Analysis Report

워너크립터 랜섬웨어 분석 보고서

Trojan/Win32.WannaCryptor 상세 분석

안랩 시큐리티대응센터(ASEC) 분석팀

AhnLab

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

01. 개요

워너크립터(WannaCryptor) 랜섬웨어(Ransomware)는 워너크라이(WannaCry), W크립트(Wcrypt) 등으로도 불리며, 지난 2017년 5월 12일(현지 시간) 스페인, 영국 등을 시작으로 전 세계에서 감염이 보고되고 있다.[1][2]

워너크립터가 최초 발견된 것은 지난 2017년 2월이다. 이번 워너크립터는 지난 2017년 5월 제작된 변종으로, 악성코드 제작자는 지난 2017년 4월 해킹 그룹 쉐도우브로커(ShadowBrokers)가 탈취한 미국 국가안보국(NSA)의 이터널블루(EternalBlue)를 이용해 변종을 제작했다. 이터널블루는 윈도우(Windows) 운영체제(OS)의 SMB(Server Message Block) 취약점(MS17-010)[3]을 이용하는 익스플로잇 킷(Exploit Kit)이다. 마이크로소프트사는 지난 2017년 3월 해당 SMB 취약점에 대한 보안 업데이트를 배포했으나, 상당수의 시스템에 해당 보안 업데이트가 적용되지 않아 위험에 노출되었다.

이번 워너크립터는 2017년 5월 12일 전세계로 확산되었으며, 2017년 5월 17일 현재 약 500개 이상(안랩 위협분석 시스템 ASD 분석 기준)의 변형이 발견되었다.

본 보고서에서 분석한 워너크립터 랜섬웨어 샘플 정보는 [표 1]과 같다.

	MD5	파일명	크기	기능
1	DB349B97C37D22F5EA1D1841E3C89EB4	mssecsvc.exe	3,723,264	드로퍼, SMB취약점 전파
2	84C82835A5D21BBCF75A61706D8AB549	tasksche.exe	3,514,368	파일 암호화

[표 1] 워너크립터 샘플 정보

[1] http://www.bbc.com/news/technology-39901382

[2] http://varlamov.ru/2370148.html

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

02. 감염 경로

대부분의 랜섬웨어는 이메일 첨부 파일이나 취약한 홈페이지 방문 시 감염되는데, 특히 워너크립터 랜섬웨어는 윈도우 취약점(MS17-010, SMB 원격코드실행 취약점)을 이용해 유포되어 피해가 더욱 확산되었다. 관련 보안 업데이트가 적용되지 않은 윈도우 시스템의 경우, 인터넷만 연결되어 있으면 별도의 사용자 동작 없이도 감염될 수 있기 때문이다.

워너크립터 랜섬웨어 유포와 관련된 윈도우 SMB 취약점은 [표 2]와 같다.

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

[표 2] 워너크립터 유포 관련 SMB 취약점 정보

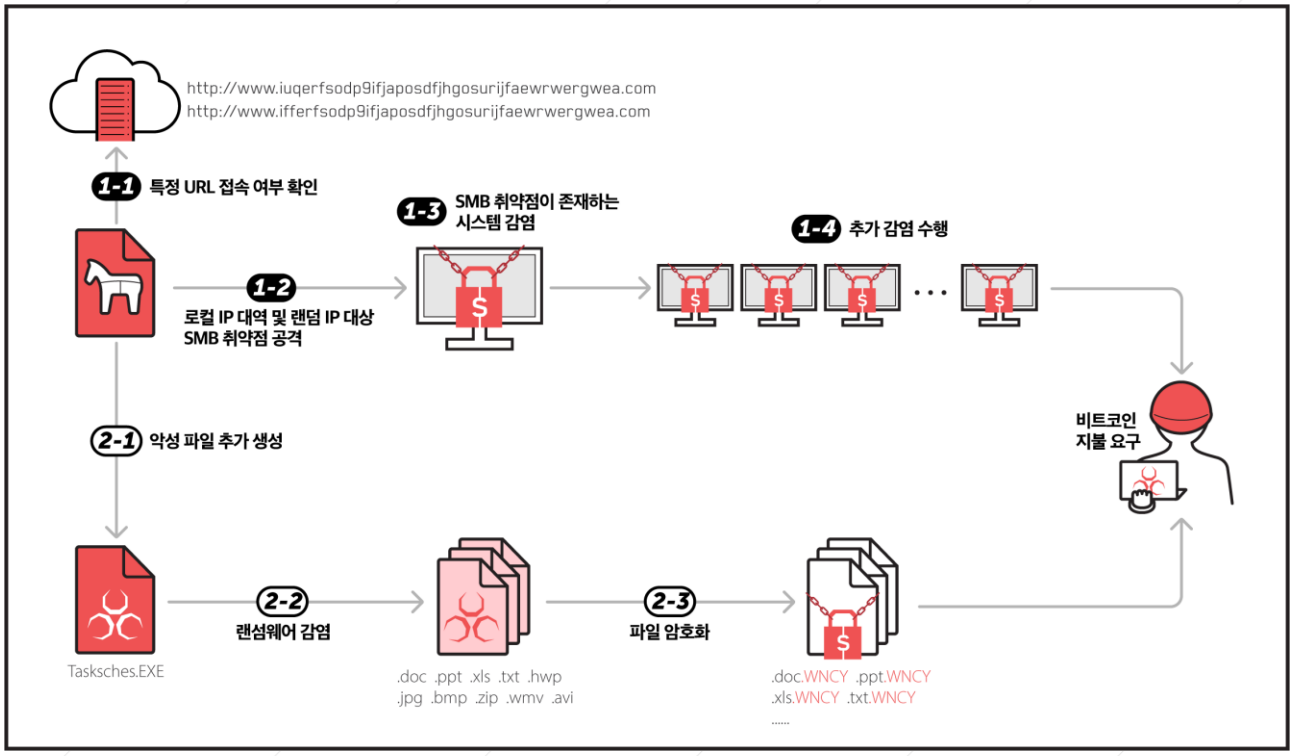
SMB 취약점에 영향을 받는 운영체제는 [표 3]과 같다. 단, 윈도우 10의 경우 해당 취약점을 갖고 있으나 워너크립터의 공격 대상은 아니다.

