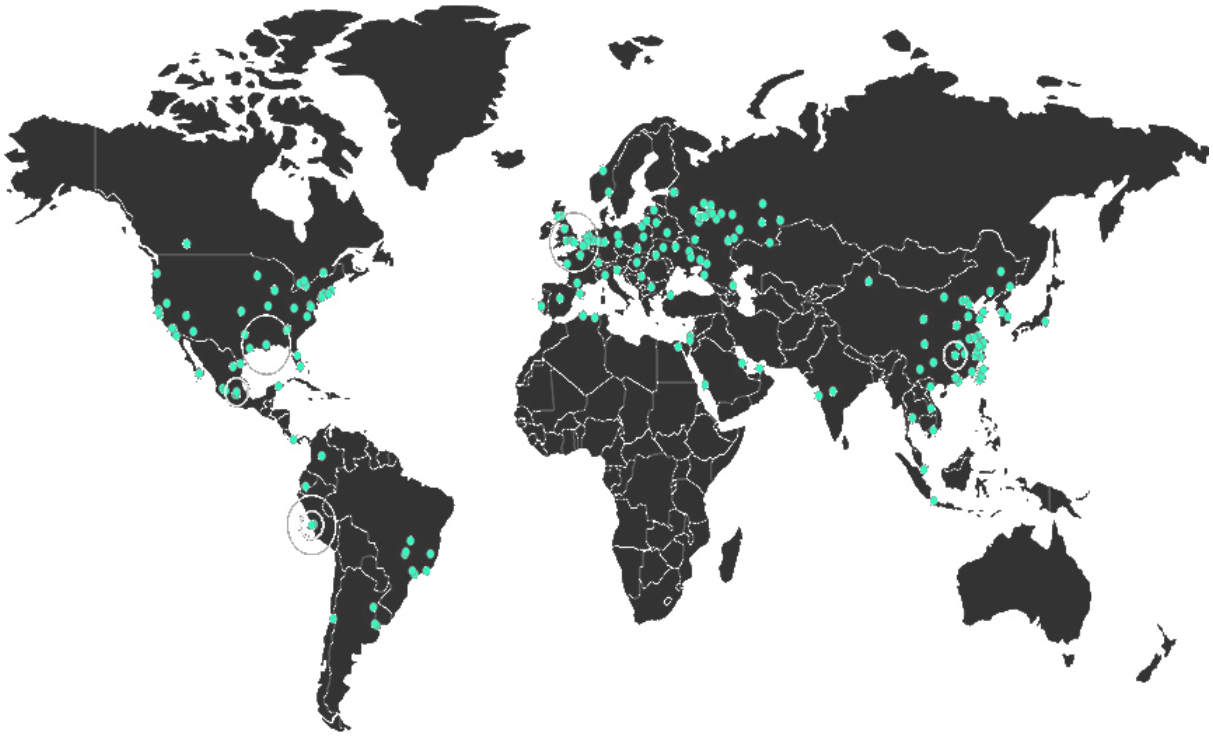
SOMANSA

No.09 | 2017년 05월

MALWARE ANALYSIS REPORT

No.9 | 2017 년 05 월

WannaCry 랜섬웨어 이슈 분석



(주) 소만사 악성코드 분석 센터

목 차

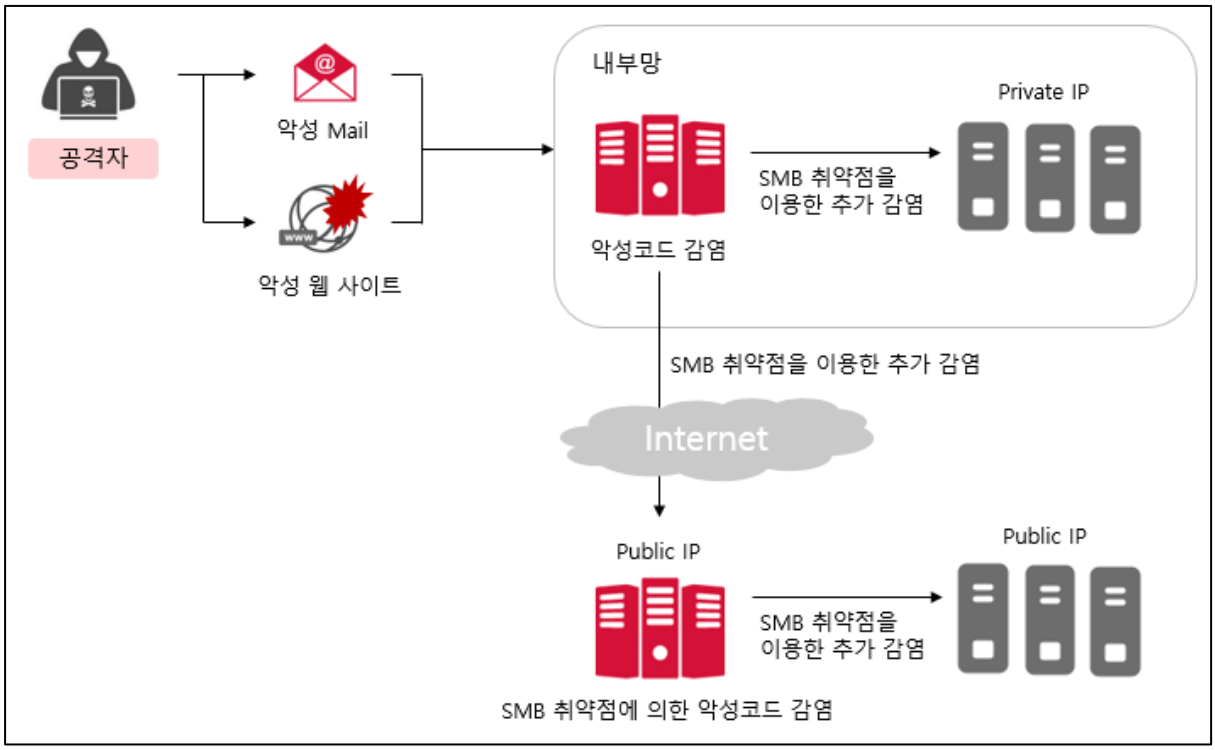
1. 개 요

1.1 배 경

SMBv2 원격코드 실행 취약점을 악용하여 확산되는 워너크라이(WannaCry) 랜섬웨어가 2017년 5월 12일 전 세계에서 감염이 보고되고 있다. 해당 랜섬웨어는 워너크립터(WannaCryptor), Wcrypt 등으로도 불리고 있으며, SMB(Server Message Block) 