreateGlo...
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000020 (32)

Значение imagePath:

`%SystemRoot%\System32\svchost.exe -k netsvcs`

говорит, что службы из группы netsvcs нужно загрузить в контексте процесса svchost.exe



Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RasMan TapiSrv RasAcad
Description	REG_SZ	@%Systemroot%\system32\rasauto.dll,-201
DisplayName	REG_SZ	@%Systemroot%\system32\rasauto.dll,-200
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	84 03 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 c0 d4 01 00 01 00 00 00 e0 93 04 00 ...
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k netsvcs
ObjectName	REG_SZ	localSystem
RequiredPrivileges	REG_MULTI_SZ	SeImpersonatePrivilege SeTcbPrivilege SeIncreaseQuotaPrivilege SeChangeNotifyPrivilege SeCreateGlo...
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000020 (32)

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

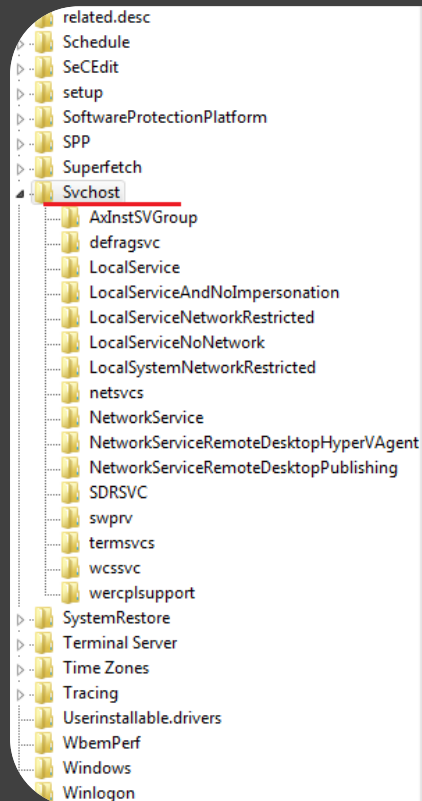
The screenshot shows the Windows Registry Editor with the path `HKLM\Software\Microsoft\Windows NT\CurrentVersion\SvcHost` selected. The right pane displays a list of registry values. The 'netsvc' value is highlighted in blue. An 'Edit Multi-String' dialog box is open in the foreground, showing the 'Value name' as 'netsvc' and a list of service names in the 'Value data' field.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AxInstSVGroup	REG_MULTI_SZ	AxInstSV
bthsvcs	REG_MULTI_SZ	bthserv
DcomLaunch	REG_MULTI_SZ	Power PlugPlay DcomLaunch
defragsvc	REG_MULTI_SZ	defragsvc
imgsvc	REG_MULTI_SZ	StiSvc
LocalService	REG_MULTI_SZ	nsi WdiServiceHost w32time EventSystem RemoteRegistry WinHttpAutoProxySvc sppuotify THREADORDER
LocalServiceAndNoImpersonation	REG_MULTI_SZ	SSDPSRV upnphost SCardSvr TBS FontCache fdrespub AppIDSvc QWAVE wcnscvc Mcx2Svc SensrSvc
LocalServiceNetworkRestricted	REG_MULTI_SZ	DHCP eventlog AudioSrv BthHFSrv LmHosts wscsvc homegroupprovider WPCSvc
LocalServiceNoNetwork	REG_MULTI_SZ	DPS PLA BFE mpsscvc WwanSvc
LocalServicePeerNet	REG_MULTI_SZ	PNRPSvc p2pimsvc p2psvc PnrpAutoReg
LocalSystemNetworkRestricted	REG_MULTI_SZ	UxSms WdiSystemHost Netman trkwks AudioEndpointBuilder WUDFSvc IPBusEnum dot3svc hidserv irmon sys
netsvc	REG_MULTI_SZ	AeLookupSvc CertPropSvc SCPolicySvc lanmanserver gpsvc IKEEXT AudioSrv FastUserSwitchingCompatibility
NetworkService	REG_MULTI_SZ	CryptSvc DHCP TermService DNSCache lanmanworkstation NapAgent nlasvc WinRM WECSVC Tapisrv
NetworkServiceAndNoImpersonation	REG_MULTI_SZ	KtmRm
NetworkServiceNetworkRestricted	REG_MULTI_SZ	PolicyAgent
PeerDist	REG_MULTI_SZ	PeerDistSvc
regsvc	REG_MULTI_SZ	RemoteRegistry
RPCSS	REG_MULTI_SZ	RpcEptMapper RpcSs
sdrsvc	REG_MULTI_SZ	sdrsvc
secsvc	REG_MULTI_SZ	WinDefend
swprv	REG_MULTI_SZ	swprv
termsvc	REG_MULTI_SZ	TermService
WbioSvcGroup	REG_MULTI_SZ	WbioSvc
wcssvc	REG_MULTI_SZ	WcsPluginService
WerSvcGroup	REG_MULTI_SZ	wersvc