Windows XP/ Vista/ 7/ 8.1/ RT 8.1
Windows 10 (해당 취약점을 갖고 있으나 워너크립터의 공격 대상은 아님)
Windows Server 2003/ 2008 R2 SP1, SP2/ 2012 R2/ 2016

[표 3] SMB 취약점에 영향 받는 운영체제

03. 워너크립터 동작 방식

[그림 1]은 워너크립터 랜섬웨어의 동작 과정을 정리한 것이다.



[그림 1] 워너크립터 동작 과정

1) 동작 과정 상세 분석

(1-1) 특정 URL 접속 여부 확인

워너크립터 랜섬웨어가 실행되면 아래의 URL로 접속을 시도하며, 접속에 실패할 경우에만 다음 동작을 수행한다. 이는 백신의 행위기반 탐지를 피하기 위해 감염된 PC 환경이 가상이 아닌 실제인지 확인하는 과정이다. 2017년 현재, 아래 URL 외에 다른 URL에 접속을 시도하는 변형들이 추가로 발견되고 있다.

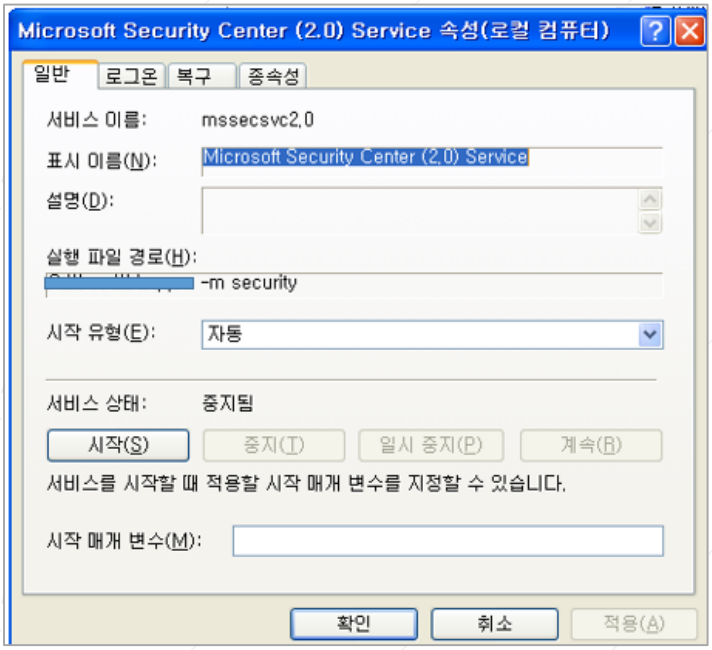
- http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

[그림 2]는 URL 접속 여부를 확인하는 실행 코드이다.

```
00408140  r$ 83EC 50      SUB ESP,50
00408143  . 56            PUSH ESI
00408144  . 57            PUSH EDI
00408145  . B9 0E000000   MOV ECX,0E
0040814A  . BE D0134300   MOV ESI,mssecsvc.004313D0                ASCII "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
0040814F  . 8D7C24 08     LEA EDI,DWORD PTR SS:[ESP+8]
00408153  . 33C0          XOR EAX,EAX
00408155  . F3:A5         REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]
00408157  . A4            MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
00408158  . 894424 41     MOV DWORD PTR SS:[ESP+41],EAX
0040815C  . 894424 45     MOV DWORD PTR SS:[ESP+45],EAX
00408160  . 894424 49     MOV DWORD PTR SS:[ESP+49],EAX
00408164  . 894424 4D     MOV DWORD PTR SS:[ESP+4D],EAX
00408168  . 894424 51     MOV DWORD PTR SS:[ESP+51],EAX
0040816C  . 66:894424 55  MOV WORD PTR SS:[ESP+55],AX
00408171  . 50            PUSH EAX
00408172  . 50            PUSH EAX
00408173  . 50            PUSH EAX
00408174  . 6A 01         PUSH 1
00408176  . 50            PUSH EAX
00408177  . 884424 6B     MOV BYTE PTR SS:[ESP+6B],AL
0040817B  . FF15 34A14000 CALL DWORD PTR DS:[<&WININET.InternetOpenA>]   WININET.InternetOpenA
00408181  . 6A 00         PUSH 0
00408183  . 68 00000084   PUSH 84000000
00408188  . 6A 00         PUSH 0
```

[그림 2] URL 접속 여부 확인 코드

또한 시스템이 시작될 때마다 자동으로 실행되도록 정상 서비스로 위장하여 시스템에 스스로를 등록한다. 마이크로소프트의 정상 서비스명과 유사한 "mssecsvc2.0" 형태로 위장하며, 서비스로 동작할 때 "-m security" 인자로 실행된다. [그림 3]은 해당 서비스 정보이다.



[그림 3] 최초 동작 시 등록하는 서비스 정보

(1-2) 로컬 IP 대역 및 랜덤 IP 대상 SMB 취약점 공격

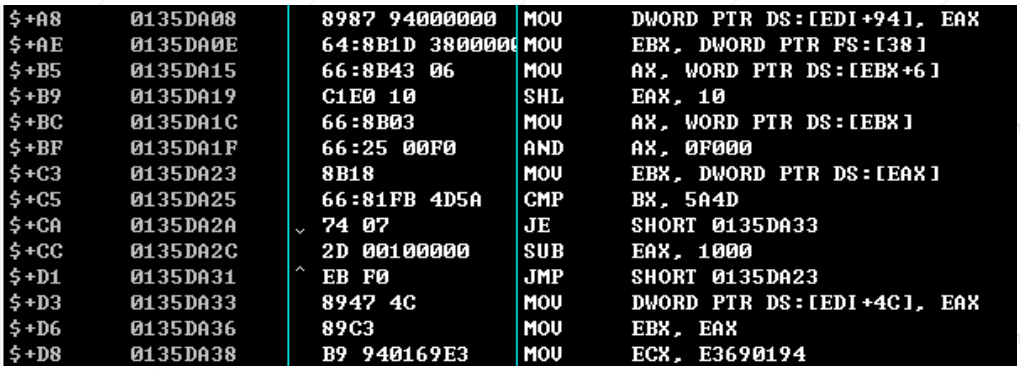
서비스로 동작하게 되면 SMB 취약점을 이용한 자체 유포 루틴이 수행된다. 자신의 네트워크 대역 IP 및 랜덤으로 생성한 IP 대역을 스캔하여 SMB 패킷(445포트)을 전송한다. 이 과정에서 과도한 패킷이 발생하여 네트워크에 트래픽 부하가 발생할 수 있다.

