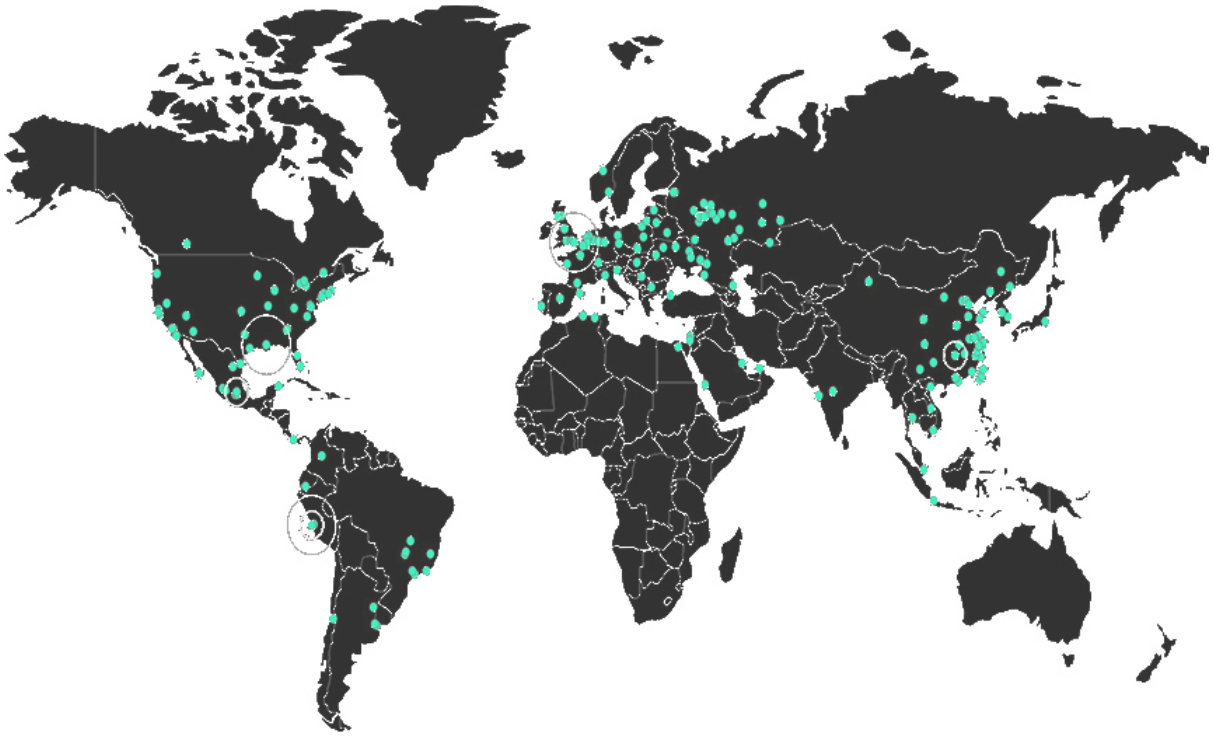
MALWARE ANALYSIS REPORT

No.10 | 2017 년 06 월

WannaCry 랜섬웨어 분석

#2 SMB 취약점 분석



목 차

1. 개 요

1.1 배 경

2017년 5월 17일 배포한 WannaCry 분석보고서에도 언급되었듯이, WannaCry 랜섬웨어의 경우 SMB 취약점을 이용하여 웜과 같이 다른 PC로 확산되어 추가 감염을 발생시키고 있다. 또한, Check Payment 등의 외부 서버와 통신이 필요한 경우에는 Tor 네트워크를 이용하는 특징이 있으며, 랜섬웨어 내부 리소스에서 Tor 프로그램을 생성하여 사용한다.

이에 소만사 악성코드분석센터에서는 SMB 취약점에 관하여 자세히 분석하여 보고서를 작성하게 되었다. 본 보고서에는 WannaCry 랜섬웨어에서 사용하는 SMB 취약점 공격의 동작 흐름과, 대상이 되는 PC에서 감염이 어떤 방식으로 이루어지는지 기술한다.

[참고] 2017년 5월 17일 배포한 월간 악성코드 리포트

1.2 파일 정보

Name	**mssecsvc.exe**
Type	Windows 실행 파일
Size	3,723,264 바이트
Sha256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Behavior	WannaCry Ransomware
Description	SMB 취약점 공격 및 tasksche.exe 생성

