ASEC Report

Vol.87

2017년 2분기

AhnLab

ASEC REPORT

VOL.87 2017년 2분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티 대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2017년 2분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 재프 랜섬웨어, 제2의 록키되나

보안 이슈

Security Issue

재프 랜섬웨어, 제2의 록키되나

지난 2017년 5월 안랩은 클라우드 기반의 악성코드 위협 분석 및 대응 시스템인 ASD(AhnLab Smart Defense)를 통해 재프(Jaff) 랜섬웨어가 국내에 급속도로 유포되고 있는 정황을 포착했다.

지난 5월에 발견된 재프 랜섬웨어는 네커스(Necurs) 봇넷을 이용한 스팸 메일을 통해 유포된 랜섬웨어로 전 세계 600만대 이상의 PC를 감염시키며 막대한 피해를 입혔다. 네커스 봇넷은 금융 정보 탈취 악성코드인 드라이덱스(Dridex)와 록키(Locky) 랜섬웨어 유포에 활용되었던 스팸 봇넷으로 알려져 있다. 이에 국내외 보안 업체들은 새로운 록키 랜섬웨어의 등장, 세대를 교체한 록키 랜섬웨어 등 여러 가능성을 제기하고 있다.

재프 랜섬웨어는 2017년 2분기에 새롭게 등장했지만 스팸 메일을 통해 불특정 다수에게 동시다발적으로 유포되어 꾸준히 감염 피해가 이어졌다. 이와 관련해 재프 랜섬웨어의 동작 과정, 그리고 일련의 암호화 과정 등을 상세히 살펴본다.

1. 유포 방식

먼저 재프 랜섬웨어가 유포되어 사용자 PC를 감염시키는 일련의 과정을 살펴보자. 재프 랜섬웨어는 [그림 1-1]과 같이 네커스 봇넷을 이용한 악

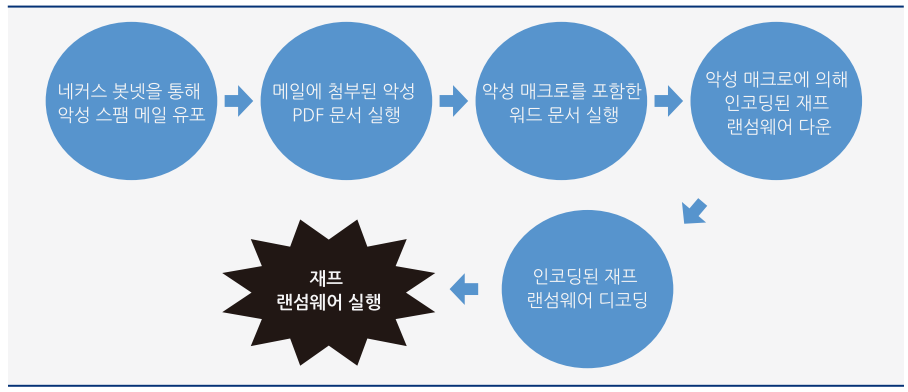


그림 1-1 | 재프 랜섬웨어의 유포 과정

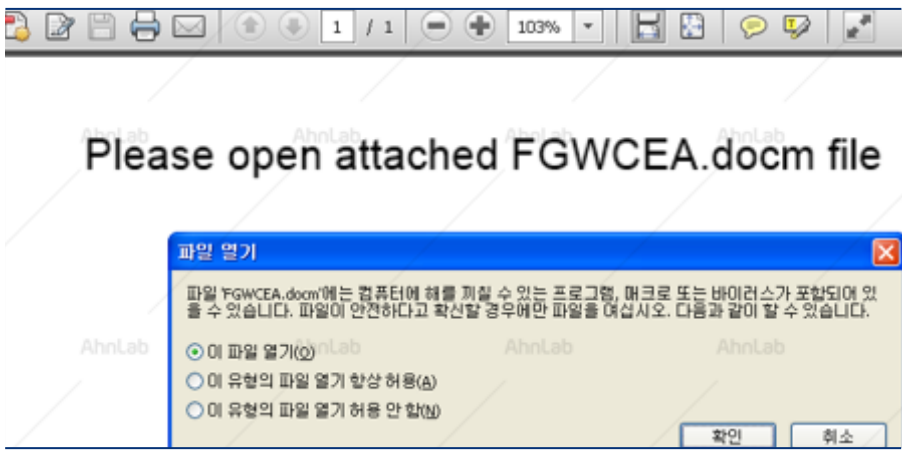


그림 1-2 | PDF 내부에 존재하는 스크립트에 의한 *.docm 실행

성 스팸 메일을 통해 유포된다. 사용자가 메일에 첨부된 PDF 문서가 포함하고 있는 *.docm 형식의 워드 파일을 실행하면, 워드 파일에 숨어있던 악성 매크로가 실행되면서 사용자 PC가 재프 랜섬웨어에 감염된다.

사용자가 첨부 파일인 PDF 문서를 열면 [그림 1-2]와 같이 '첨부된 .docm 파일을 실행하라'는 내용의 메시지 창이 나타난다.

이때 사용자가 docm 확장자의 워드 파일을 실행하고 [그림 1-3]과 같이 매크로 사용 버튼을 누르게 되면 docm 파일은 특정 URL로부터 인코딩된 바이너리를 내려 받는다.

그림 1-3 | *.docm 파일 실행 화면

악성 매크로가 실행되면서 내려받은 바이너리는 32바이트(byte) 길이의 XOR키 값을 통해 디코딩된다. 디코딩 과정이 모두 완료되면 최종적으로 랜섬웨어가 실행되면서 사용자 PC의 파일들이 암호화된다.

```
Public Function Assimptota4(FullPath As String, NumHoja As Integer) As String
  WidthA PUKALA_ProjectBBB, PUKALA_Project, "QOfPWKYMzQzNuuzBQGeax2Lkh3YOoWEl"

PUKALA_GMAKO.Open (PUKALA_Project)

End Function
```

그림 1-4 | *.docm 파일 내부에 존재하는 XOR 키 값

2. 동작 과정

다음은 실행된 재프 랜섬웨어의 동작 과정을 살펴보자. 재프 랜섬웨어는 윈도우(Windows)에서 제공하는 전력 관리 API인 GetSystemPowerStatus를 이용해 시스템의 배터리 절약 모드 사용 여부와 언어 환경에 따라 감염 여부를 결정한다.

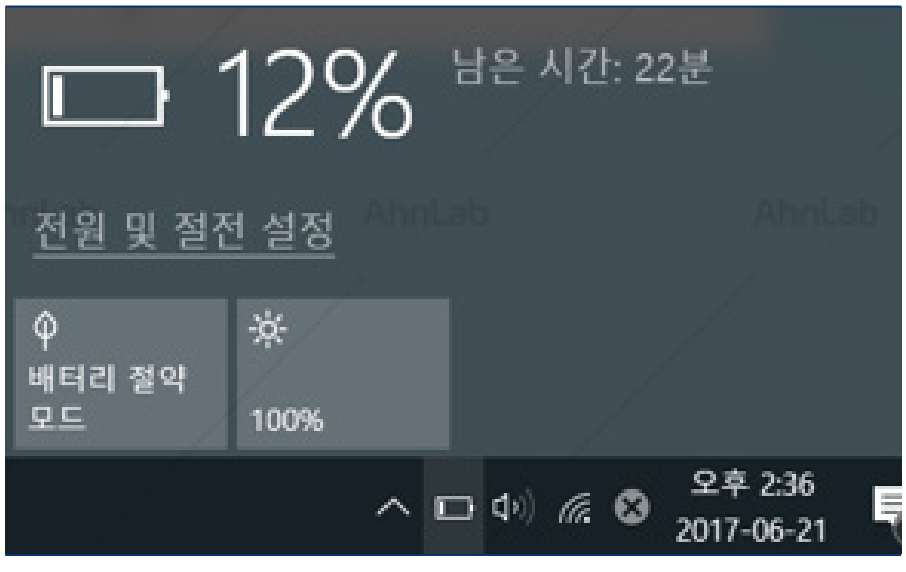


그림 1-5 | 배터리 절약 모드

```
BYTE ACLineStatus;
BYTE BatteryFlag;
BYTE BatteryLifePercent;
BYTE SystemStatusFlag; -> 배터리 절약 모드 Flag 값
(0이면 사용 x, 1이면 사용)
DWORD BatteryLifeTime;
DWORD BatteryFullLifeTime;
```

표 1-1 | GetSystemPowerStatus API에서 사용하는 SYSTEM_POWER_STATUS 구조체

배터리 절약 모드 기능은 윈도우 10 노트북에 기본으로 탑재되는 기능 중 하나로, [그림 1-5]와 같이 배터리 아이콘을 클릭하면 배터리 절약 모드를 사용하고 있는 것을 확인할 수 있다. 재프 랜섬웨어는 [그림 1-6]과 같이 배터리 절약 모드의 플래그(Flag) 값을 확인하여 사용자가 배터리 절약 모드를 사용하는 경우에는 감염을 진행하지 않고 자기 자신을 종료한다.

또한 사용자 PC의 언어 환경을 확인하여 러시아어 환경의 PC일 경우에도 감염을 진행하지 않고 종료한다. 러시아는 공격 대상이 아닌 것으로 추정되는 이유다.