(1-3) SMB 취약점이 존재하는 시스템 감염

IP 스캐닝을 통해 공격 대상 시스템을 찾아 SMB 취약점 발생을 유발하는 패킷을 추가로 전송한다. [그림 4]와 같이 SMB 취약점을 이용한 원격 실행 코드를 SMB 패킷 헤더에 삽입한 형태의 데이터를 생성하며, 공격 대상 시스템의 운영체제에 관련 보안 패치가 적용되지 않은 환경일 경우 쉘코드가 동작한다.

[그림 4] SMB 원격 실행 코드 취약점 발생 유발 패킷

[그림 5]는 취약점 발생 이후 실행되는 쉘코드에 포함된 내용이다.



[그림 5] SMB 취약점 발생 후 실행되는 쉘코드

(1-4) 추가 감염 수행

워너크립터 랜섬웨어는 최초 감염 시스템에서 실행된 후 다시 SMB 취약점을 통해 유포를 수행하기 때문에 감염 시스템이 증가할 우려가 있다.

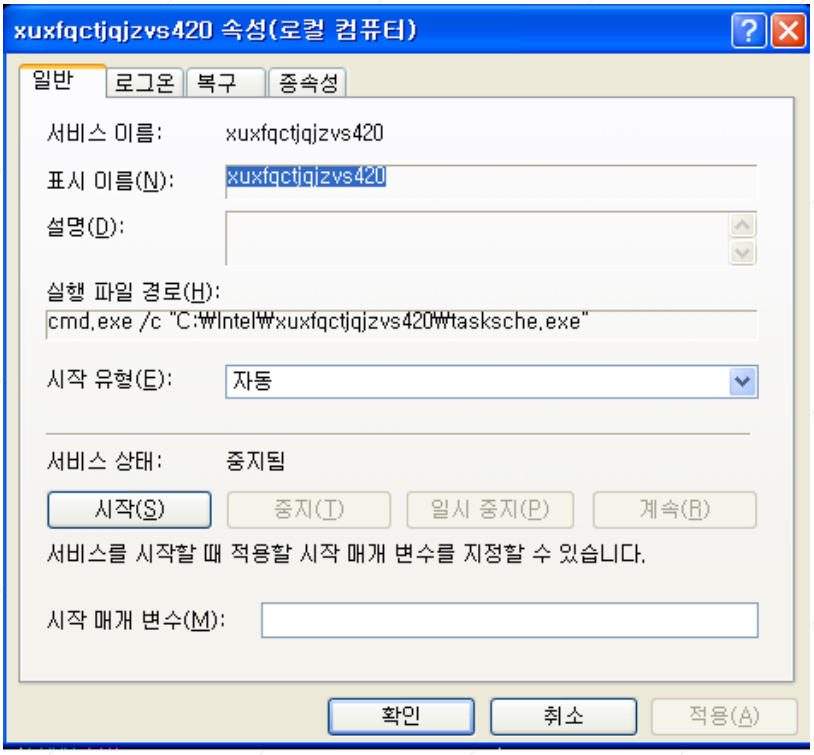
(2-1) 악성 파일 추가 생성

워너크립터 랜섬웨어는 최초 실행 후 시스템에 존재하는 다음 경로 중 한 곳에 추가로 악성 파일을 생성한다. 단, 파일 생성 경로는 윈도우 버전에 따라 상이할 수 있다. 생성하는 폴더명의 [Random] 부분은 시스템 정보를 조합하여 생성한 유니크한 값이다.

- C:₩ProgramData₩[Random]₩tasksche.exe
- C:₩Intel₩[Random]₩tasksche.exe
- C:₩Windows₩tasksche.exe
- C:₩User₩(사용자명)₩AppData₩Local₩Temp₩[Random]₩tasksche.exe

2) 감염 증상

실제 랜섬웨어 행위를 수행하는 것은 추가로 생성된 tasksche.exe 파일이며, 드로퍼에 의해 "/i" 인자를 이용해 인스톨(Install) 모드로 실행된다. "/i" 인자로 최초 실행될 때 [그림 6]과 같이 서비스로 등록된다. 서비스명은 해당 파일이 존재하는 랜덤한 폴더명을 사용한다.