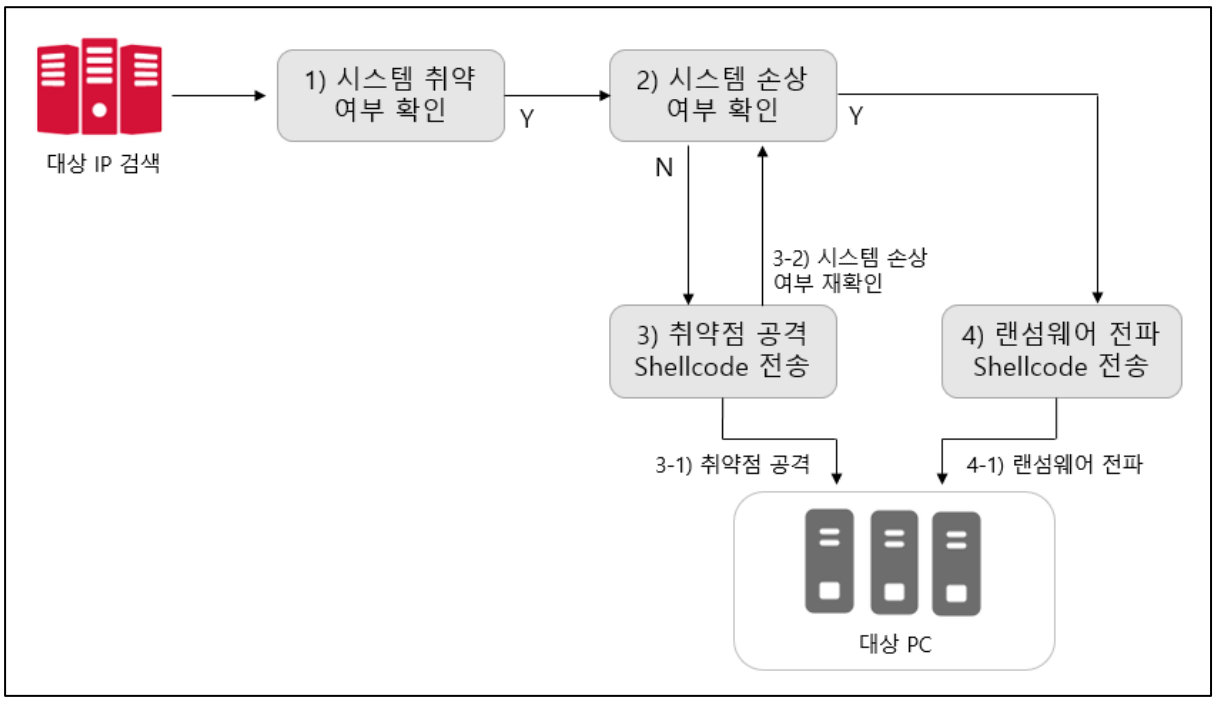
Name	**tasksche.exe**
Type	Windows 실행 파일
Size	3,514,368 바이트
Sha256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Behavior	WannaCry Ransomware
Description	파일 암호화

2. 상세 분석

WannaCry 랜섬웨어의 가장 큰 특징인 SMB 원격코드 실행 취약점을 이용한 전파 기능의 전체적인 동작 흐름에 대해서 기술한다.

SMB(Server Message Block) 도스나 윈도우에서 파일이나 디렉터리 및 주변 장치들을 공유하는데 사용되는 메시지 형식이다. WannaCry 랜섬웨어는 SMB 메시지를 대상 PC에 전송하여 취약점을 공격하고, 랜섬웨어를 전파한다.

2.1 SMB 취약점 공격 흐름



[그림 1] SMB 취약점 공격 흐름

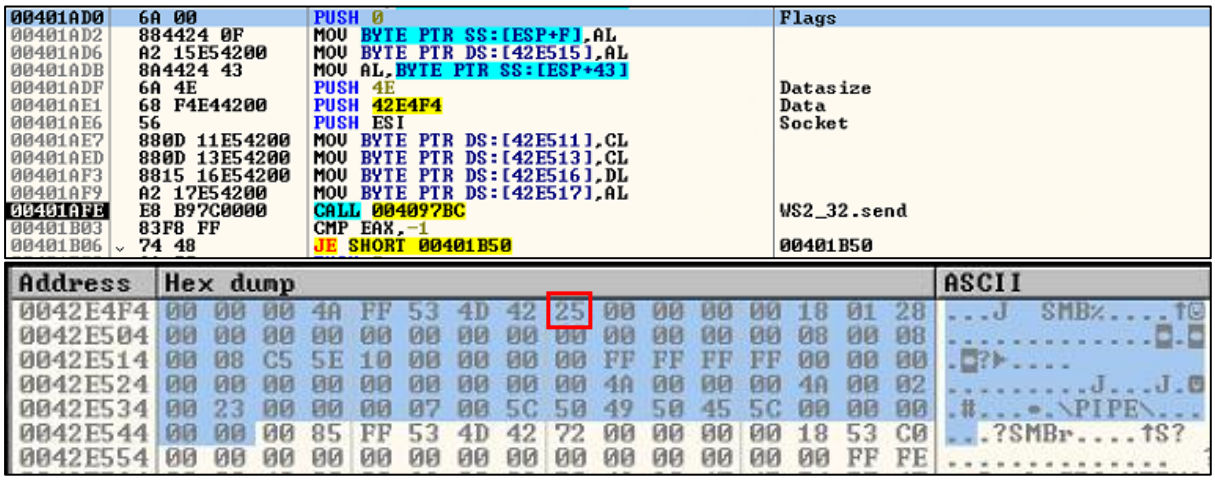
WannaCry 랜섬웨어의 취약점 공격 흐름은 대상 PC의 취약 여부를 확인 후 취약하다고 판단되면 shellcode를 전송하여 취약점 공격 및 악성코드 감염을 시도한다.