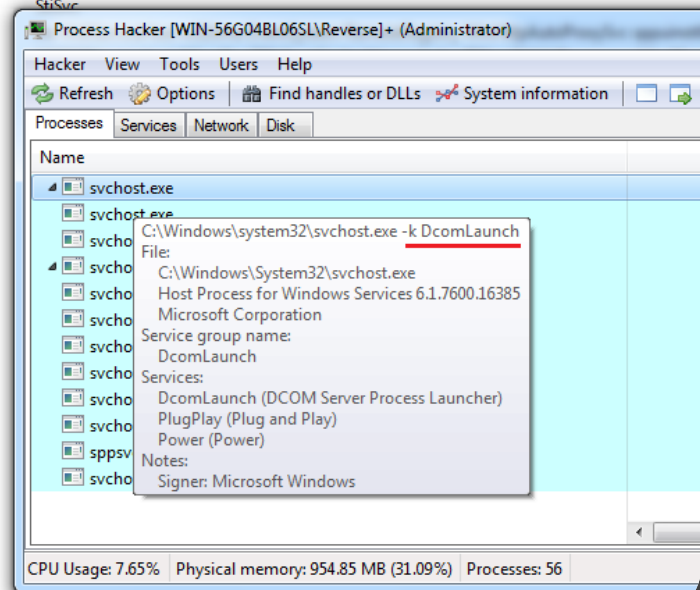
Edit Multi-String Dialog:

- Value name: netsvc
- Value data: AeLookupSvc, CertPropSvc, SCPolicySvc, lanmanserver, gpsvc, IKEEXT, AudioSrv, FastUserSwitchingCompatibility, las, lmon, Nla, Ntmsvc

Каждая группа загружается в контексте отдельного процесса svchost.exe



Name	Type	Data
(Default)	REG_SZ	(value not set)
AxInstSVGroup	REG_MULTI_SZ	AxInstSV
bthsvcs	REG_MULTI_SZ	bthserv
<u>DcomLaunch</u>	REG_MULTI_SZ	<u>Power PlugPlay DcomLaunch</u>
defragsvc	REG_MULTI_SZ	defragsvc
imgsvc	REG_MULTI_SZ	
LocalService	REG_MULTI_SZ	
LocalServiceAndNoImpersonation	REG_MULTI_SZ	
LocalServiceNetworkRestricted	REG_MULTI_SZ	
LocalServiceNoNetwork	REG_MULTI_SZ	
LocalServicePeerNet	REG_MULTI_SZ	
LocalSystemNetworkRestricted	REG_MULTI_SZ	
netssvc	REG_MULTI_SZ	
NetworkService	REG_MULTI_SZ	
NetworkServiceAndNoImpersonat...	REG_MULTI_SZ	
NetworkServiceNetworkRestricted	REG_MULTI_SZ	
PeerDist	REG_MULTI_SZ	
regsvc	REG_MULTI_SZ	
RPCSS	REG_MULTI_SZ	
sdrsvc	REG_MULTI_SZ	
secsvc	REG_MULTI_SZ	
swprv	REG_MULTI_SZ	
termssvc	REG_MULTI_SZ	
WbioSvcGroup	REG_MULTI_SZ	
wcssvc	REG_MULTI_SZ	
WerSvcGroup	REG_MULTI_SZ	



Внимание!