[그림 6] 실제 랜섬웨어 행위를 수행하는 tasksche.exe 파일의 서비스 등록 정보

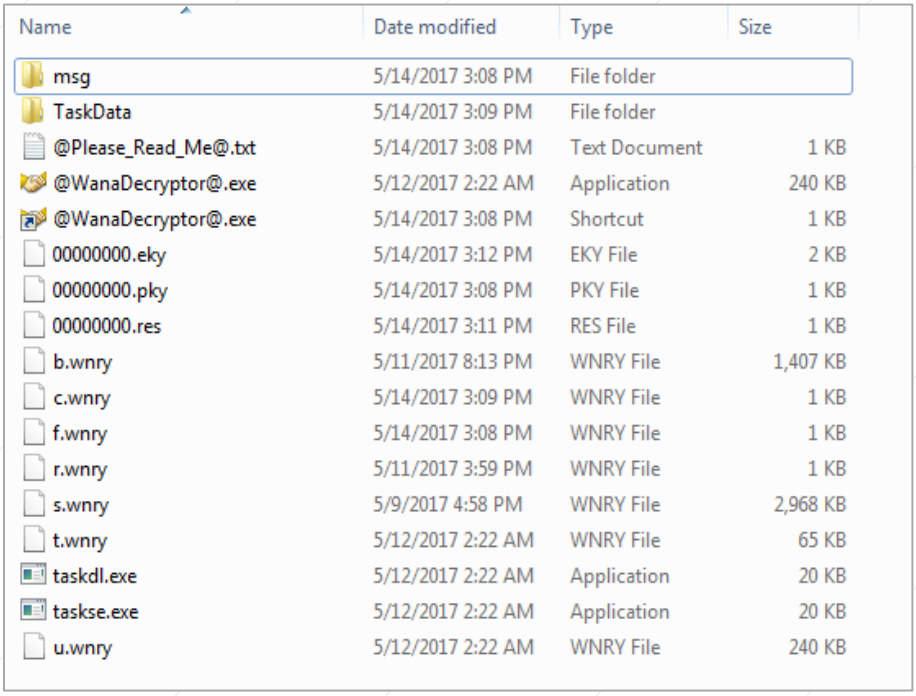
이후 서비스로 동작하면서 동일한 경로에 [표 4]와 같은 파일을 추가로 생성하며, 숨김 속성을 ("attrib +h .") 부여한다.

파일명	파일 기능
b.wnry	파일 암호화 후 바탕화면으로 설정되는 이미지 파일
c.wnry	tor 관련 설정 파일 (접속 URL, 다운로드 URL)
f.wnry	샘플로 복호화할 파일 목록 저장

r.wnry	readme.txt
s.wnry	tor 모듈 ZIP 압축 파일
t.wnry	암호화된 암호화 모듈
u.wnry	비트코인 결재를 유도하는 @WanaDecryptor@.exe 프로그램과 동일한 파일
taskdl.exe	암호화 모듈에서 사용하는 내부 프로그램
taskse.exe	암호화 모듈에서 사용하는 내부 프로그램
00000000.pky	공개키 파일
00000000.eky	암호화된 개인키 파일

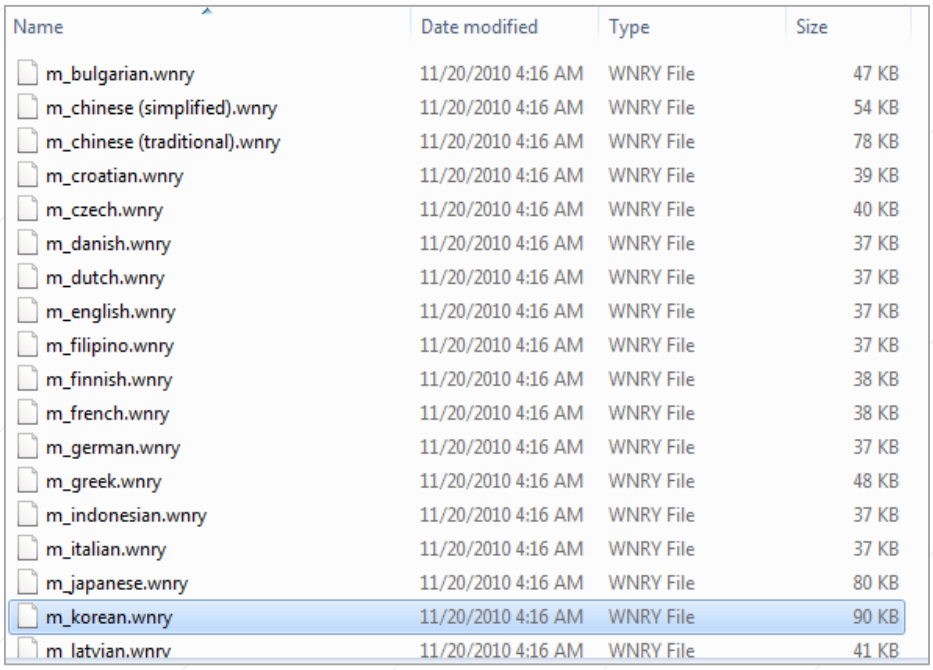
[표 4] tasksche.exe가 생성하는 파일 목록

생성된 파일 목록은 [그림 7] 과 같다.



[그림 7] tasksche.exe가 생성하는 파일 목록 (2)

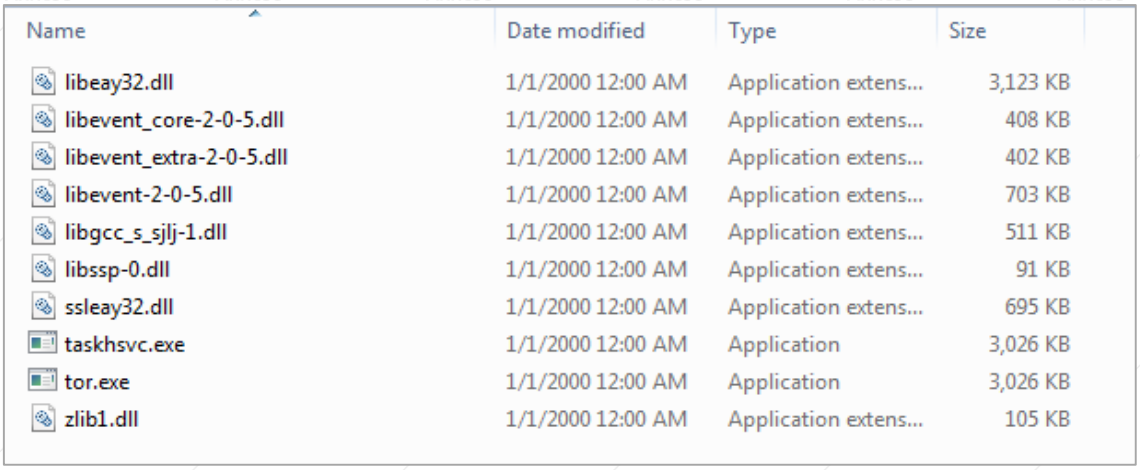
msg 폴더에는 [그림 8]와 같이 랜섬노트로 출력할 28개 언어의 메시지 파일을 생성한다.