1) 대상 PC의 취약 여부 확인

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_TRANSACTION	0x25	서버에서 메일 슬롯 및 namedpipe를 생성

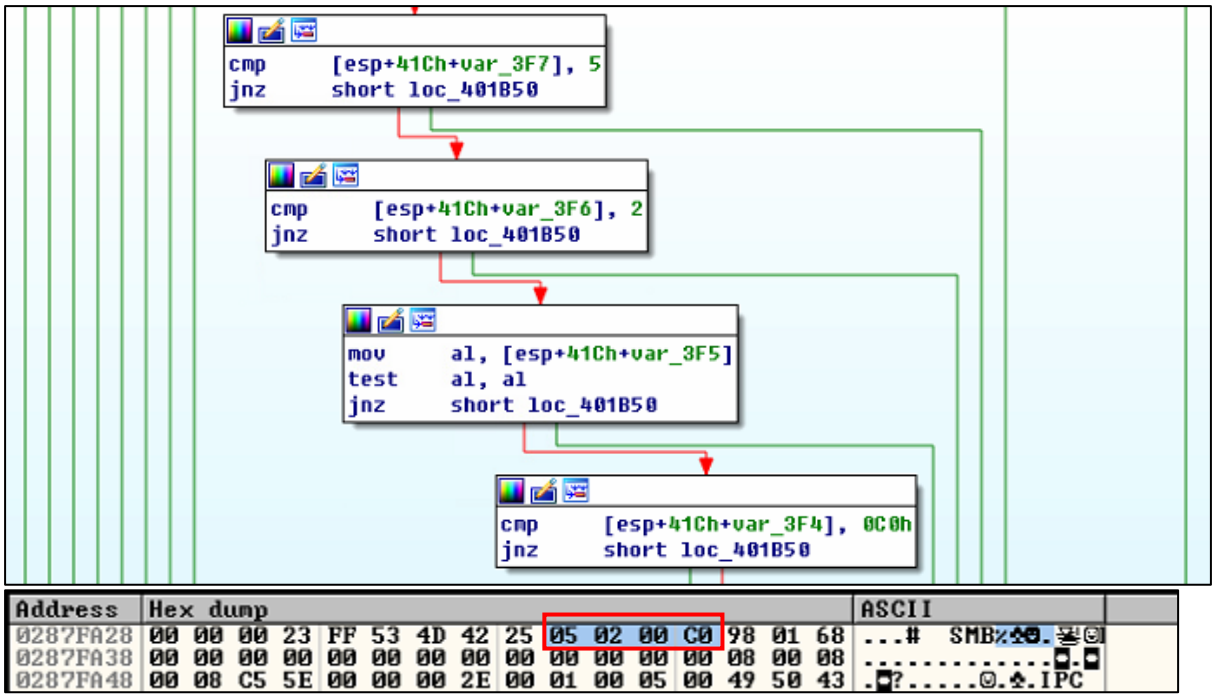
[취약 여부 판단에 사용되는 SMB 메시지]

WannaCry 랜섬웨어는 대상 PC의 취약 여부를 판단하기 위해 SMB_COM_NEGOTIATE 메시지를 시작으로 하는 일반적인 SMB 연결 과정을 거치고, SMB_COM_TRANSACTION 메시지의 response 값을 참조한다. 해당 메시지는 서버에서 메일 슬롯 및 Namedpipe를 생성하기 위해 사용하는 메시지 이다.



[그림 2] SMB_COM_TRANSACTION Request Message (0x25)

대상 PC에 send 함수를 이용하여 [그림 2]의 SMB 메시지를 전송하고 response 메시지를 받는다.



[그림 3] Response 값의 NTSTATUS 값 확인 (0xC0000205)