Легитимный svchost.exe всегда является дочерним процессом services.exe

The image shows a Windows Registry Editor window with the 'Svchost' key selected. The right pane displays a list of registry values. The 'DcomLaunch' value is highlighted with a red line. Below the registry window, the Process Hacker application is open, showing the 'Services' tab. The 'svchost.exe' process is selected, and a tooltip displays its properties, including the command line: 'C:\Windows\system32\svchost.exe -k DcomLaunch'.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AxInstSVGroup	REG_MULTI_SZ	AxInstSV
bthsvcs	REG_MULTI_SZ	bthserv
<u>DcomLaunch</u>	REG_MULTI_SZ	<u>Power PlugPlay DcomLaunch</u>
defragsvc	REG_MULTI_SZ	defragsvc
imgsvc	REG_MULTI_SZ	
LocalService	REG_MULTI_SZ	
LocalServiceAndNoImpersonation	REG_MULTI_SZ	
LocalServiceNetworkRestricted	REG_MULTI_SZ	
LocalServiceNoNetwork	REG_MULTI_SZ	
LocalServicePeerNet	REG_MULTI_SZ	
LocalSystemNetworkRestricted	REG_MULTI_SZ	
netsh	REG_MULTI_SZ	
NetworkService	REG_MULTI_SZ	
NetworkServiceAndNoImpersonat...	REG_MULTI_SZ	
NetworkServiceNetworkRestricted	REG_MULTI_SZ	
PeerDist	REG_MULTI_SZ	
regsvc	REG_MULTI_SZ	
RPCSS	REG_MULTI_SZ	
sdrsvc	REG_MULTI_SZ	
secsvc	REG_MULTI_SZ	
swprv	REG_MULTI_SZ	
termshvc	REG_MULTI_SZ	
WbioSvcGroup	REG_MULTI_SZ	
wcssvc	REG_MULTI_SZ	
WerSvcGroup	REG_MULTI_SZ	

Process Hacker [WIN-56G04BL06SL\Reverse]+ (Administrator)

Process: svchost.exe

File: C:\Windows\System32\svchost.exe

Host Process for Windows Services 6.1.7600.16385

Microsoft Corporation

Service group name: DcomLaunch

Services: DcomLaunch (DCOM Server Process Launcher), PlugPlay (Plug and Play), Power (Power)

Notes: Signer: Microsoft Windows

CPU Usage: 7.65% Physical memory: 954.85 MB (31.09%) Processes: 56

2

Пример

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;
```

```
return result;  
}  
return result;
```

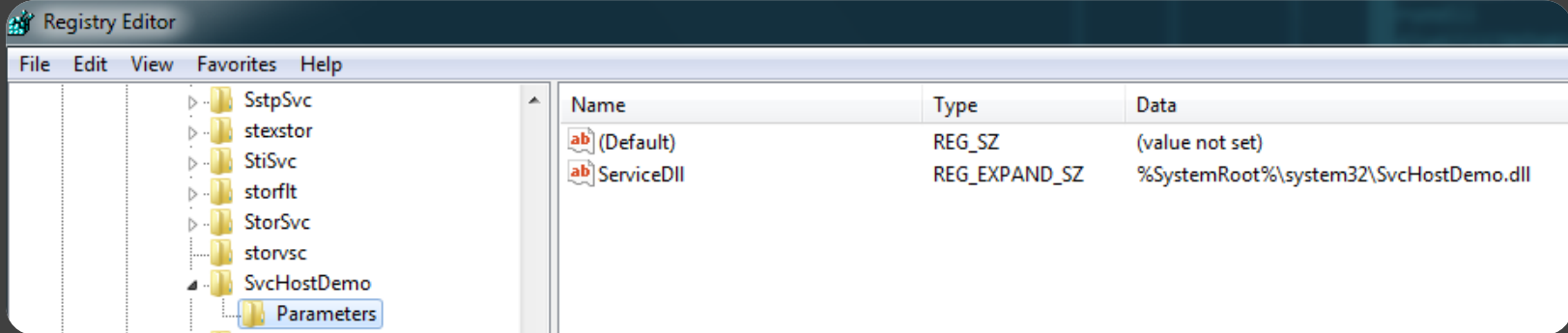
Затем создаём параметр «Description» и подключаем «Parameters» с значением «ServiceDll»