Name	Date modified	Type	Size
m_bulgarian.wnry	11/20/2010 4:16 AM	WNRY File	47 KB
m_chinese (simplified).wnry	11/20/2010 4:16 AM	WNRY File	54 KB
m_chinese (traditional).wnry	11/20/2010 4:16 AM	WNRY File	78 KB
m_croatian.wnry	11/20/2010 4:16 AM	WNRY File	39 KB
m_czech.wnry	11/20/2010 4:16 AM	WNRY File	40 KB
m_danish.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_dutch.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_english.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_filipino.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_finnish.wnry	11/20/2010 4:16 AM	WNRY File	38 KB
m_french.wnry	11/20/2010 4:16 AM	WNRY File	38 KB
m_german.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_greek.wnry	11/20/2010 4:16 AM	WNRY File	48 KB
m_indonesian.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_italian.wnry	11/20/2010 4:16 AM	WNRY File	37 KB
m_japanese.wnry	11/20/2010 4:16 AM	WNRY File	80 KB
m_korean.wnry	11/20/2010 4:16 AM	WNRY File	90 KB
m_latvian.wnry	11/20/2010 4:16 AM	WNRY File	41 KB

[그림 8] msg 폴더에 생성하는 언어별 랜섬노트 파일 목록

TaskData 폴더에는 [그림 9]과 같이 토르(Tor) 네트워크 관련 파일을 생성한다. 추적을 어렵게 하기 위해 온라인 상에서 익명을 보장하는 토르 네트워크를 이용한 것이다.



Name	Date modified	Type	Size
libeay32.dll	1/1/2000 12:00 AM	Application extens...	3,123 KB
libevent_core-2-0-5.dll	1/1/2000 12:00 AM	Application extens...	408 KB
libevent_extra-2-0-5.dll	1/1/2000 12:00 AM	Application extens...	402 KB
libevent-2-0-5.dll	1/1/2000 12:00 AM	Application extens...	703 KB
libgcc_s_sjlj-1.dll	1/1/2000 12:00 AM	Application extens...	511 KB
libssp-0.dll	1/1/2000 12:00 AM	Application extens...	91 KB
ssleay32.dll	1/1/2000 12:00 AM	Application extens...	695 KB
taskhsvc.exe	1/1/2000 12:00 AM	Application	3,026 KB
tor.exe	1/1/2000 12:00 AM	Application	3,026 KB
zlib1.dll	1/1/2000 12:00 AM	Application extens...	105 KB

[그림 9] TaskData 폴더에 생성하는 토르(Tor) 파일

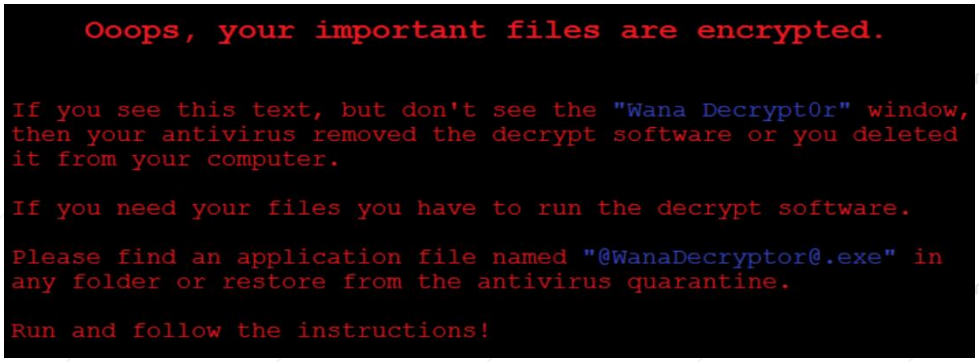
워너크립터는 감염된 시스템 내의 [표 5]의 확장자를 가진 파일을 암호화한 후, 확장자에 .WNCRY를 추가한다.

.der	.pfx	.key	.crt	.csr
.p12	.pem	.odt	.ott	.sxw
.stw	.uot	.3ds	.max	.3dm
.ods	.ots	.sxc	.stc	.dif
.slk	.wb2	.odp	.otp	.sxd

.std	.uop	.odg	.otg	.sxm
.mml	.lay	.lay6	.asc	.sqlite3
.sqllitedb	.sql	.accdb	.mdb	.db
.dbf	.odb	.frm	.myd	.myi
.ibd	.mdf	.ldf	.sln	.suo
.cs	.c	.cpp	.pas	.h
.asm	.js	.cmd	.bat	.ps1
.vbs	.vb	.pl	.dip	.dch
.sch	.brd	.jsp	.php	.asp
.rb	.java	.jar	.class	.sh
.mp3	.wav	.swf	.fla	.wmv
.mpg	.vob	.mpeg	.asf	.avi
.mov	.mp4	.3gp	.mkv	.3g2
.flv	.wma	.mid	.m3u	.m4u
.djvu	.svg	.ai	.psd	.nef
.tiff	.tif	.cgm	.raw	.gif
.png	.bmp	.jpg	.jpeg	.vcd
.iso	.backup	.zip	.rar	.7z
.gz	.tgz	.tar	.bak	.tbk
.bz2	.PAQ	.ARC	.aes	.gpg
.vmx	.vmdk	.vdi	.sldm	.sldx
.sti	.sxi	.602	.hwp	.snt
.onetoc2	.dwg	.pdf	.wk1	.wks
.123	.rtf	.csv	.txt	.vsdx
.vsd	.edb	.eml	.msg	.ost
.pst	.potm	.potx	.ppam	.ppsx
.ppsm	.pps	.pot	.pptm	.pptx
.ppt	.xltm	.xltx	.xlc	.xlm
.xlt	.xlw	.xlsb	.xlsm	.xlsx
.xls	.dotx	.dotm	.dot	.docm
.docb	docx	.doc		