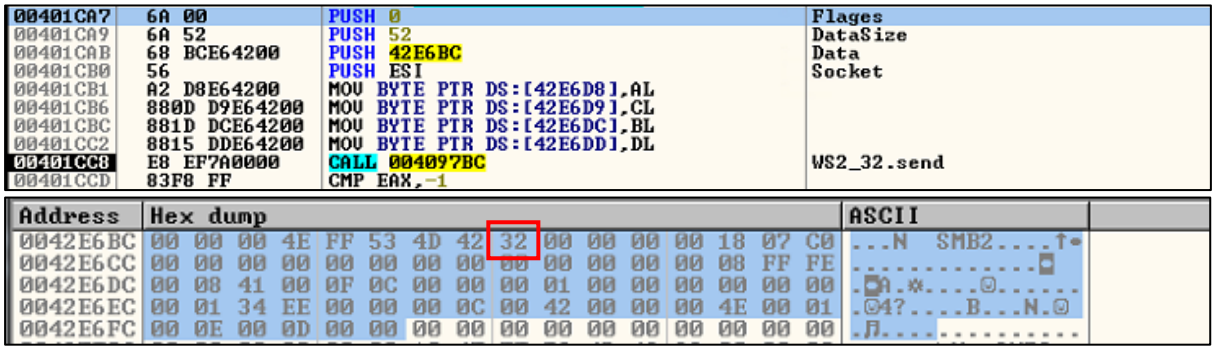
Response 메시지의 NTSTATUS 값을 확인하여 0xC0000205와 일치하면 대상이 되는 PC는 취약(SMB 취약점에 대한 업데이트가 되지 않은 경우)하다고 판단한다.
(0xC0000205 : STATUS_INSUFF_SERVER_RESOURCES)

2) 대상 PC 손상 확인

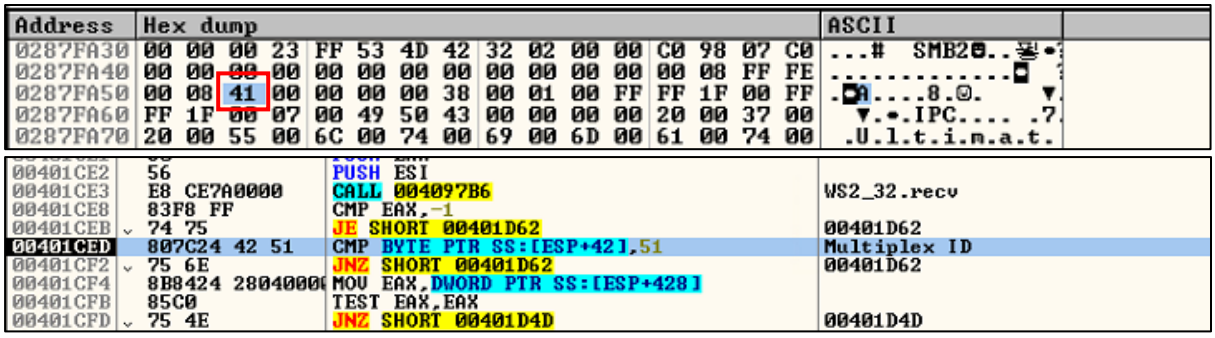
SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_TRANSACTION2	0x32	서버에서 특정 작업 실행(디렉토리 검색 등)

[손상 여부 확인에 사용되는 SMB 메시지]

대상 PC가 취약하다고 판단되면 해당 시스템이 이미 손상 되었는지 확인하기 위하여 SMB_COM_TRANSACTION2 Request 메시지를 전송한다.



[그림 4] SMB_COM_TRANSACTION2 Request Message (0x32)



[그림 5] Response 값의 Multiplex ID 값 확인

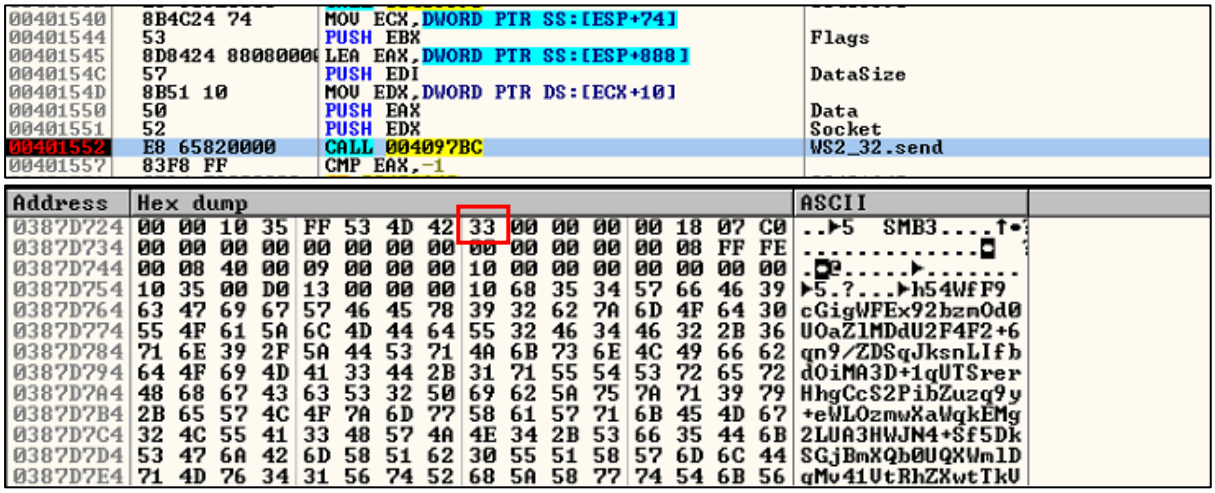
해당 메시지의 Response 값에서 Multiplex ID 값을 확인하여 대상 PC의 손상 여부를 확인한다. 이미 손상된 PC는 0x51이 반환되고, 손상되지 않은 PC에서는 0x41이 반환된다.