```
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;
```

```
return result;  
}  
return result;
```

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



Добавляем нашу службу в группу netsvcs

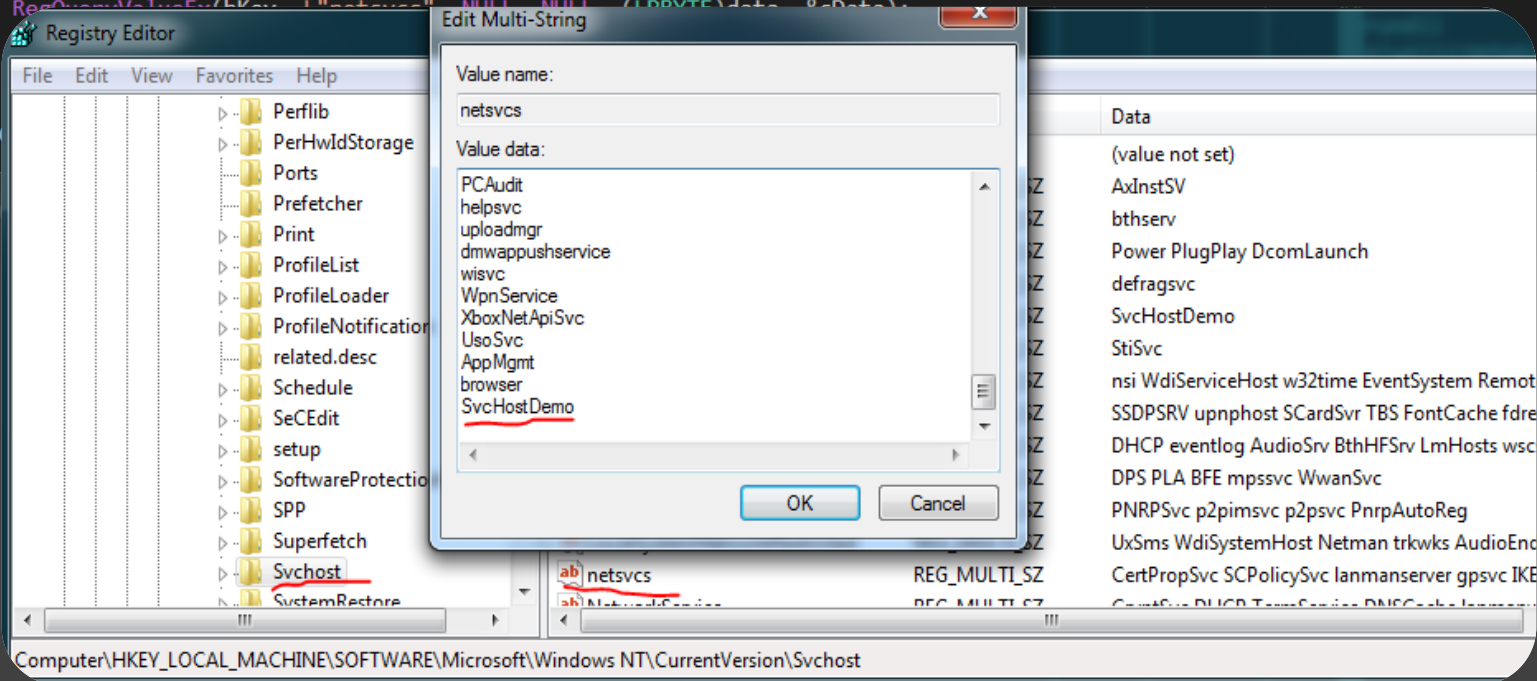
```
wsprintf(szRegPath, L"SYSTEM\\CurrentControlSet\\Services\\%s", szServiceName);  
wsprintf(szServiceDll, L"%%SystemRoot%%\\system32\\%s", dllName);
```