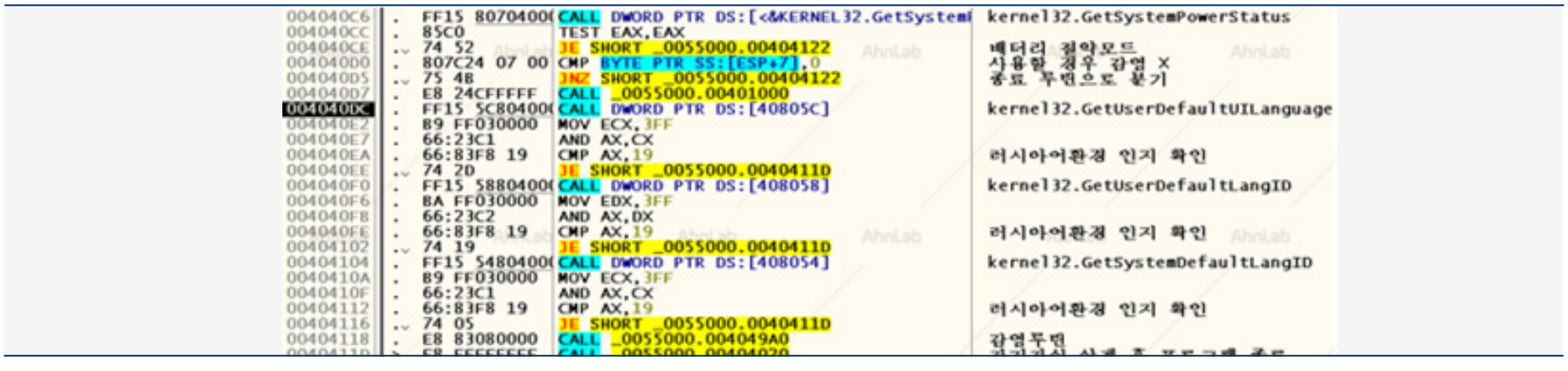


그림 1-6 | 감염 여부 결정 루틴

재프 랜섬웨어는 [그림 1-6]과 같은 루틴을 통해 감염 여부가 결정되면 파일 암호화를 진행하며, 변형에 따라 암호화한 파일의 확장자를 .jaff, .wlu, .svn으로 변경한다.

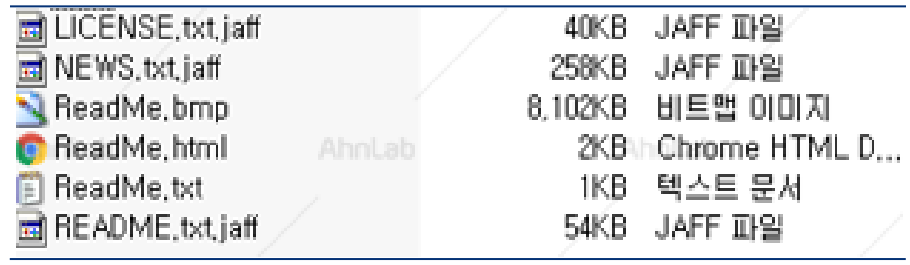


그림 1-7 | 재프 랜섬웨어에 의해 감염된 파일

재프 랜섬웨어는 암호화 대상 파일의 확장자를 랜섬웨어 프로세스 메모리 공간에 저장한다. CD-ROM 드라이브를 제외한 나머지 루트 디렉터리에 존재하는 파일들의 확장자를 하나씩 비교하여 해당 파일이 암호화 대상 확장자와 일치할 경우 암호화를 진행한다. 재프 랜섬웨어가 암호화하는 확장자는 [표 1-2]와 같다.

.xlsx .acd .pdf .pfx .crt .der .cad .dwg .MPEG .rar .veg .zip .txt .jpg .doc .wbk .mdb .vcf .docx .ics .vsc .mdf .dsr .mdi .msg .xls .ppt .pps .obd .mpd .dot .xlt .pot .obt .htm .html .mix .pub .vsd .png .ico .rtf .odt .3dm .3ds .dxf .max .obj .7z .cbr .deb .gz .rpm .sitx .tar .tar .gz .zipx .aif .iff .m3u .m4a .mid .key .vib .stl .psd .ova .xmod .wda .prn .zpf .swm .xml .xlsm .par .tib .waw .001 .002003 . .004 .005 .006 .007 .008 .009 .010 .contact .dbx .jnt .mapimail .oab .ods .ppsm .pptm .prf .pst .wab .1cd .3g2 .7ZIP .accdb .aoi .asf .asp .aspx .asx .avi .bak .cer .cfg .class .config .css .csv .db .dds .fif .flv .idx .js .kwm .laccdb .idf .lit .mbx .md .mlb .mov .mp3 .mp4 .mpg .pages .php .pwm .rm .safe .sav .save .sql .srt .swf .thm .vob .wav .wma .wmv .xlsb .aac .ai .arw .c .cdr .cls .cpi .cpp .cs .db3 .docm .dotm .dotx .drw .dxb .eps .fla .flac .fxg .java .m .m4v .pcd .pct .pl .potm .potx .ppam .ppsx .ps .pspimage .r3d .rw2 .sldm .sldx .svg .tga .wps .xla .xlam .xlm .xltm .xltx .xlw .act .adp .al .bkp .blend .cdf .cdx .cgm .cr2 .dac .dbf .dcr .ddd .design .dtd .fdb .fff .fpx .h .iif .indd .jpeg .mos .nd .nsd .nsf .nsg .nsh .odc .odp .oil .pas .pat .pef .ptx .qbb .qbm .sas7bdat .say .st4 .st6 .stc .sxc .sxw .tlg .wad .xlk .aiff .bin .bmp .cmt .dat .dit .edb .flvv .gif .groups .hdd .hpp .log .m2ts .m4p .mkv .ndf .nvram .ogg .ost .pab .pdb .pif .qed .qcow .qcow2 .rvt .st7 .stm .vbox .vdi .vhd .vhdx .vmdk .vmsd .vmx .vmxf .3fr .3pr .ab4 .accde .accdt .ach .acr .adb .srw .st5 .st8 .std .sti .stw .stx .sxd .sxg .sxi .sxm .tex .wallet .wb2 .wpd .x11 .x3f .xis .ycbcra .qbw .qbx .qby .raf .rat .raw .rdbrwl .rwz .s3db .sd0 .sda .sdf .sqlite .sqlite3 .sqlitedb .sr .srf .oth .otp .ots .ott .p12 .p7b .p7c .pdd .pem .plus_muhd .plc .pptx .psafe3 .py .qba .qbr .myd .ndd .nef .nk .nop .nrw .ns2 .ns3 .ns4 .nwb .nx2 .nxl .nyf .odb .odf .odg .odm .ord .otg .ibz .iiq .incpas .jpe .kc2 .kdbx .kdc .kpdx .lua .mdc .mef .mfw .mmw .mny .moneywell .mrw .des .dgc .djvu .dng .drf .dxg .eml .erbsql .erd .exf .ffd .fh .fhd .gray .grey .gry .hbk .ibank .ibd .cdr4 .cdr5 .cdr6 .cdrw .ce1 .ce2 .cib .craw .crw .csh .csl .db_journal .dc2 .dcs .ddoc .ddrw .ads .agdl .ait .apj .asm .awg .back .backup .backupdb .bank .bay .bdb .bgt .bik .bpw .cdr3 .as4 .tif .asp .hdr .iso

표 1-2 | 암호화 대상 파일 확장자

그림 1-8 | 랜섬노트

파일 암호화가 모두 완료되면 [그림 1-8]과 같은 랜섬노트를 띄워 사용자에게 감염 사실을 알린다.

3. 암호화/복호화 방식

재프 랜섬웨어가 파일을 암호화 및 복호화하는 일련의 과정은 다음과 같다.

재프 랜섬웨어는 파일 암/복호화를 위해 AES-256 대칭키 알고리즘을 사용한다. 또한 CryptGenKey API를 활용하여 AES-256 알고리즘에 사용되는 무작위의 키 블랍(Binary Large Object, BLOB) 데이터를 생성한다. 한번 생성한 키 블랍 데이터는 모든 암호화 대상 파일의 키로 사용된다.

① CryptGenKey API를 활용하여 AES-256 키 블랍 데이터 생성

② 리소스 섹션의 RCDATA 영역에 위치한 데이터, 사용자 decrypt ID, AES-256 키 블랍 데이터 정보들을 특정 암호화 데이터로 인코딩