취약점을 이용하여 웜과 같이 다른 PC로 확산되어 추가 감염을 발생시키기 때문에 급속도로 피해가 심각해지고 있다. 이미 2017년 3월에 관련 취약점에 대한 보안 업데이트는 발표되었지만, 보안 업데이트가 적용되지 않은 시스템은 감염 위험에 노출되어 있기 때문에 피해 사례가 증가하고 있다.

2. 분 석

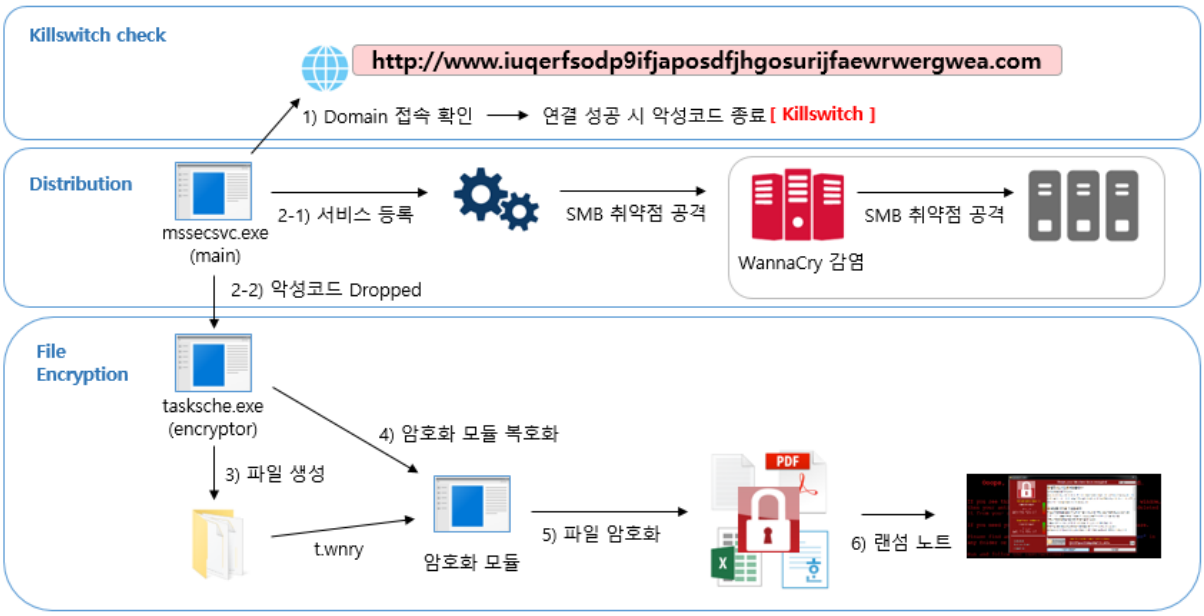
2.1 감염 경로



[그림 1] WannaCry 랜섬웨어 감염 경로

공격자가 악성 메일 및 악성 웹사이트를 이용하여 악성코드를 감염시키고 감염된 WannaCry 악성코드에서 SMB 프로토콜 취약점을 이용하여 동일 IP 대역 및 랜덤으로 생성된 IP를 대상으로 추가 감염을 발생시켜 확산된다.