3) 대상 PC의 취약점 공격

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다.
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다.
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다.
SMB_COM_NT_TRANSACT	0xA0	서버에 작업을 지정하는데 사용한다.
SMB_COM_TRANSACTION2_SECONDARY	0x33	SMB_COM_TRANSACTION2 요청에 의해 시작된 데이터 전송을 완료하는데 사용된다.
SMB_COM_ECHO	0x2B	서버와 클라이언트 간 전송 계층 연결 테스트

[취약점 발생 유도 에 사용되는 SMB 메시지]

대상 PC가 손상 되지 않았다고 판단되면 취약점 공격을 발생 시키는 메시지를 전송한다. 메시지에는 쉘코드가 포함되어 있으며, 해당 쉘코드가 실행되면 대상 PC에서 취약점 공격이 실행된다.



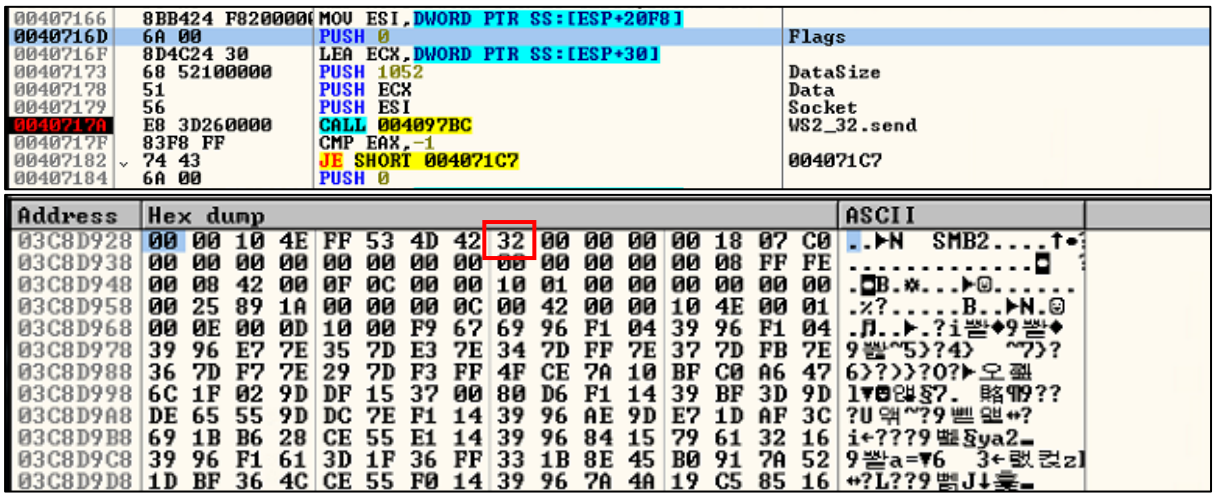
[그림 6] SMB_COM_TRANSACTION2_SECONDARY Request Message (0x33)

상기 메시지 전송이 완료되면 2) 대상 PC 손상 확인 동작을 다시 실행하여 대상 시스템이 손상된 것을 확인하고 랜섬웨어 전파 동작으로 넘어간다.

4) 악성코드 전파

SMB Message	Value	Description
SMB_COM_NEGOTIATE	0x72	서버와 클라이언트 간 SMB 연결을 시작한다
SMB_COM_SESSION_SETUP_ANDX	0x73	SMB 세션을 구성하는데 사용된다
SMB_COM_TREE_CONNECT_ANDX	0x75	서버 공유에 대한 클라이언트 연결을 설정한다
SMB_COM_TRANSACTION2	0x32	서버에서 특정 작업 실행(디렉토리 검색 등)

[악성코드 전파 에 사용되는 SMB 메시지]