③ ①에서 생성한 AES-256 키 블랍 데이터를 사용하여 CBC 모드로 파일 암호화를 진행

④ 암호화된 파일의 헤더 부분에 ②에서 생성한 인코딩 데이터 덧붙임

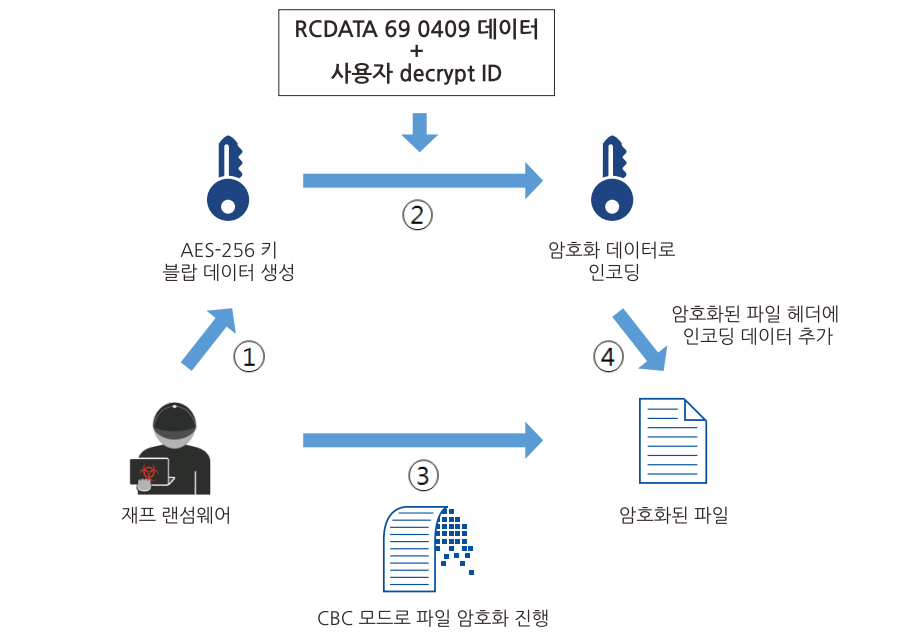


그림 1-9 | 재프 랜섬웨어 암호화 과정

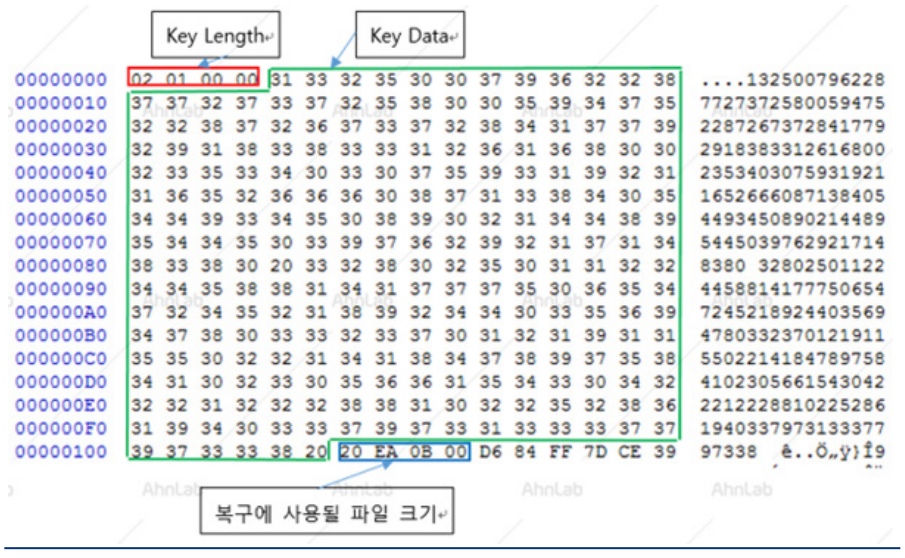


그림 1-10 | 암호화된 파일의 구조

재프 랜섬웨어는 [그림 1-9]와 같은 과정을 통해 파일을 암호화한 후, [그림 1-10]과 같이 암호화가 완료된 파일 데이터 앞 부분에 키의 길이 정보, 키 데이터, 복구에 사용될 파일 크기 정보를 저장한다.

앞서 언급한 바와 같이 암호화 과정에서 최초 생성된 AES-256 대칭 키 데이터는 모든 파일 암호화에 이용된다. 이때 암호화된 파일에 저장할 키 데이터를 생성하기 위해 사용자 decrypt ID 정보, AES-256 키 블롭 데이터 정보, RCDATA 영역에 저장된 고정된 0x104 크기의 데이터가 사용된다.

```
000069C0  33 35 33 32 36 30 35 34  30 33 31 38 36 31 33 36  3532605403186136
000069D0  38 31 33 39 35 36 33 33  30 36 31 38 34 31 33 34  8139563306184134
000069E0  31 36 37 30 31 38 31 33  30 37 31 38 35 36 39 34  1670181307185694
000069F0  38 32 37 33 31 36 36 36  30 30 31 36 35 30 38 31  8273166600165081
00006A00  37 35 33 39 31 30 38 37  34 34 34 30 31 30 31 36  7539108744401016
00006A10  36 33 33 32 33 31 33 30  34 34 33 37 32 32 34 37  6332313044372247
00006A20  33 30 37 39 30 36 33 38  36 31 35 37 36 36 37 34  3079063861576674
00006A30  30 32 37 32 31 30 36 34  30 33 31 34 33 32 35 36  0272106403143256
00006A40  0D 0A 33 35 33 32 36 30  35 34 30 33 31 38 36 31  ..35326054031861
00006A50  33 36 38 31 33 39 35 36  33 33 30 36 31 38 34 31  3681395633061841
00006A60  33 34 31 36 37 30 31 38  31 33 30 37 31 38 35 36  3416701813071856
00006A70  39 34 38 32 37 33 31 36  36 36 30 30 31 36 35 30  9482731666001650
00006A80  38 32 39 38 36 34 35 36  38 33 37 31 30 39 34 34  8298645683710944
00006A90  34 34 32 30 33 35 35 37  36 30 31 31 37 30 32 30  4420355760117020
00006AA0  36 38 34 34 30 30 33 36  33 31 31 30 31 37 32 32  6844003631101722
00006AB0  32 30 32 32 33 33 33 36  37 39 37 35 39 36 38 36  2022333679759686
00006AC0  36 37 0D 0A                                       67..
```

그림 1-11 | RCDATA 영역에 위치한 0x104 크기의 데이터

최근 유포된 재프 랜섬웨어는 지난 5월에 유포된 재프 랜섬웨어와 RCDATA 영역의 고정된 0x104 크기의 데이터가 같다. 따라서 랜섬노트에 적힌 사용자의 decrypt ID 정보만 얻을 수 있다면 파일 암호화에 사용된 AES-256 키 블롭 데이터 정보를 추출할 수 있고, 추출된 키 블롭 데이터 정보를 통해 암호화된 파일들은 모두 복호화가 가능하다.

http://txxxlitranxxxsixxx .nxt/ax/

표 1-3 | C&C 서버 정보

재프 랜섬웨어가 접속하는 C&C 서버의 주소는 [표 1-3]과 같으며, 상세 주소 값은 변형마다 다르다.

재프 랜섬웨어의 특징적인 점은 다른 랜섬웨어와 달리 C&C 서버에서 받아온 데이터로 특정 명령을 수행하거나 감염된 PC 정보를 C&C 서버로 전송하는 것이 확인되지 않았다는 점이다. 이를 통해 재프 랜섬웨어 C&C 서버의 용도는 주로 감염자의 수치를 파악하기 위한 것으로 추정된다.

이번에 발견된 재프 랜섬웨어의 경우 키 블롭 데이터를 통해 암호화된 파일의 복호화가 가능했지만, 일단 대부분의 랜섬웨어에 감염되면 암호화된 파일을 완벽하게 복구하는 방법은 없다. 따라서 랜섬웨어 피해를 최소화하기 위해서 윈도우 보안 패치 및 V3 백신 프로그램을 항상 최신 업데이트 상태로 유지하는 등의 평소 예방을 수행하는 것이 무엇보다 중요하다.

특히 재프 랜섬웨어와 같이 스팸 메일에 첨부된 파일을 통해 불특정 다수에게 무작위로 유포되는 랜섬웨어가 꾸준히 발견되고 있으므로, 평소 신뢰할 수 없는 메일의 첨부 파일을 실행할 때에도 사용자의 각별한 주의가 요구된다.

V3 제품군에서는 재프 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군 진단명>

- Trojan/Win32.Jaff (2017.05.12.00)
- Trojan/Win32.JaffCrypto (2017.05.12.03)

상반기 결산

1H THREAT REVIEWS

- 2017년 상반기 랜섬웨어 동향 분석

상반기 결산

1H Threat Reviews

2017년 상반기 랜섬웨어 동향 분석

전 세계에 막대한 피해를 입힌 랜섬웨어 폭풍이 2017년에도 그칠 기미가 보이지 않는다. 2017년 상반기 랜섬웨어 위협은 적색 경보 수준에 이르렀다. 한동안 잠잠했던 록키(Locky) 랜섬웨어가 귀환한데 이어 새로운 기능을 탑재한 케르베르(Cerber) 랜섬웨어도 더욱 강력하게 활동 중이다. 특히 지난 5월 초에 등장한 워너크립터(WannaCryptor)는 단시간에 확산되며 세계 곳곳의 주요 기관 및 기업을 마비시켰다.

한편 2016년부터 본격적으로 파일을 암호화하는 랜섬웨어가 등장하면서 랜섬웨어의 수익 모델과 시장이 형성된데 이어 올해 상반기에는 시장 확대와 함께 고수익 추구 등의 경향이 두드러지게 나타났다.

이와 관련해 안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)는 주요 랜섬웨어를 중심으로 2017년 상반기 랜섬웨어의 동향을 분석했다.

그림 2-1 | 2015년 대규모 유포된 크립토락커(CryptoLocker) 랜섬웨어

1. 상반기 랜섬웨어의 주요 특징

초기 랜섬웨어는 PC 바탕화면의 아이콘과 시작 버튼을 선택할 수 없도록 한 다음 돈을 요구하는 '화면잠금형 랜섬웨어'가 주류를 이뤘다면, 지난 2015년부터는 사용자의 파일을 암호화하는 '데이터잠금형(Data Locker)

랜섬웨어’가 본격적으로 유포되기 시작했다. 크립토락커(CryptoLocker), 크립토월(CryptoWall), CTB락커(CTBLocker), 나부커(Nabucur), 테슬라크립트 (TeslaCrypt) 등이 대표적인 예이다.

랜섬웨어는 주로 스팸 메일을 통해 유포되거나, 인터넷 익스플로러, 자바, 플래시 플레이어 등의 응용 프로그램 취약점을 악용하는 익스플로잇 킷(Exploit Kit)을 이용해 유포된다. 랜섬웨어의 공통적인 특징은 파일 암호화가 완료된 후 파일에 고유한 확장자명을 추가한다는 점이다. 또한 PC의 바탕화면을 변경하고 암호화 사실을 알리는 메시지 창을 띄워 결제를 유도하는 행위를 보인다.