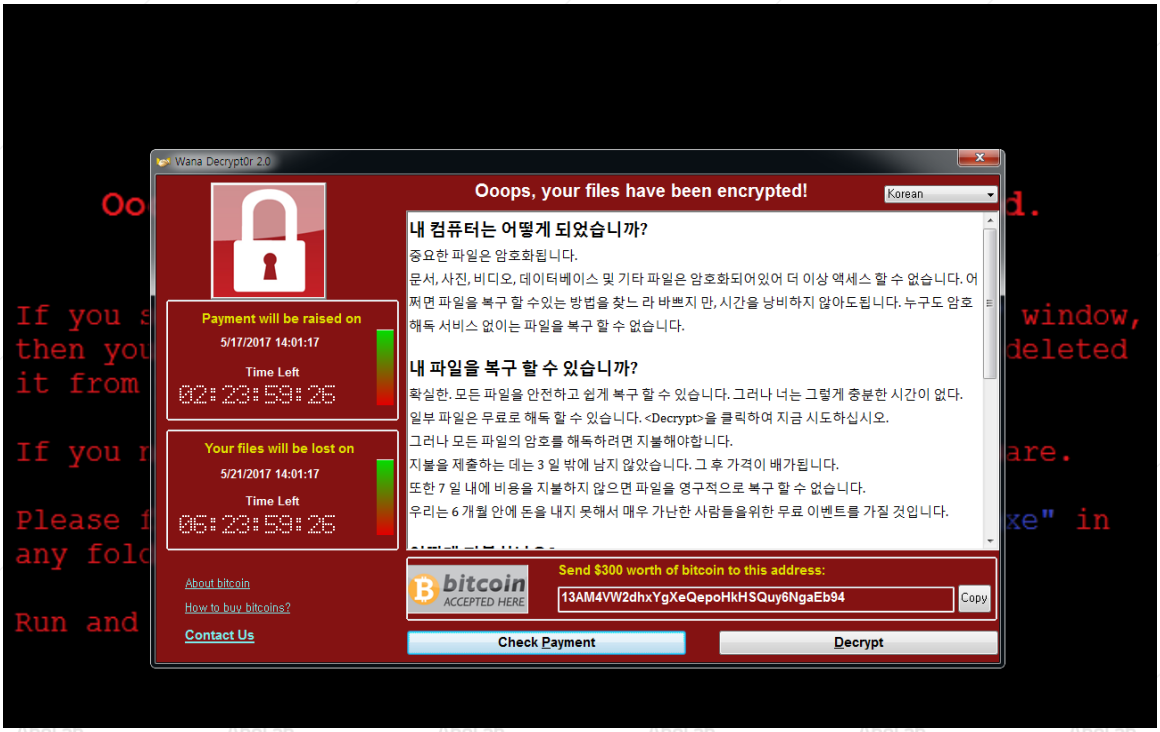
[표 5] 워너크립터 감염 대상 확장자 목록

파일을 암호화한 후 바탕화면을 [그림 10]과 같이 변경하여 사용자에게 랜섬웨어 감염 사실을 알린다.



[그림 10] 파일 암호화 후 변경하는 바탕화면 이미지

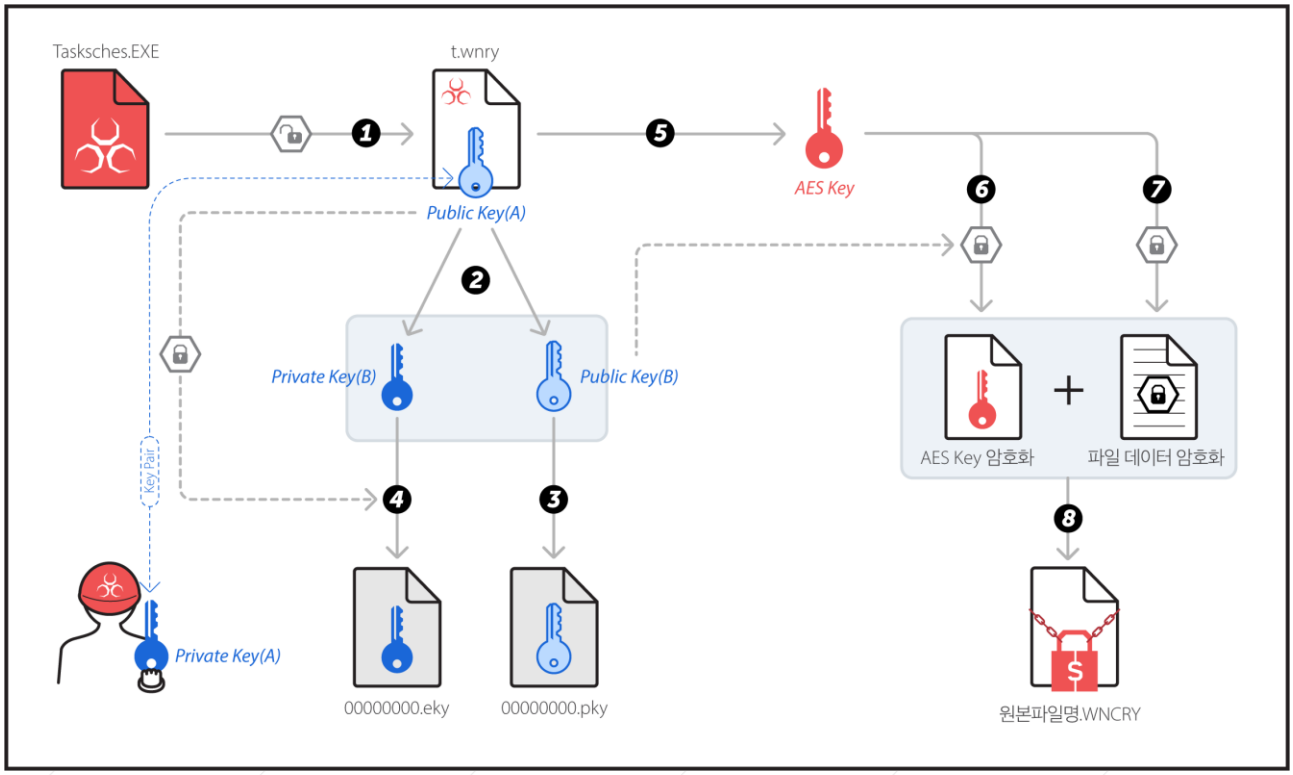
이후 [그림 11]와 같이 암호화된 파일 복구를 위해 300 달러 상당의 비트코인(Bitcoin)을 요구하는 랜섬노트를 노출한다. 랜섬노트는 28개 언어로 제공된다.