2.2 WannaCry 랜섬웨어 분석



[그림 2] WannaCry 랜섬웨어 동작

WannaCry 랜섬웨어가 시스템에 감염되면 dropper인 mssecsvc.exe가 tasksche.exe를 생성하여 실행시키고, 자기 자신은 서비스로 등록하여 추가 감염 기능을 수행한다.

2.2.1. mssecsvc.exe (dropper)

```
qmemcpy(&szUrl, aHttpWww_iuqerf, 0x39u);      // http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
v8 = 0;
v9 = 0;
v10 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

[그림 3] Domain 접속 확인 (Killswitch)

악성코드가 실행되면 아래의 도메인으로 연결 시도하여 성공 시 프로세스가 종료된다.

- "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

해당 도메인은 WannaCry 랜섬웨어의 Killswitch 역할을 하고 있으며, 발견 초기에 도메인이 등록되어 악성코드의 확산이 차단되었다.

도메인에 연결 실패 시 악성 행위가 시작되며, 주요 동작은 크게 2가지로 나눌 수 있다.

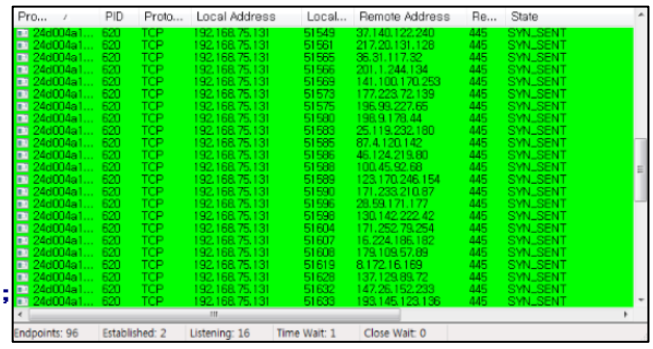
1) 서비스로 등록되어 SMB 취약점을 이용한 감염 확산

- 서비스 이름 : mssecsvc2.0
- 인 자 : -m security

서비스로 동작하게 되면 SMB 취약점을 이용한 감염 확산 루틴이 실행된다. 대상이 되는 IP에 SMB 패킷을 전송하여 취약점 발생을 유도한다.

```
v10 = sub_407660(v7) % 0xFFu;
v11 = sub_407660((void *)0xFF);
sprintf(&Dest, aD_D_D_D, v6, v19, v10, v11 % 0xFFu);// %d.%d.%d.%d -> random IP
v12 = inet_addr(&Dest);
if ( sub_407480(v12) > 0 )                    // connect to port 445
  break;
```

