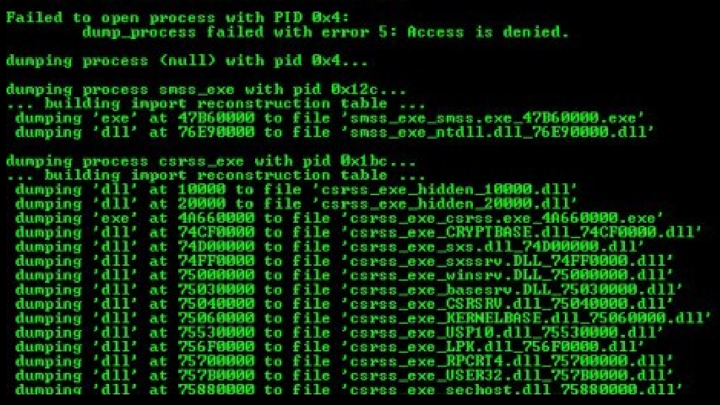
SECURITY LIST NETWORK™
"TO KEEP EVERYTHING TESTED AND SECURE"

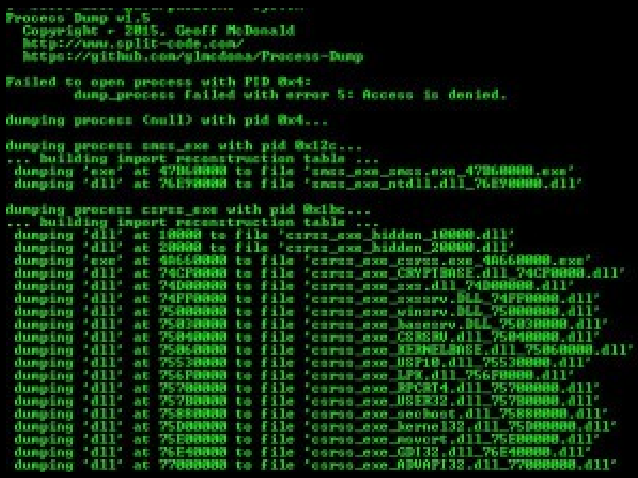


```
Failed to open process with PID 0x4:
        dump_process failed with error 5: Access is denied.

dumping process (null) with pid 0x4...

dumping process smss_exe with pid 0x12c...
... building import reconstruction table ...
 dumping 'exe' at 47B60000 to file 'smss_exe_smss.exe_47B60000.exe'
 dumping 'dll' at 76E90000 to file 'smss_exe_ntdll.dll_76E90000.dll'

dumping process csrss_exe with pid 0x1bc...
... building import reconstruction table ...
 dumping 'dll' at 10000 to file 'csrss_exe_hidden_10000.dll'
 dumping 'dll' at 20000 to file 'csrss_exe_hidden_20000.dll'
 dumping 'exe' at 4A660000 to file 'csrss_exe_csrss.exe_4A660000.exe'
 dumping 'dll' at 74CF0000 to file 'csrss_exe_CRYPTBASE.dll_74CF0000.dll'
 dumping 'dll' at 74D00000 to file 'csrss_exe_sxs.dll_74D00000.dll'
 dumping 'dll' at 74FF0000 to file 'csrss_exe_sxssrv.DLL_74FF0000.dll'
 dumping 'dll' at 75000000 to file 'csrss_exe_winsrv.DLL_75000000.dll'
 dumping 'dll' at 75030000 to file 'csrss_exe_basesrv.DLL_75030000.dll'
 dumping 'dll' at 75040000 to file 'csrss_exe_CSRSRV.dll_75040000.dll'
 dumping 'dll' at 75060000 to file 'csrss_exe_KERNELBASE.dll_75060000.dll'
 dumping 'dll' at 75530000 to file 'csrss_exe_USP10.dll_75530000.dll'
 dumping 'dll' at 756F0000 to file 'csrss_exe_LPK.dll_756F0000.dll'
 dumping 'dll' at 75700000 to file 'csrss_exe_RPCRT4.dll_75700000.dll'
 dumping 'dll' at 757B0000 to file 'csrss_exe_USER32.dll_757B0000.dll'
 dumping 'dll' at 75880000 to file 'csrss_exe_sechost.dll_75880000.dll'
```

PROCESS DUMP V1.5 RELEASED ; WINDOWS TOOL FOR DUMPING MALWARE PE FILES FROM MEMORY.