최근 유포되고 있는 랜섬웨어의 감염 증상들을 정리하면 다음과 같다.

그림 2-2 | 최근 랜섬웨어 특징

1) 암호화 대상 범위 확대

랜섬웨어가 암호화하는 대상 파일이 사용자가 주로 사용하는 문서 파일과 그림 파일 뿐 아니라 데이터베이스 저장 파일이나 이메일 백업 파일과 같은 다양한 확장자로 확대되었다.

2) 다국어 지원

초기에는 사용자에게 암호화 사실을 알리고 지불을 요구하는 감염 메시지나 랜섬노트에 영어, 러시아

어 등의 제한적인 언어만 사용되었지만 최근에는 스페인어, 독일어, 포르투갈어, 이탈리아어, 아랍어, 한국어 등 다양한 언어를 지원한다.

3) 복구 방해

일부 취약하게 만들어졌거나 복호화 마스터키가 공개된 랜섬웨어를 제외하고, 대부분의 랜섬웨어는 고도의 암호화 기법을 사용하여 자체 복구가 불가능하다.

4) 익명 통신

사용자의 추적이 불가능하도록 하기 위해 암호화 익명 통신 기술인 토르(Tor)를 이용한다. 특히 비트코인 지불, C&C 서버 통신과 같은 경우 대부분 토르 네트워크를 이용한다. 랜섬웨어 자체에 토르 클라이언트 프로그램이 포함된 경우도 있다.

5) 비트코인 요구

사용자의 데이터를 암호화하고 비트코인을 요구한다. 초기에는 온라인 결제 서비스와 신용카드 결제를 이용하여 달러나 유로화로도 지불이 가능했지만, 최근에는 대부분 비트코인으로 결제를 요구한다.

6) 복구 기능 비활성화

감염 즉시 볼륨 쉐도우 카피(Volume Shadow Copy) 영역을 삭제하여, 윈도우의 자체 백업 데이터를 이용한 복구를 불가능하게 한다.

7) 확장자명 변경

사용자가 파일이 암호화된 것을 알아차릴 수 있도록 대부분의 랜섬웨어는 암호화가 완료된 파일의 확장자명을 변경하거나 추가한다. 일부는 파일명도 함께 변경한다. 매우 드물지만 확장자명을 변경하지 않는 경우도 있다.

안랩 통계 분석 결과, 랜섬웨어는 이미 초기 등장기와 성장기를 넘어 관련 시장이 형성된 성숙기에 접어든 것으로 볼 수 있다. 이는 월별 발견된 랜섬웨어 종류의 수를 통해서도 확인할 수 있다. 2016년 상반기에는 월별 랜섬웨어가 순차적으로 증가했다면, 2017년 상반기는 [그림 2-3]과 같이 1월부터 6월까지 고르게 다수 발견되는 양상을 보였다.

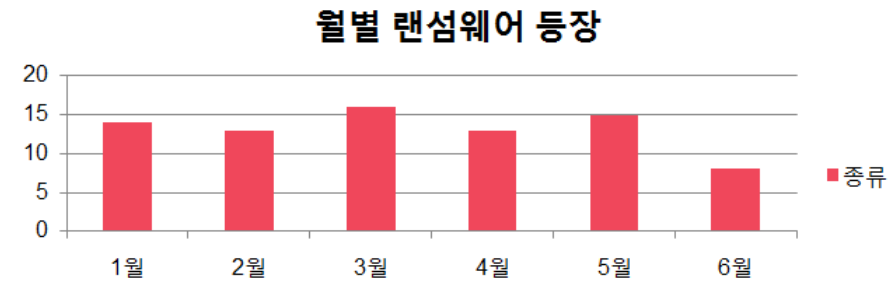


그림 2-3 | 2017년 월별 랜섬웨어 발견 수

2017년 상반기에 발견된 랜섬웨어 종류 또한 2016년에 비해 훨씬 다양해졌다. 2017년 1월부터 6월까지 약 79종의 랜섬웨어가 발견되었는데, 이는 전년도 동일 기간 동안 발견된 65종을 훨씬 웃도는 수치다. 이와 같이 랜섬웨어 종류가 빠르게 증가할 수 있었던 원인은 2016년 상반기부터는 서비스형 랜섬웨어인 RaaS(Ransomware as a Service) 랜섬웨어의 등장과 함께 오픈소스를 이용한 랜섬웨어 제작이 활성화되었기 때문이다. 특히 2017년에는 이와 같은 제작 방식이 더욱 일반화되면서 랜섬웨어 종류가 폭발적으로 증가했다.

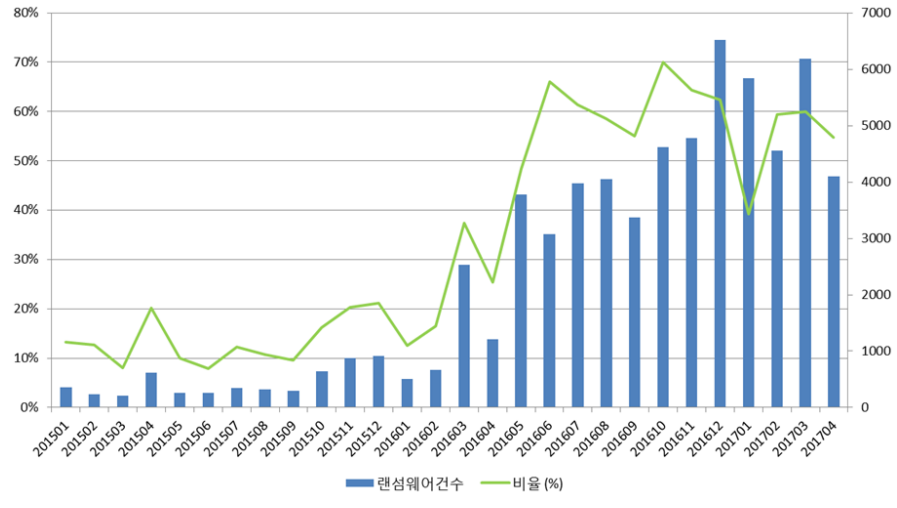


그림 2-4 | 랜섬웨어 관련 문의 추이

한편 2015년 1월부터 2017년 4월까지 ASEC에 접수된 랜섬웨어 문의 관련 통계를 확인해보면, 2017년 초부터 이미 상당 수의 문의가 접수된 것을 확인할 수 있다. 2017년 상반기에는 록키 랜섬웨어의 활동이 잠시 주춤했지만, 케르베르 랜섬웨어와 오픈소스 기반의 랜섬웨어 관련 문의, 그리고 랜섬웨어를 유포하는 스팸 봇넷 관련 문의가 다수 접수된 바 있다.

2017년에는 신종 랜섬웨어뿐만 아니라 기존 랜섬웨어의 변형도 다수 발견된 것이 특징이다. 특히

1분기에 잠시 활동이 없었던 록키 랜섬웨어가 2분기인 4월 중순에 다시 복귀했다. 또한 2월에는 케르베르 랜섬웨어가 윈도우 방화벽 차단 목록으로 PC에 설치된 보안 제품을 추가하는 버전 6으로 다시 등장했다. 5월에는 윈도우의 SMB(Server Message Block) 취약점을 악용하여 확산된 워너크립터(WannaCryptor) 랜섬웨어가 전 세계적으로 악명을 떨쳤다.