```
*(_WORD *)&name.sa_data[0] = htons(0x1BDu);   // port 445
v1 = socket(2, 1, 6);
v2 = v1;
if ( v1 == -1 )
{
  result = 0;
}
else
{
  ioctlsocket(v1, -2147195266, &argp);
  writefds.fd_array[0] = v2;
  writefds.fd_count = 1;
  timeout.tv_sec = 1;
  timeout.tv_usec = 0;
  connect(v2, &name, 16);
  v4 = select(0, 0, &writefds, 0, &timeout);
  closesocket(v2);
  result = v4;
```



[그림 4] 랜덤 IP 생성 후 SMB 포트(445)로 접속 시도

[대상 IP 및 Port]

- 로컬 시스템의 IP 대역 전체 및 랜덤으로 생성한 IP
- 445 Port

2) 파일 암호화 악성코드 생성

파일을 암호화하는 등의 추가 악성행위를 하는 악성코드를 내부 리소스에서 로드하여 파일로 생성 후 실행한다.

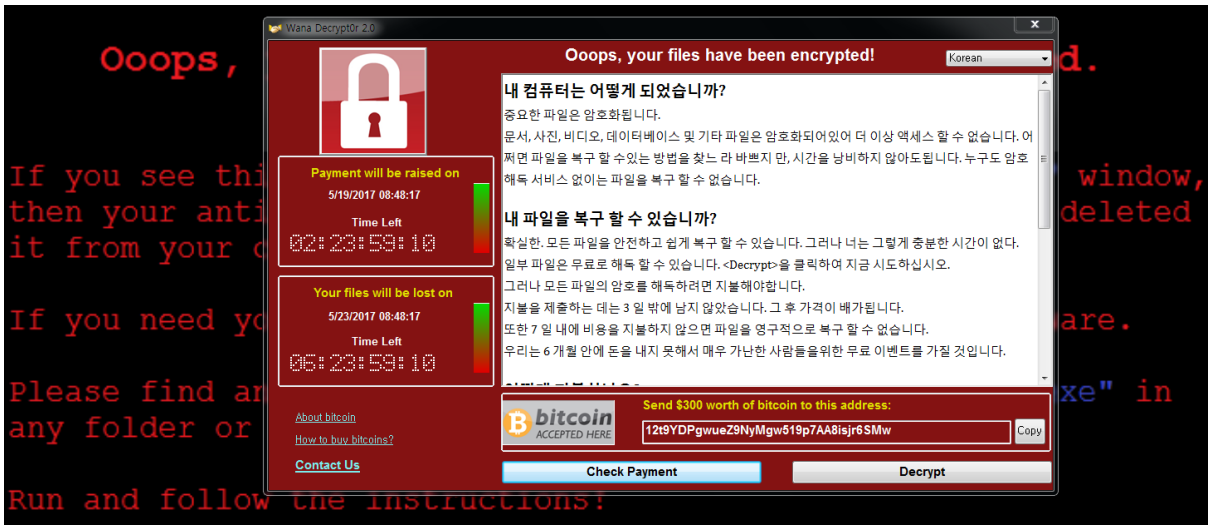
2.2.2. tasksche.exe

mssecsvc.exe에 의해 생성된 악성코드이다. 압축 형태로 되어 있으며 아래의 Password를 사용하여 리소스를 압축 해제하여 사용한다.

- Password : "WNcry@2ol7"

이름	수정한 날짜	유형	크기
msg	2017-05-14 오후...	파일 폴더	
b.wnry	2017-05-11 오후...	WNRY 파일	1,407KB
c.wnry	2017-05-11 오후...	WNRY 파일	1KB
r.wnry	2017-05-11 오후...	WNRY 파일	1KB
s.wnry	2017-05-09 오후...	WNRY 파일	2,968KB
t.wnry	2017-05-12 오전...	WNRY 파일	65KB
taskdl.exe	2017-05-12 오전...	응용 프로그램	20KB
taskse.exe	2017-05-12 오전...	응용 프로그램	20KB
u.wnry	2017-05-12 오전...	WNRY 파일	240KB

생성된 파일은 악성 행위 시 메모리에 로드하여 사용하며, msg 폴더에는 랜섬노트에 사용되는 언어별 메시지 파일이 존재한다.



파일 암호화가 완료되면 위와 같이 바탕화면을 변경하고, 랜섬노트를 실행한다.
랜섬노트는 총 28개 언어로 볼 수 있으며 300 달러 상당의 비트코인을 요구하고 있다.

[관련 취약점]

Windows SMB 원격코드 실행 취약점 (CVE-2017-0143)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0144)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0145)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0146)
Windows SMB 정보 유출 취약점 (CVE-2017-0147)
Windows SMB 원격코드 실행 취약점 (CVE-2017-0148)

(관련 취약점에 대한 자세한 내용은 상세 분석 후 제공 예정)

[영향 받는 시스템]

Windows 10
Windows 8.1
Windows RT 8.1
Windows 7
Windows Vista
Windows XP
Windows Server 2016
Windows Server 2012R2
Windows Server 2012
Windows Server 2008R2
Windows Server 2008
Windows Server 2003

[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

3. 대 응

1. 시스템을 네트워크와 분리 후 방화벽 설정에서 SMB 관련 포트를 차단한다.
   관련 포트 : 137, 138, 139, 445
2. C&C 서버 리스트의 IP를 차단하여 추가적인 악성행위를 예방한다.
   해당 C&C IP는 WebKeeper DB의 차단 대상 IP로 실시간 반영

	C&C 서버		C&C 서버
1	62.138.10.60:9001	14	2.3.69.209:9001
2	82.94.251.227:443	15	146.0.32.144:9001
3	213.239.216.222:443	16	50.7.161.218:9001
4	51.255.41.65:9001	17	217.79.179.77
5	86.59.21.38:443	18	128.31.0.39
6	198.199.64.217:443	19	213.61.66.116
7	83.169.6.12:9001	20	212.47.232.237
8	192.42.115.102:9004	21	81.30.158.223
9	104.131.84.119:443	22	79.172.193.32
10	178.254.44.135:9001	23	89.45.235.21
11	163.172.25.118:22	24	38.229.72.16
12	188.166.23.127:443	25	188.138.33.220
13	193.23.244.244:443		

3. MS에서 제공하는 보안 업데이트를 진행한다. (MS17-010)
4. 사용중인 소프트웨어 최신 업데이트 유지한다.
5. 백신 최신 업데이트 유지한다.
6. 주요 문서는 주기적으로 백업하고 물리적으로 분리하여 관리한다.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 해주세요.