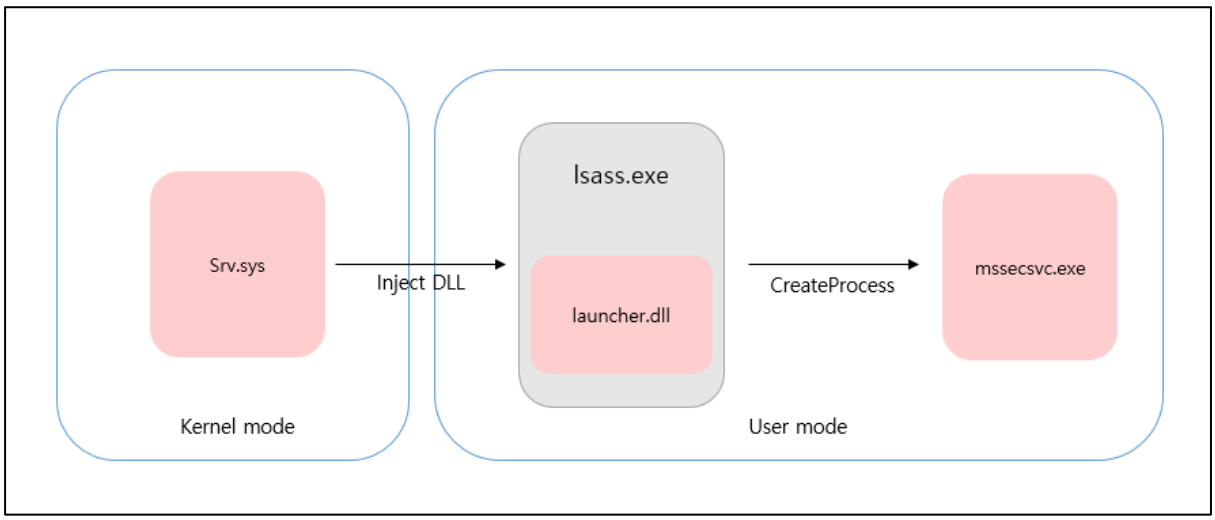


[그림 7] SMB_COM_TRANSACTION2 Request Message (0x32)

최종적으로 악성 DLL 파일이 포함된 SMB 메시지를 대상 PC에 전송한다. 대상 PC에서 DLL 파일이 실행되면 WannaCry 랜섬웨어에 감염되게 된다.

5) 대상 PC에서 악성코드 실행

악성코드는 DLL 형태의 실행 파일이며 대상 PC로 전송 시 암호화 되어 전송된다.
복호화되면 launcher.dll로 생성되어 악성동작을 하게 된다.