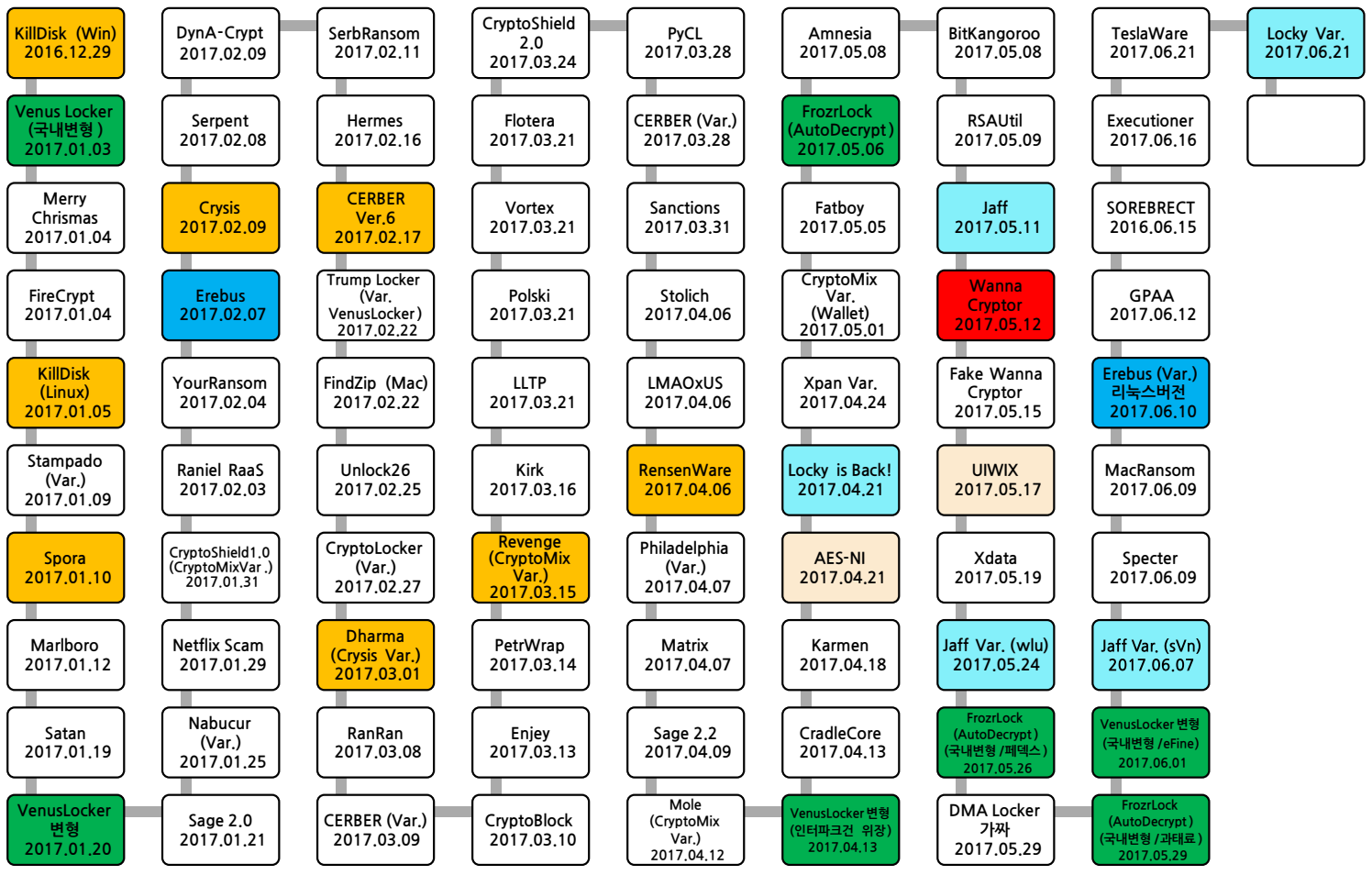


그림 2-5 | 2017년 발견된 랜섬웨어 목록

2017년 상반기 랜섬웨어 동향은 '진화'라는 단어로 정의할 수 있다. 기존 기능과 더불어 윈도우 취약점과 윈도우 보안 기능을 악용하는 방법을 추가하여 기능을 더욱 강력하게 개선했다. 이 밖에 상반기에 발견된 랜섬웨어의 주요 특징들을 정리하면 다음과 같다.

그림 2-6 | 2017년 상반기 랜섬웨어의 주요 특징

1) 부익부빈익빈 극대화

2016년 3월 발견된 케르베르는 여전히 건재함을 과시하며, 2017년 2월에 윈도우의 방화벽 차단 기능을 악용한 버전 6로 돌아왔다. 또한 워너크립터는 윈도우 취약점을 이용하여 전 세계적으로 막대한 감염 피해를 입혔다. 한편 유포 경로의 한계로 인해 록키는 1분기에 자취를 감췄고, 그 밖에 다양하게 발견된 신종 랜섬웨어도 큰 영향력을 발휘하지는 못했다.

2) 재활용의 일반화

기존에 발견된 비너스락커(VenusLocker), 크립토믹스(CryptoMix), 크라이시스(Crysis) 랜섬웨어의 변형이 다수 발견되었다. 과거의 랜섬웨어를 재활용하면 제작자는 투입되는 노력을 최소화하면서 수익을 추구할 수 있기 때문이다.

3) 오픈소스의 대중화

오픈소스 랜섬웨어인 EDA2, 히든 티어(Hidden Tear)의 코드를 활용한 랜섬웨어가 2017년 상반기에도 지속적으로 발견되었다. 프로그래밍 능력이 있으면 누구나 제작할 수 있기 때문에 점차 대중화되어가고 있다.

4) 서비스형 랜섬웨어(Ransomware as a service, RaaS)의 보편화

2016년 RaaS 랜섬웨어는 그 등장만으로 큰 이슈였다. 웹이나 제너레이터(빌더)를 이용한 제작 수단과 웹페이지를 통한 수익 관리가 간편화되었기 때문이다. 2017년은 제작자의 수익 증대 목적으로 다크웹에서 자리를 잡은 RaaS가 더욱 보편화되고 있다.

5) 익스플로잇 킷(Exploit Kit, EK)의 몰락과 스팸 활성화

2016년은 각종 익스플로잇 킷을 활용한 랜섬웨어의 유포가 활성화되었다. 하지만 그 중 뉴클리어(Nuclear) EK, 앵글러(Angler) EK는 현재 사라졌다. 2017년 상반기에는 리그(RIG) EK를 중심으로 여전

히 익스플로잇 킷이 활동 중이지만, 전체적인 EK의 활동이 작년의 10% 수준으로 눈에 띄게 감소했다.

6) 기술의 고도화

쉐도우 브로커스(Shadow Brokers)가 공개한 SMB(Server Message Block) 취약점인 이터널블루(Eternal Blue)를 악용한 워너크립터, 윈도우의 보안 기능인 방화벽 차단 목록을 악용한 케르베르 버전 6과 같이 랜섬웨어에 적용된 기술이 갈수록 고도화되고 있다.

2. 유포 방식의 변화

랜섬웨어의 주요 유포 기법은 크게 2가지로 나눌 수 있다. 스팸 메일의 첨부파일을 통한 랜섬웨어 대량 감염 유도와 보안이 취약한 사이트를 악용하여 익스플로잇 킷을 통해 랜섬웨어를 유포하는 드라이브-바이-다운로드(Drive-by-download) 방식이다. 2017년에는 이들 주요 유포 방식에 어떤 변화가 있었는지 살펴보자.

1) 스팸 메일을 통한 유포 증가

가장 전통적인 악성코드 유포 기법인 스팸 메일은 여전히 가장 강력한 수단으로 악명을 떨치고 있다. 시스코(CISCO)에서 발표한 자료에 따르면 올해 상반기 스팸 메일은 2016년 초반에 비해 급증했고, 전체 이메일 트래픽의 65%를 차지했으며 스팸 메일의 80%가 악성 파일을 첨부한 것으로 나타났다.

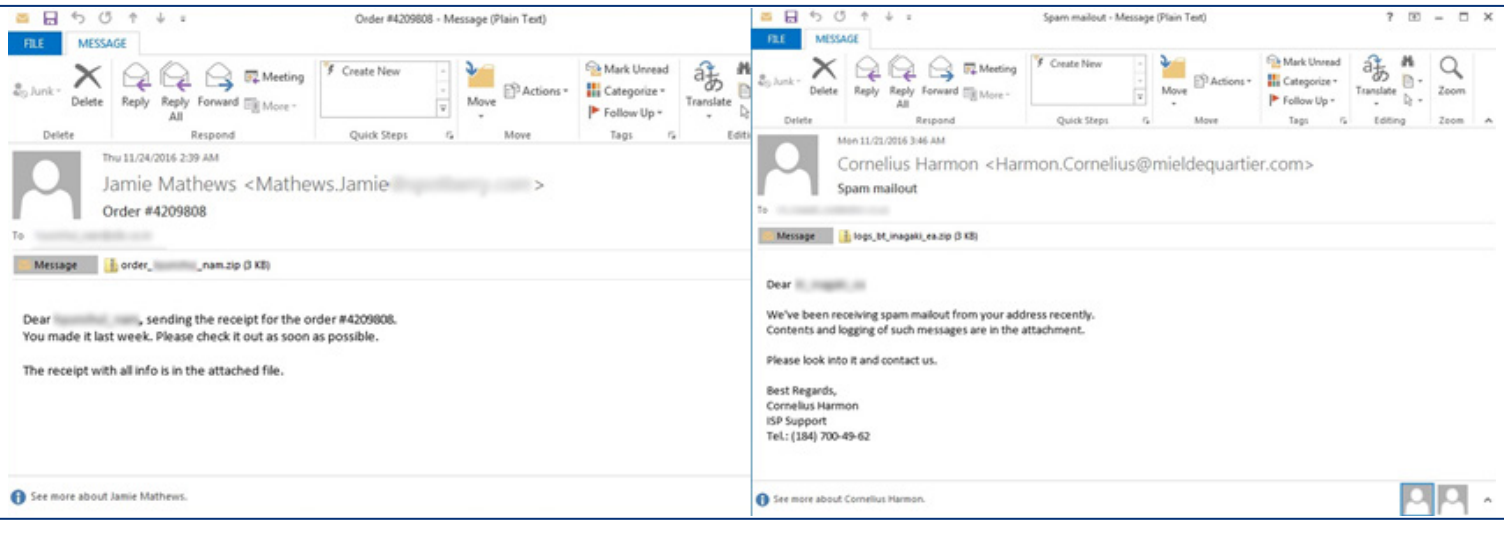


그림 2-7 | 사회공학기법을 이용한 스팸 메일

특히 스팸 메일을 통한 유포는 사용자가 메일을 열람하고 첨부파일을 실행해야 하기 때문에 사용자의 의심을 피하기 위한 사회공학적 기법이 동반된다. 주로 이벤트, 경품, 배송 관련 메일로 위장하며, 최근에는 개인정보 유출사고 관련 메일이나 공공기관을 사칭한 메일도 다수 발견되고 있다. 또한 최근에는 실행 파일, 압축 파일, 스크립트 파일이 첨부된 메일에 대한 차단이 강화되고 있기 때문에 보안 솔루션을 우회하기 위한 기법이 적용되고 있다.

록키 랜섬웨어는 스팸 메일을 통해 랜섬웨어가 유포된 대표적인 사례다. 해외에서 가장 유명한 금융 악성코드 중 하나인 드라이덱스(Dridex) 악성코드를 유포해온 네커스(Necurs) 봇넷에 의해 록키 랜섬웨어가 유포되기 시작하면서 전 세계적으로 피해가 발생했다. 하지만 2016년 12월 25일 전후로 네커스 봇넷은 록키의 유포를 중단하였는데 이는 록키 랜섬웨어가 자취를 감추는 가장 큰 원인이 되었다.