[그림 11] 한글을 지원하는 워너크립터 랜섬노트

3) 파일 암호화 및 복호화 방식

tasksche.exe 파일을 이용해 암호화 모듈인 t.wnry 파일을 복호화하고 이를 자신의 메모리에 로드하여 암호화를 진행한다. 암호화 방식은 [그림 12]과 같다.



[그림 12] 워너크립터 랜섬웨어 암호화 과정

❶ tasksche.exe 파일에 의해 복호화되어 실행되는 t.wnry 파일 내부에 공개키(Public Key A) 존재

❷ 파일을 암호화하기 전에 RSA 공개키/개인키(Private Key) 생성 (감염 시스템마다 다른 키 생성)

❸ 공개키 B는 00000000.pky 파일에 저장되며, 이후 파일을 암호화할 때 마다 해당 키를 읽어서 암호화 과정에 사용

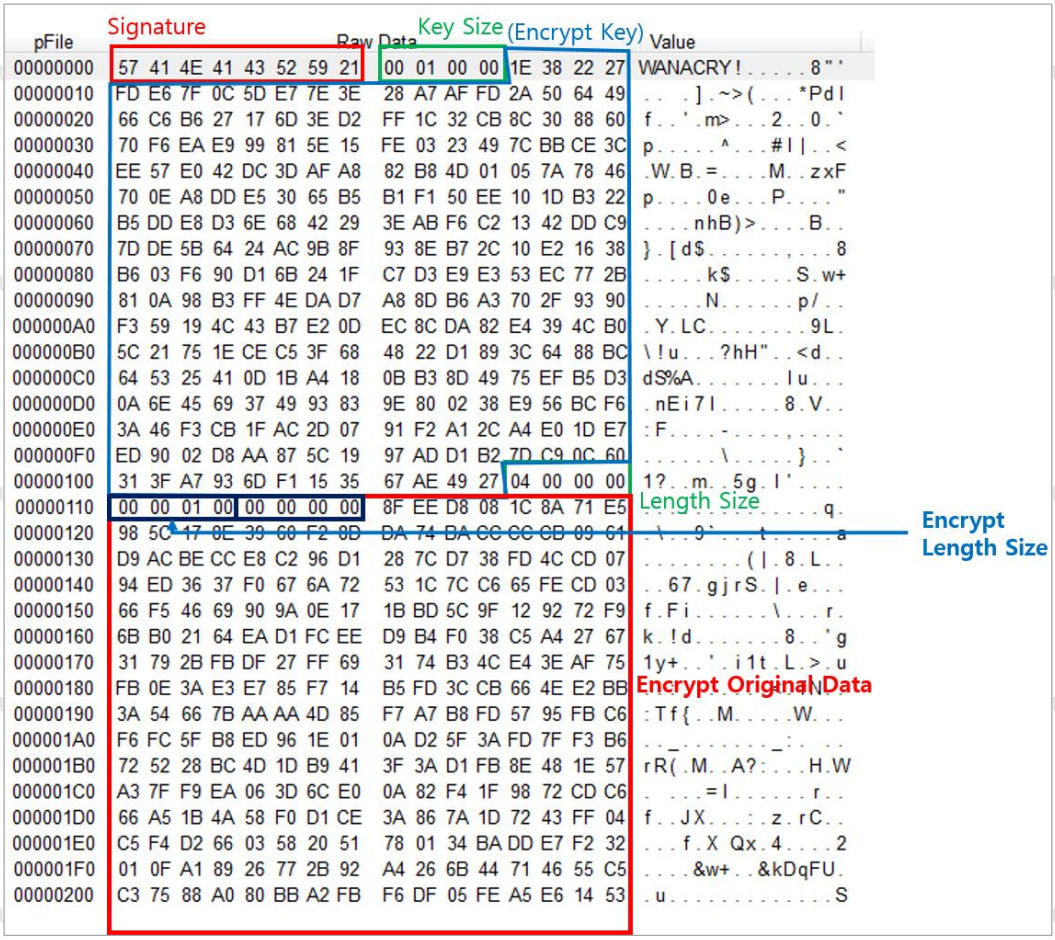
❹ 개인키 B는 공개키 A에 의해 암호화되어 00000000.eky 파일에 저장됨

❺ 파일별로 암호화할 때 마다 AES 키를 생성하는데, 이때 AES_128 CBC 방식으로 암호화되며 이때 사용되는 키는 랜덤하게 생성됨

❻❼ 랜덤한 AES 키를 이용하여 파일을 암호화하고, 랜덤한 AES 키는 공개키 B에 의해 암호화됨

❽ 암호화된 AES 키와 파일 암호화 데이터를 시그니처, 사이즈 정보와 조합하여 '원본 파일명.WNCRY' 파일을 생성

이렇게 암호화된 파일들의 구조는 [그림 13]와 같다.