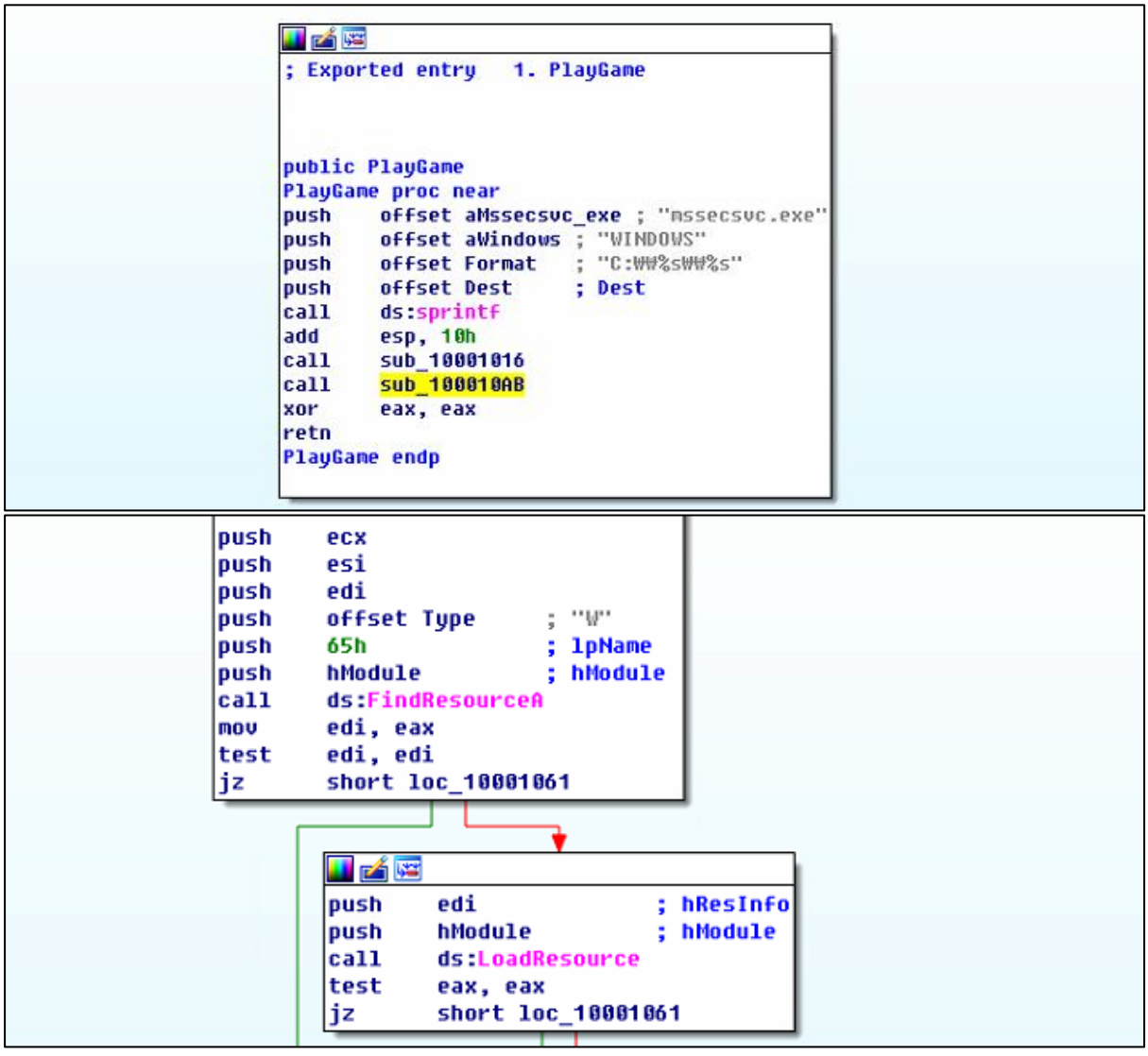
[그림 8] 대상 PC 감염 동작

취약점 발생 코드에 의해 패치 된 SMB 드라이버 Srv.sys에 의해서 유저모드에서 실행 중인 lsass.exe에 launcher.dll이 인젝션되게 된다. 인젝션 후 해당 launcher.dll에 존재하는 Export 함수인 PlayGame이 실행된다.

```
00 00 00 01 00 00 00 01 00 00 00 B8 21 00 00 BC  ............¸!..¼
21 00 00 C0 21 00 00 14 11 00 00 CF 21 00 00 00  !..À!.....Ï!...
00 6C 61 75 6E 63 68 65 72 2E 64 6C 6C 00 50 6C  .launcher.dll.Pl
61 79 47 61 6D 65 00 00 00 00 00 00 00 00 00 00  ayGame..........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[그림 9] lsass.exe에 인젝션된 launcher.dll

[launcher.dll PlayGame 함수]



[그림 10] 내부 리소스의 mssecsvs.exe 생성

Launcher.dll 의 Export 함수인 PlayGame을 살펴보면 내부 리소스에서 PE 실행 파일을 로드하여 mssecsvc.exe 이름으로 생성한다.

```
lea     eax, [ebp+ProcessInformation]
mov     [ebp+StartupInfo.cb], 44h
push    eax             ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax             ; lpStartupInfo
push    edx             ; lpCurrentDirectory
push    edx             ; lpEnvironment
push    8000000h        ; dwCreationFlags
push    edx             ; bInheritHandles
push    edx             ; lpThreadAttributes
push    edx             ; lpProcessAttributes
push    offset Dest     ; lpCommandLine
push    edx             ; lpApplicationName
mov     [ebp+StartupInfo.wShowWindow], dx
mov     [ebp+StartupInfo.dwFlags], 81h
call    ds:CreateProcessA
test    eax, eax
```

[그림 11] Ransomware 메인 실행

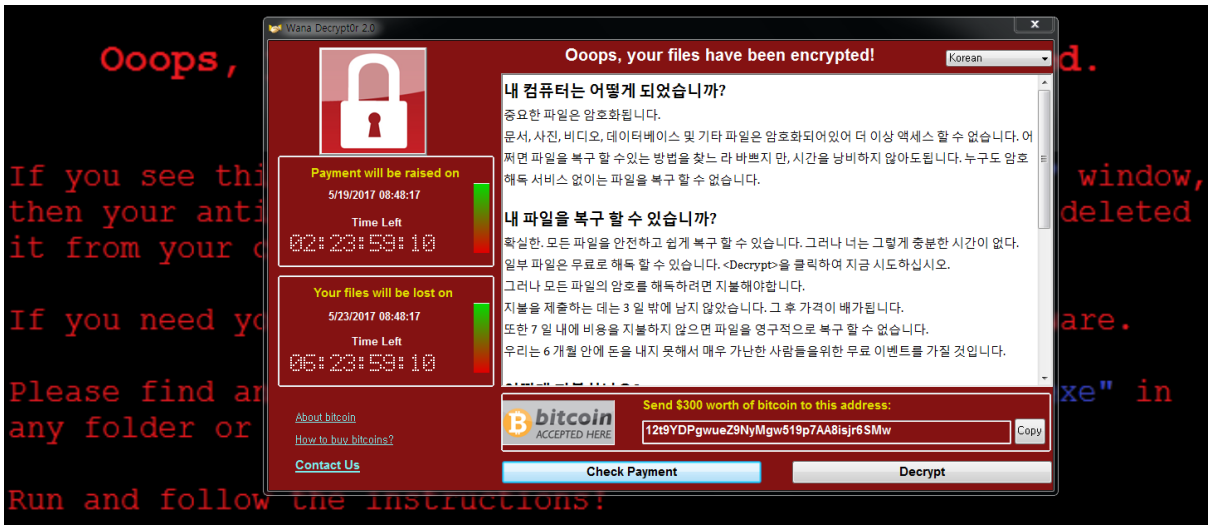
생성된 mssecsvc.exe를 CreateProcessA를 호출하여 실행시킨다. 해당 프로세스가 실행되면 시스템의 감염은 완료된다.

[감염 확인]

svchost.exe		1,244 K	4,400 K	1412 Host Process for Windo...
lsass.exe		13,072 K	15,744 K	484 Local Security Authority...
mssecsvc.exe	96.12	3,688 K	2,512 K	100 Microsoft® Disk Defrag...
lsm.exe		1,220 K	1,472 K	492 로컬 세션 관리자 서비스
csrss.exe	0.13	6,908 K	6,624 K	384 Client Server Runtime P...

[그림 12] 대상 PC 감염

대상 PC에서 감염 동작을 확인하면 lsass.exe 하위로 mssecsvc.exe가 실행되는 것을 확인 할 수 있다. 이후로 파일 암호화 동작 및 추가 감염 동작이 실행 된다.



[그림 13] 랜섬노트 실행

파일 암호화가 완료되면 위와 같이 바탕화면을 변경하고, 랜섬노트를 실행한다.

2.2 특징적인 행위

[Tor를 이용한 외부 통신]
WannaCry 랜섬웨어는 디코딩 및 추가 동작을 위하여 외부 서버와 통신을 해야 할 경우 Tor 네트워크를 이용한다.