그림 2-8 | 록키 유포 주역인 네커스 봇넷 활동 타임라인

올해 2017년에도 네커스 봇넷이 디도스(DDoS) 기능을 추가한 악성코드를 2월에 유포하였고, 3월에는 주가 조작을 시도하는 스팸 메일을 대량으로 유포했다. 이어서 4월에는 네커스 봇넷의 주요 악성코드인 드라이덱스를 다시 유포하기도 했다.

또한 네커스 봇넷을 통해 온라인 데이트 신청으로 가장한 스팸 메일을 보내는 데이팅 스팸이 유포된 사례도 다수 발견되었다. 데이팅 스팸의 경우 또 다른 봇넷인 켈리호스(Kelihos) 봇넷의 주요 활동 영역이었는데, 4월 10일 해당 봇넷 운영자가 체포된 이후 네커스 봇넷이 해당 영역을 이어 받아 활동한 것으로 추정된다.

현재까지 확인된 네커스 봇넷의 가장 최근 활동은 5월 중순 경 재프 랜섬웨어를 유포한 것이다. 재프 랜섬웨어는 록키 랜섬웨어에서 사용된 지불 사이트의 레이아웃 및 HTML 코드를 도용하여 사용한 것으로 유명한 랜섬웨어다. 그러나 록키와 재프 랜섬웨어의 제작자가 동일한지 여부와, 앞으로 네커스 봇넷이 지속적으로 재프 랜섬웨어를 유포할지 여부는 더 지켜봐야 할 것으로 보인다.

2) 익스플로잇 킷 사용의 감소

2017년에는 익스플로잇 킷(EK)을 사용한 유포 방식이 2016년 대비 큰 폭으로 감소한 것으로 확인됐다. EK는 인터넷 익스플로러, 플래시 플레이어, 자바, 실버라이트 등의 프로그램의 취약점을 발생시키는 스크립트 코드를 자동으로 생성하는 프로그램이다. EK를 통해 스크립트 코드를 보안이 취약한 웹사이트에 미리 심어놓으면, 해당 프로그램의 최신 버전을 사용하지 않는 사용자가 해당 사이트를 방문 시 악성 사이트로 자동으로 연결되어 사용자 PC에 악성코드가 다운로드된다.

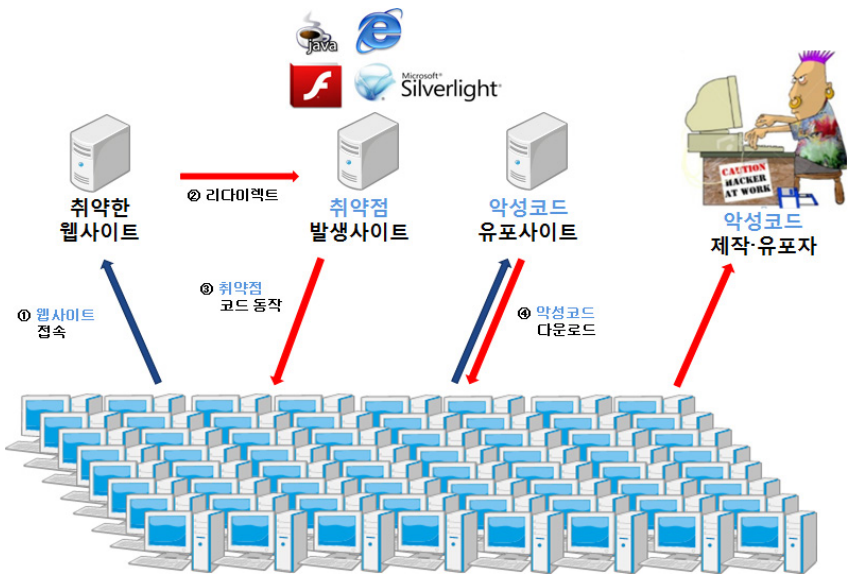


그림 2-9 | EK를 통한 악성코드 감염 과정

2015년에는 뉴클리어, 2016년 상반기에는 앵글러 EK가 활발하게 활동했으며, 랜섬웨어 감염에 큰 역할을 했다. 특히 웹사이트에 온라인 광고를 제공하는 업체의 서버를 악용하여 악성 파일을 유포하는 멀버타이징(Malvertising) 방식도 랜섬웨어 유포에 많이 사용되었다. 2016년 국내 커뮤니티 사이트를 통해 악성코드가 유포된 것도 이러한 방식으로 유포된 것이다.

여기서 주목할 만한 점은 2017년에는 EK의 활동이 급격하게 감소했다는 점이다. 마이크로소프트(Microsoft)에서 발표한 자료에 따르면, 2016년의 최대치에 비해 25% 수준으로 감소한 것으로 나타났다.

감소 요인 중 하나로 2016년 7월부터 앵글러 EK가 활동을 중단한 점을 꼽을 수 있다. 이후 뉴트리노(Neutrino) EK가 그 자리를 차지하는 것 같았지만, 뉴트리노 EK 역시 공개적인 활동 대신 소수의 사용자에게만 서비스를 제공하는 프라이빗(Private) 형태로 활동 방식을 변경하면서 2016년 10월 이후 활동이 급격히 감소했다. 이후 리그(RIG) EK가 주도적인 위치로 부상하며 지금까지 활동하고 있지만, 전체적인 EK의 활동이 감소함에 따라 2016년과 같은 대규모 유포 형태는 확인되지 않고 있다.

이 외에도 해외에서 발견된 선다운(Sundown)과 테러(Terror) EK은 존재하지만 아직 국내에서 큰 피해를 발생시키지는 않았다. 결론적으로 2017년에는 EK의 활동은 큰 폭으로 감소했지만 국내에서는 여전히 멀버타이징 및 EK에 의한 랜섬웨어 감염 사례가 지속적으로 발견되기 때문에 항상 주의를 기울여야 한다.

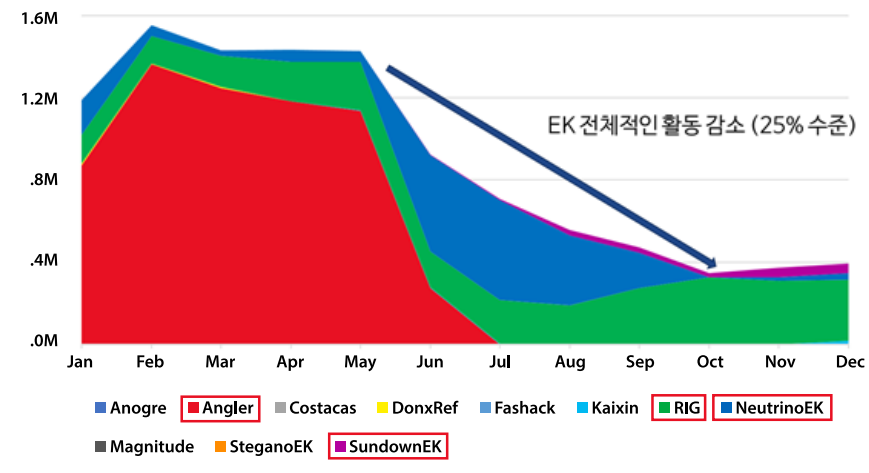


그림 2-10 | 전체적인 EK의 활동 감소 (*출처: 마이크로소프트)

3. 2017년 상반기 랜섬웨어 공격 Top 10

2016년에 이어 2017년 상반기에도 다수의 랜섬웨어 피해 사례가 발견되었다. 데이터베이스 자체를 암호화시킨 사례도 발견되었을 뿐만 아니라 공공, 서비스, 비영리, 교육 등 다양한 영역으로 랜섬웨어의 피해 범위가 확산되었다. 2017년 상반기에 나타난 랜섬웨어 중 가장 특징적인 랜섬웨어 사례 10건은 다음과 같다.

1) 데이터베이스 서버 공격한 랜섬웨어

2017년 1월부터 2월까지, 약 두달에 걸쳐 데이터베이스를 암호화하는 공격이 발견되었다. 1월 3일에는 오픈소스 프로그램인 몽고DB(MongoDB) 서버, 13일에는 분산형 검색 및 분석 엔진인 엘라스틱서치(ElasticSearch) 서버에 대한 암호화 공격이 발견되었으며 18일에는 빅데이터를 처리할 수 있는 오픈

소스 프레임워크인 하둡(Hadoop) 서버에 대한 암호화 공격이 확인됐다. 또한 2월 25일에는 오픈소스 데이터베이스 프로그램으로 널리 사용되고 있는 MySQL 서버에 대한 암호화 공격도 발견되었다. 이러한 데이터베이스 관련 서버 공격은 서버에 저장된 대량의 데이터에 대해 피해를 발생시킬 수 있기 때문에 각별한 주의가 요구된다. 서버 관리자는 운영 프로그램에 대한 보안 업데이트를 꾸준히 설치하고, 사용자 접근제어 등의 보안 대책을 강화할 필요가 있다.

그림 2-11 | 데이터베이스 서버 관련 공격 흐름

2) 공공, 서비스, 비영리, 교육 영역으로 확산된 랜섬웨어

미국에서 2017년 1~2월 사이에 공공, 서비스, 교육 등 여러 영역에 걸쳐 다수의 랜섬웨어 피해 사례가 확인되었다.

그림 2-12 | 공공, 서비스, 비영리, 교육 영역으로 랜섬웨어 피해 확대

가장 먼저 1월 10일에는 미국 LA 지역 대학에서 랜섬웨어에 대량 감염되는 사고가 발생했고, 20일에는 미국 세인트루이스 지역 공공 도서관이 랜섬웨어에 감염되어 도서 대여 및 출납 업무가 마비된 사례도 있었다. 이어서 26일에는 미국 텍사스주 콕렐힐시(市)에서 록키 랜섬웨어에 감염 피해가 발생하여 8년간의 수사 증거물들이 훼손되는 사고가 발생했다.