November 21, 2015 · by Fragile · in Anti Malware/Virus - Malware Analysis, Security Tools

Windows reverse-engineering command-line tool to dump malware memory components back to disk for analysis. This is a common task for malware researchers who need to dump unpacked or injected code back to disk for analysis with static analysis tools such as IDA.



```
Process Dump v1.5
  Copyright © 2015, Geoff McDonald
  http://www.split-code.com/
  https://github.com/glmcdona/Process-Dump

Failed to open process with PID 0x4:
        dump_process failed with error 5: Access is denied.

dumping process (null) with pid 0x4...

dumping process smss_exe with pid 0x12c...
... building import reconstruction table ...
 dumping 'exe' at 47B60000 to file 'smss_exe_smss.exe_47B60000.exe'
 dumping 'dll' at 76E90000 to file 'smss_exe_ntdll.dll_76E90000.dll'

dumping process csrss_exe with pid 0x1bc...
... building import reconstruction table ...
 dumping 'dll' at 10000 to file 'csrss_exe_hidden_10000.dll'
 dumping 'dll' at 20000 to file 'csrss_exe_hidden_20000.dll'
 dumping 'exe' at 4A660000 to file 'csrss_exe_csrss.exe_4A660000.exe'
 dumping 'dll' at 74CF0000 to file 'csrss_exe_CRYPTBASE.dll_74CF0000.dll'
 dumping 'dll' at 74D00000 to file 'csrss_exe_sxs.dll_74D00000.dll'
 dumping 'dll' at 74FF0000 to file 'csrss_exe_sxssrv.DLL_74FF0000.dll'
 dumping 'dll' at 75000000 to file 'csrss_exe_winsrv.DLL_75000000.dll'
 dumping 'dll' at 75030000 to file 'csrss_exe_basesrv.DLL_75030000.dll'
 dumping 'dll' at 75040000 to file 'csrss_exe_CSRSRV.dll_75040000.dll'
 dumping 'dll' at 75060000 to file 'csrss_exe_KERNELBASE.dll_75060000.dll'
 dumping 'dll' at 75530000 to file 'csrss_exe_USP10.dll_75530000.dll'
 dumping 'dll' at 756F0000 to file 'csrss_exe_LPK.dll_756F0000.dll'
 dumping 'dll' at 75700000 to file 'csrss_exe_RPCRT4.dll_75700000.dll'
 dumping 'dll' at 757B0000 to file 'csrss_exe_USER32.dll_757B0000.dll'
 dumping 'dll' at 75880000 to file 'csrss_exe_sechost.dll_75880000.dll'
 dumping 'dll' at 75D00000 to file 'csrss_exe_kernel32.dll_75D00000.dll'
 dumping 'dll' at 75E00000 to file 'csrss_exe_msvcrt.dll_75E00000.dll'
 dumping 'dll' at 76E40000 to file 'csrss_exe_GDI32.dll_76E40000.dll'
 dumping 'dll' at 77000000 to file 'csrss_exe_ADVAPI32.dll_77000000.dll'
```

Windows tool for dumping malware PE files from memory back to disk for analysis

Process Dump works for 32 and 64 operating systems, uses an aggressive import reconstruction approach, and allows for dumping of regions without PE headers – in these cases PE headers and import tables will automatically be generated. Process Dump supports creation and use of a clean-hash database, so that dumping of clean files such as kernel32.dll can be skipped

Example Usage:

```
Dump all modules from all processes (ignor

    pd64.exe -system

Dump all modules from a specific process i

    pd64.exe -pid 0x18A

Dump all modules by process name:

    pd64.exe -p .chrome.

Build clean-hash database. These hashes wi

    pd64.exe -db gen

Dump code from a specific address in PID 0

    pd64.exe -pid 0x1a3 -a 0xffb4000 Gener
```

Download executable file for Windows 32&64 bit :

pd_latest(100.32 KB)

or you can build itself using Visual Studio here

Source : https://github.com/glmcdona

Tags: Malware Analysis, PE(Portable Executable), Reverse Engineering, Visual-Studio

← CTB-Locker Ransomware Scripts.

SimpleEmail v0.5 released – is a email recon tool that is fast and easy framework to build on. →

DIGITAL FORENSICS / NETWORKING / PENETRATION TEST / SECURITY TOOLS