```
lea     edi, [esp+46Ch+var_40F]
push    offset aTaskhsvc_exe ; "taskhsvc.exe"
rep stosd
stosw
push    offset aTor      ; "Tor"
push    offset PathName ; "TaskData"
lea     ecx, [esp+478h+Dest]
push    offset aSSS      ; "%s\%s\%s"
push    ecx              ; Dest
stosb
call    sprintf
mov     esi, ds:GetFileAttributesA
add     esp, 14h
lea     edx, [esp+46Ch+Dest]
push    edx              ; lpFileName
call    esi ; GetFileAttributesA
cmp     eax, 0FFFFFFFFh
```

[그림 14] Tor 파일 확인

아래의 경로에서 Taskhsvc.exe 파일이 존재하는지 확인한다. 해당 파일은 tor 파일을 이름만 변경한 것으로 네트워크 통신 시 이 파일을 사용한다.

```
  sprintf(&FileName, aSSS, PathName, aTor, aTor_exe);
  if ( GetFileAttributesA(&FileName) == -1 )
    return 0;
  CopyFileA(&FileName, &Dest, 0);
}
StartupInfo.cb = 68;
ProcessInformation.hProcess = 0;
memset(&StartupInfo.lpReserved, 0, 0x40u);
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
StartupInfo.wShowWindow = 0;
StartupInfo.dwFlags = 1;
if ( CreateProcessA(0, &Dest, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
{
  if ( WaitForSingleObject(ProcessInformation.hProcess, 0x1388u) == 258 )
    WaitForSingleObject(ProcessInformation.hProcess, 0x7530u);
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
  result = 1;
```

[그림 15] Tor 프로세스 실행

해당 파일이 존재하지 않으면 다시 생성하고, CreateProcessA를 호출하여 해당 파일을 프로세스로 실행한다.

System	4	TCP	192.168.158.129	139	0.0.0.0	0	LISTENING
System	4	UDP	192.168.158.129	137	*	*	
System	4	UDP	192.168.158.129	138	*	*	
taskhsvc.exe	1916	TCP	127.0.0.1	9050	0.0.0.0	0	LISTENING
taskhsvc.exe	1916	TCP	127.0.0.1	49172	127.0.0.1	49173	ESTABLISHED
taskhsvc.exe	1916	TCP	127.0.0.1	49173	127.0.0.1	49172	ESTABLISHED
taskhsvc.exe	1916	TCP	192.168.158.129	49182	198.100.147.184	9001	ESTABLISHED

[그림 16] 로컬 9050 포트 Listening

Tor 프로세스는 9050 포트를 열고 접속 대기한다. 해당 포트는 랜섬웨어가 외부 통신을 할 경우 로컬 프록시 역할을 한다.

Time...	Process Name	PID	Operation	Path	Result	Detail
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 4, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 6, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 1, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 45, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 2, seqnum: 0, connid: 0
오후 5:...	@WanaDecryptor@...	1240	TCP Receive	127.0.0.1:49203 -> 127.0.0.1:9050	SUCCESS	Length: 1, seqnum: 0, connid: 0

[그림 17] Check Payment 실행 시의 Tor를 이용한 외부 서버와의 통신

랜섬노트에서 Check Payment 버튼을 눌렀을 때 Tor 프로세스가 생성한 프록시를 통해 외부 서버와 통신한다.

3. 대 응

1. 시스템을 네트워크와 분리 후 방화벽 설정에서 SMB 관련 포트를 차단한다.
   관련 포트 : 137, 138, 139, 445
2. MS에서 제공하는 보안 업데이트를 진행한다. (MS17-010)
   랜섬웨어의 전파는 SMB 취약점을 이용하는 것으로 취약점 발생의 원인이 되는 취약한 시스템에 대한 보안 업데이트를 진행하는 것이 근본적인 해결 방안이다.

   [Update Link] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

궁금하신 점이나 문의사항은 malware@somansa.com 으로 해주세요.