```
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);
```

```
увсгтозекел(μκελ)?  
}
```

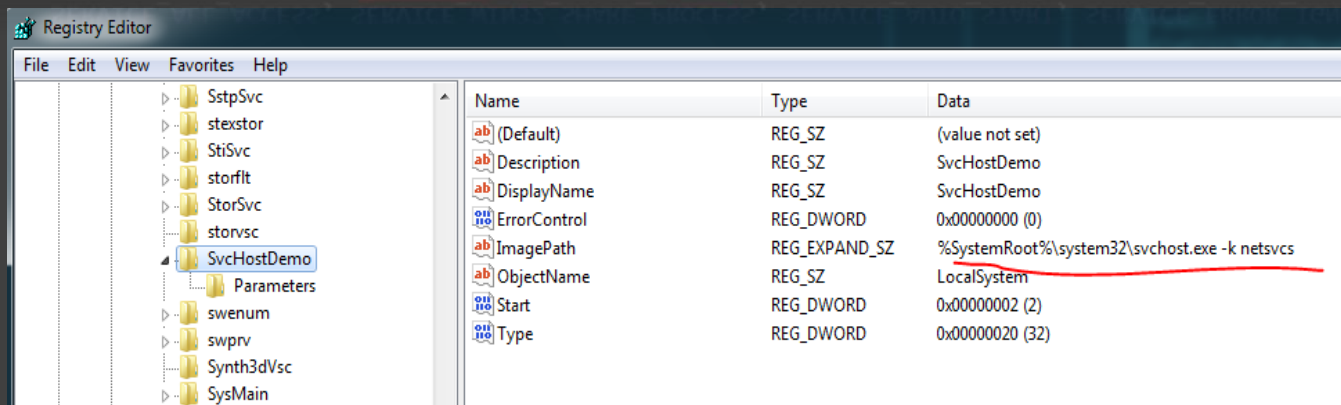
Добавляем нашу службу в группу netsvcs

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



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);
```



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

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

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information demo

Processes Services Network Disk

Name	Display name	Type	Status	Start type	PID
SvcHostDemo	SvcHostDemo	Share process	Running	Auto start	1176

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information demo

Processes Services Network Disk

Name	CPU	File name	I/O total rate	Privat...	User name	Integrity	Descript
svchost.exe		C:\Windows\System32\svchost.exe	16.91 ...		NT AUTHORITY\SYSTEM	System	Host Pr

svchost.exe (1176) Properties

General Statistics Performance Threads Token Modules Memory Environment Handles Services GPU Disk and Network Comment

Name	Base address	Size	Verified signer	Description
vssapi.dll	0x71c30000	1.09 MB	Microsoft Windows	Microsoft® Volume Shadow Copy Requestor/Writer Services API DLL
vsstrace.dll	0x71910000	64 kB	Microsoft Windows	Microsoft® Volume Shadow Copy Service Tracing Library
SvcHostDemo.dll	0x718f0000	100 kB		
api-ms-win-core-synch-l1-2-0.dll	0x718e0000	12 kB	Microsoft Windows	ApiSet Stub DLL

3

Код службы

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);  
}
```

O T U S

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