1월 30일에는 미국 워싱턴 DC에서의 HDD크립터(HDDCryptor) 감염으로 CCTV 시스템들이 작동하

지 않은 사고가 있었는데, 미국 트럼프 대통령의 취임식이 있었던 시기와 겹쳐 큰 주목을 받았다. 마지막으로 2월 3일에는 미국 오하이오주 행정기관이 랜섬웨어에 감염되어 업무가 마비된 사고도 있었다. 이들은 모두 랜섬웨어가 개인 PC의 데이터 손상을 넘어 공공 및 서비스 등의 마비를 초래한 대표적 사례로, 공공 영역으로 랜섬웨어 피해가 확대되었다는 점에 주목할 필요가 있다.

3) MBR 영역을 덮어쓰는 킬디스크 (2017.01)

2016년 11월 샌프란시스코의 경전철 운행을 중단시킨 사고와 2017년 1월 30일 워싱턴 DC의 CCTV가 마비된 사건은 모두 MBR 영역을 암호화하는 HDD크립터 랜섬웨어에 의한 것이었다. MBR 영역을 암호화하는 랜섬웨어는 페트야(Petya)를 시작으로 다수 발견되었지만, 2017년 1월에 킬디스크(KillDisk)라는 새로운 MBR 암호화 랜섬웨어가 발견되었다.

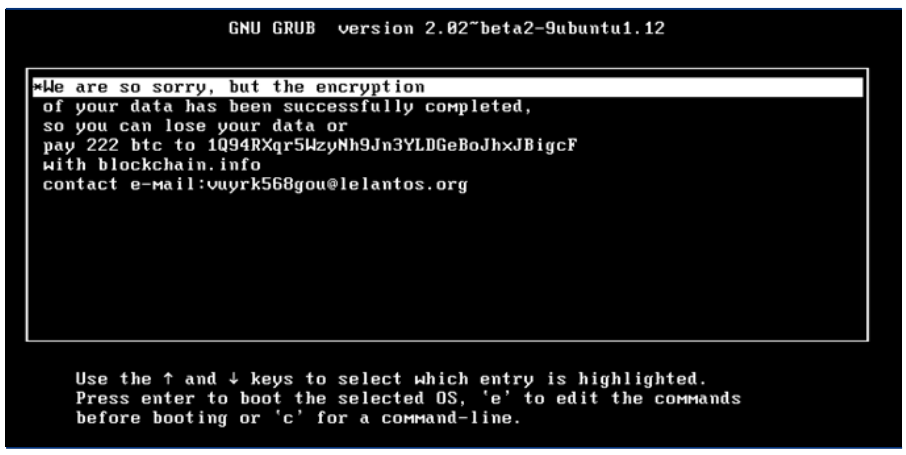


그림 2-13 | MBR 영역을 덮어쓰는 킬디스크(KillDisk)

기존의 킬디스크는 산업 분야를 대상으로 하는 표적 공격에 사용되던 악성코드로, 데이터 복구가 불가능하도록 완전히 삭제시키는 디스크 와이핑(Disk Wiping) 악성코드였다. 대표적으로 우크라이나의 블랙에너지(Black Energy) 사이버 공격을 비롯한 여러 공격에 사용된 것으로 유명하다. 이와 같은 기존 악성코드에서 디스크 와이핑 기능이 제거되고, MBR 영역과 사용자의 데이터를 암호화하는 기능이 추가된 것이 현재의 킬디스크 랜섬웨어다. 윈도우와 리눅스 운영체제를 모두 공격 대상으로 하고 있으며, 222 비트코인을 요구했다. 당시 시세로 2억 8천만원 상당이고, 최근 시세로는 약 5억 5천만원에 달하는 아주 큰 금액이다.

4) 국내 대상 사회공학기법 이용한 비너스락커(VenusLocker) (2016.12 ~ 2017.04)

비너스락커(VenusLocker) 랜섬웨어 자체는 새로운 랜섬웨어가 아니다. 지난 2017년 1분기 ASEC 리

포트에서도 다룬 바 있는 비너스락커는 이미 지난 2016년 8월 초에 발견된 적이 있으며, 오픈소스 랜섬웨어인 EDA2의 변형으로 알려져있다. 주로 사회공학기법을 이용해 기관과 기업 사용자를 대상으로 유포된 것으로 확인된 비너스락커는 2017년 1월 사내 내부지침사항과 블로그 사진 수정을 요구하는 고소장으로 위장한 메일을 통해 유포되었다. 2월에는 병역지정업체대상 교육일정안내 위장 메일, 4월에는 2016년에 발생한 국내 쇼핑 사이트의 개인정보 유출 관련 메일로 위장하여 유포되었다.

그림 2-14 | 국내 사용자 대상으로 사회공학기법을 이용한 비너스락커(VenusLocker)

첨부 파일로는 .egg, .zip, .7z 압축 파일을 이용했고, 압축 파일 내부에는 문서 파일(.doc)로 위장한 바로가기(.lnk) 파일과 사진 파일(.jpg)로 위장한 실행 파일(.exe)이 포함되어 있다. 바로가기 파일을 통해 문서 파일 확장자명으로 위장한 EXE 실행 파일을 실행하는 구조다.

5) 지불 옵션이 다양화된 스포라 (2017.01)

스포라(Spora) 랜섬웨어는 다른 랜섬웨어와 크게 다르지 않지만, 랜섬웨어에 감염된 피해자에게 다양한 지불 옵션을 제공한다는 점이 특징이다.

스포라가 제공하는 옵션 중에서 필요한 기능만 별도로 구입할 수도 있다. 무료 복구는 2개까지 가능

하고, 전체 복구는 79달러, 재감염을 방지하는 면역 기능은 50달러, 랜섬웨어 관련 파일 제거는 20달러, 일부 파일 복구는 30달러를 요구한다. 지불 페이지가 영어와 러시아어를 사용하는 것으로 보아 러시아 언어권 사용자를 대상으로 한 것으로 보인다.

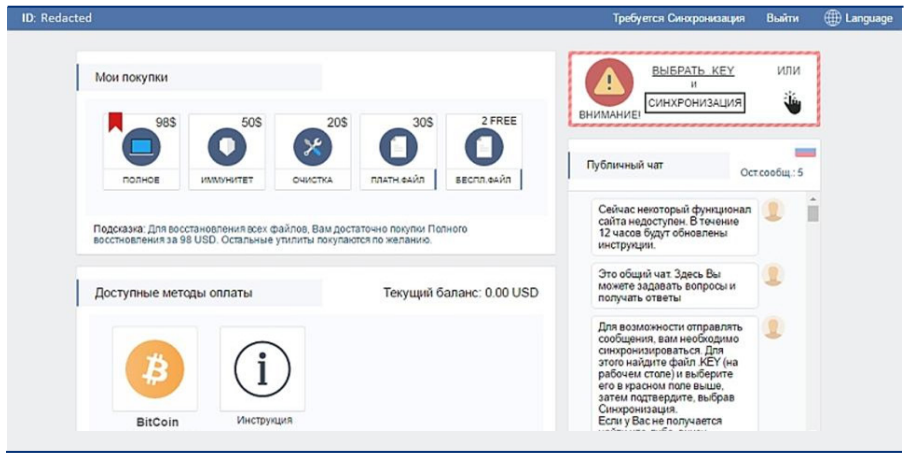


그림 2-15 | 지불 옵션이 다양화 된 스포라(Spora)

6) 보안 제품 업데이트를 방해하는 케르베르 버전 6 (2017.02)

케르베르(Cerber)는 2016년 3월에 최초 발견된 후 가장 오랜 기간 동안 활발하게 활동하고 있는 랜섬웨어로 암호화 사실을 음성으로 알려주는 최초의 랜섬웨어다. 록키와 마찬가지로 대부분 스팸 메일로 유포되며, 첨부하는 파일 형식이 DOCX, DOCM, HTA, VBS 등으로 지속적으로 변경되었다. 암호화된 파일에 CERBER 확장자명을 추가하며, 버전 3까지는 CERBER3과 같이 숫자를 추가하여 버전을 구분했다. 버전 4 이후로는 무작위 4글자 확장자명을 추가하며, 크리스마스 버전 발표 이후 활동이 잠잠해졌다.

이번 2017년 2월에 새롭게 발견된 케르베르 버전 6는 윈도우 보안 센터에 등록된 보안 제품 실행 경로를 윈도우 방화벽 차단 목록에 추가하여 정상적인 보안 제품의 동작을 방해하는 것이 가장 큰 특징이다.