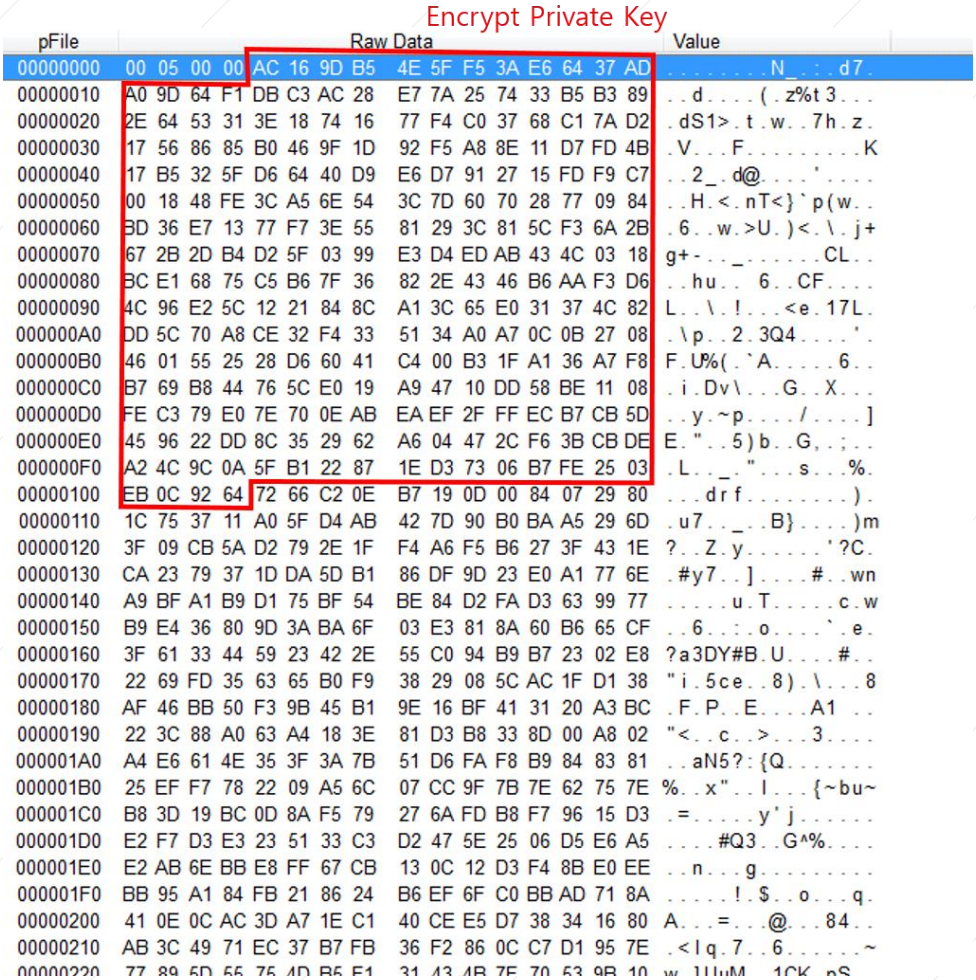


[그림 13] 암호화된 파일의 구조 (예시: t.wnry 파일)

암호화된 파일들은 다음과 같은 구조로 구성되어 있다.

- "WANACRY!" 시그니처
- AES 키 암호화 크기
- AES 키 암호화
- Key Size Length
- 원본 파일 Length
- 암호화된 파일 데이터

한편, 00000000.eky 파일은 [그림 14]와 같은 구조를 갖고 있다.



[그림 14] 암호화된 개인키 파일 구조

해당 키 파일은 처음 4바이트(Byte)를 제외하고는 RSA 개인키 B를 암호화하여 저장한 파일이다. 해당 파일을 복호화하면 암호화된 파일에 존재하는 AES 키 파일을 얻을 수 있으며, 파일 복호화에 사용할 수 있다.

암호화된 파일의 복호화 과정은 다음과 같다.

(1) 공격자가 갖고 있는 개인키 A 값을 이용하여 00000000.eky 파일에서 개인키 B 추출

(2) 개인키 B를 이용하여 각 파일들에 암호화 되어있는 AES 키 획득

(3) AES 키를 이용해 [그림 14]의 암호화된 파일 데이터 부분에 존재하는 원본 파일에 대한 복호화 진행

현재 워너크립터에 의해 암호화된 파일을 복호화하기 위해서는 반드시 개인키 A가 필요하다. 개인키 A는 공격자가 갖고 있으며, 해당 키 없이는 파일 복호화가 불가능하다.

04. 안랩 대응 현황

현재 안랩 제품별로 아래와 같은 기능을 통해 워너크립터 랜섬웨어를 진단 및 제거할 수 있다.

1. V3 제품군

- 워너크립터 진단 및 제거 (진단명: Trojan/Win32.WannaCryptor.xxxxxxxx)
- '자동 업데이트 적용' 시 최신 엔진 유지
- '실시간 검사 기능' 사용 가능
- MS 윈도우 최신 보안 패치 적용

2. AhnLab MDS

- 워너크립터 행위 탐지 (Suspicious/MDP.Behavior, Malware/MDP.Create)
- MDS 에이전트의 실행 보류(Execution Holding) 기능을 이용한 해당 악성코드의 실행 보류 및 분석/차단
- MS 윈도우 최신 보안 패치 적용

3. AhnLab TrusLine / AhnLab EPS

- 'Lock 모드 운영 상태'일 경우 워너크립터가 실행되지 않음

4. AhnLab Patch Management

- 중앙 제어에 통해 MS 윈도우 보안 패치 적용 가능
- 안랩의 자체 패치랩(Patch lab)을 통해 2017년 3월 및 5월 보안 패치 지원 (* 폐쇄망 환경용 업데이트 완료)
- 3월 보안 패치 제공 (지난 3월 적용 조치 완료)
- 5월 보안 패치 (MS 서비스 중단 OS의 패치 지원: Windows XP/ 8, Windows Server 2003 대상 패치)
- 해당 패치 적용 시 시스템 재시작 필요

5. AhnLab TrusGuard / AhnLab TrusGuard IPX

- 이터널블루(EternalBlue) 취약점 및 워너크립터 행위 차단

또한 안랩은 워너크립터로 인한 추가 피해가 발생하지 않도록 안랩 홈페이지를 통해 '안랩 워너크립터 사전 예방 툴'을 무료로 배포하고 있다. 이 툴은 워너크립터가 악용하는 보안 취약점(MS17-010)이 시스템에 존재하는지 확인하고, 악용되는 프로토콜(SMB)을 비활성화하여 워너크립터에 감염되는 것을 예방하는 프로그램이다. 이 외에도 ASEC 블로그, 랜섬웨어 보안센터를 통해 워너크립터 분석정보를 비롯해 최신 동향, 대응 가이드, 감염 예방을 위한 보안 수칙 등 랜섬웨어와 관련된 다양한 정보를 제공하고 있다.