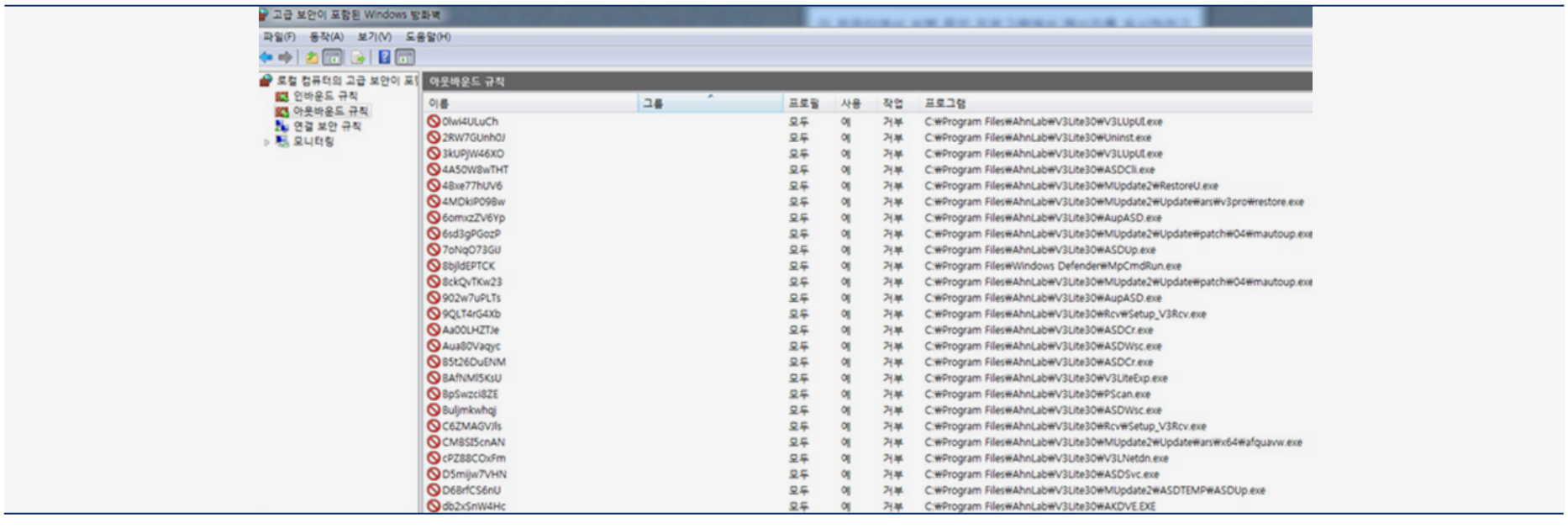


그림 2-16 | 윈도우 방화벽 차단 목록에 보안 제품을 추가하는 케르베르 버전 6

7) 게임 사용자 노린 렌센웨어 (2017.04)

2017년 4월에 발견된 '렌센웨어(RensenWare)'는 무엇보다 한국인 사용자에 의해 만들어졌다는 사실 때문에 세계적으로 유명해졌다. 국내 유명 커뮤니티 사이트 사용자에 의해 제작되었으며, 금전을 요구하지 않고 제작자가 지정한 게임에서 2억점 이상 획득해야 파일을 복구할 수 있는 점이 특징적이다.

재미있는 사실은 제작자도 해당 랜섬웨어에 감염되어 스스로 소스코드를 공개하고, 복구툴과 사과문까지 발표했다는 것이다. 또한 렌센웨어는 모든 드라이브를 대상으로 암호화하도록 되어 있으나, 예외 처리가 제대로 되어있지 않아 CD-ROM 부분에서 오류가 발생하는 버그도 존재한다. 암호화되면 RENSENWARE라는 확장자명을 추가하며 게임 프로세스를 강제로 종료하면 파일의 복구는 불가능하다.

그림 2-17 | 게임에서 고득점 요구하는 렌센웨어(RensenWare)

8) 다시 돌아온 록키 (2017.04.28)

2016년 케르베르와 함께 랜섬웨어 양대 산맥을 구축했지만 2017년부터 갑자기 종적을 감췄던 록키(Locky)랜섬웨어가 지난 4월 다시 등장했다.

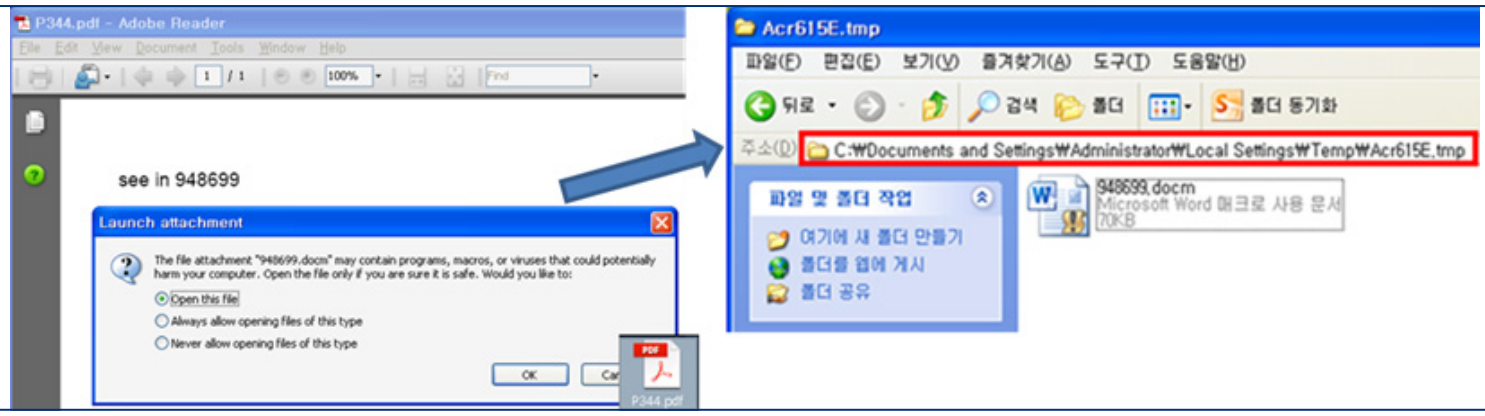


그림 2-18 | 록키(Locky)의 귀환

이번에 발견된 록키 랜섬웨어의 암호화 방식과 랜섬노트는 작년 말에 활동하던 방식과 동일하지만,

유포 방식의 경우 사용자가 스팸 메일에 첨부된 PDF 파일을 실행하면 악성 DOCM 파일을 다운로드하고 실행하도록 유도하는 방식으로 변경되었다.

9) 윈도우 취약점을 악용한 역대급 랜섬웨어, 워너크립터 (2017.05.12)

지난 2017년 4월, 해킹 그룹 쉐도우 브로커스(Shadow Brokers)가 '이터널블루(Eternal Blue)'라는 윈도우 운영체제 취약점을 공개했다. 해당 취약점을 악용한 워너크립터(WannaCryptor) 랜섬웨어는 5월 12일 전 세계적으로 확산됨과 동시에 약 120여개국에 있는 25만대 이상의 PC에 감염 피해를 입혔다.

워너크립터는 이미 지난 4월 12일에 국내에서도 언급된 바 있어, 새로운 랜섬웨어라고 하기는 어렵다. 해외에서는 WCry, WannaCry, WannaCrypt0r, WannaCrypt 등의 이름으로 알려져 있고, 안랩에서는 워너크립터(WannaCryptor)라는 명칭으로 통일하여 사용한다.

워너크립터는 이터널블루라는 SMB(Server Message Block) 프로토콜 취약점과 악성코드 감염 기법인 더블펄사(Double Pulsar)를 통해 급속도로 확산되었다. 특히 해당 기법은 감염된 PC가 연결된 LAN 네트워크 상의 다른 PC를 감염시키는 기법으로 워너크립터가 더욱 빠르게 퍼져나간 요인으로 작용했다.

한편 이터널블루 취약점을 이해하기 위해서는 쉐도우 브로커스라는 해킹 그룹을 주목할 필요가 있다. 이미 2013년에 에드워드 스노든이 미국 국토안보국(NSA) 의 프리즘(PRISM)이라는 사이버 감시 및 첩보 활동에 대해 폭로한 적이 있다. 특히 2016년 8월에 쉐도우 브로커스가 NSA에서 사용한 해킹 툴들을 유출한 사건이 발생하면서 NSA의 감시 활동은 거의 사실로 받아들여졌다.

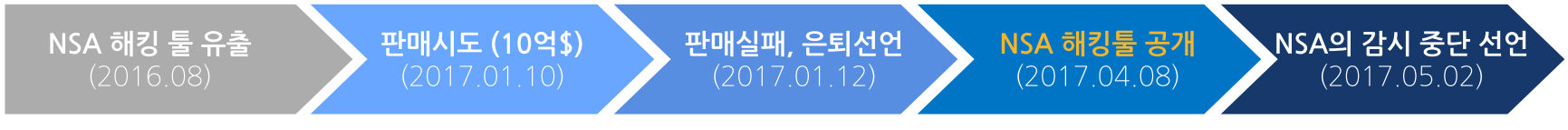


그림 2-19 | 쉐도우 브로커스(Shadow Brokers)의 해킹 툴 공개

쉐도우 브로커스는 지난 2017년 1월 10일 10억 달러(약 1조 2천억원)에 해당 해킹 툴 판매를 시도하다가 실패한 이후, 4월 8일에 해당 툴을 인터넷에 공개해버린 바 있다. 이어서 4월 22일에는 이터널블루와 더블펄사 기법을 공개했다. 해당 기법은 윈도우 운영체제에서 사용하는 SMB 프로토콜 취약점에 대한 것이므로 이미 3월에 마이스로소프트에서 해당 취약점에 대한 보안 업데이트를 발표했다. 그러나 당시에는 윈도우 XP, 2003 등 지원이 종료된 운영체제에 대한 보안업데이트는 제공하지 않아, 5월 12일에 구버전 운영체제를 포함하는 긴급 패치를 추가로 발표했다.

워너크립터는 유포되는 압축 파일 내부에 있는 파일을 해당 국가에 맞는 버전으로 압축 해제한다. 한국어를 포함한 다양한 언어를 지원하며 감염되면 토르(Tor) 클라이언트 파일을 다운로드하고 설치한다. 데이터베이스 서버 또는 메일 서버 관련 프로세스가 존재하면 종료한 다음 암호화를 진행한다. 암호화된 파일에 WNCRY, WCRY, WCRCRT 등의 확장자명을 추가하며, 암호화된 파일의 시작 부분에 WANACRY! 문자열을 추가하는 것이 특징이다.

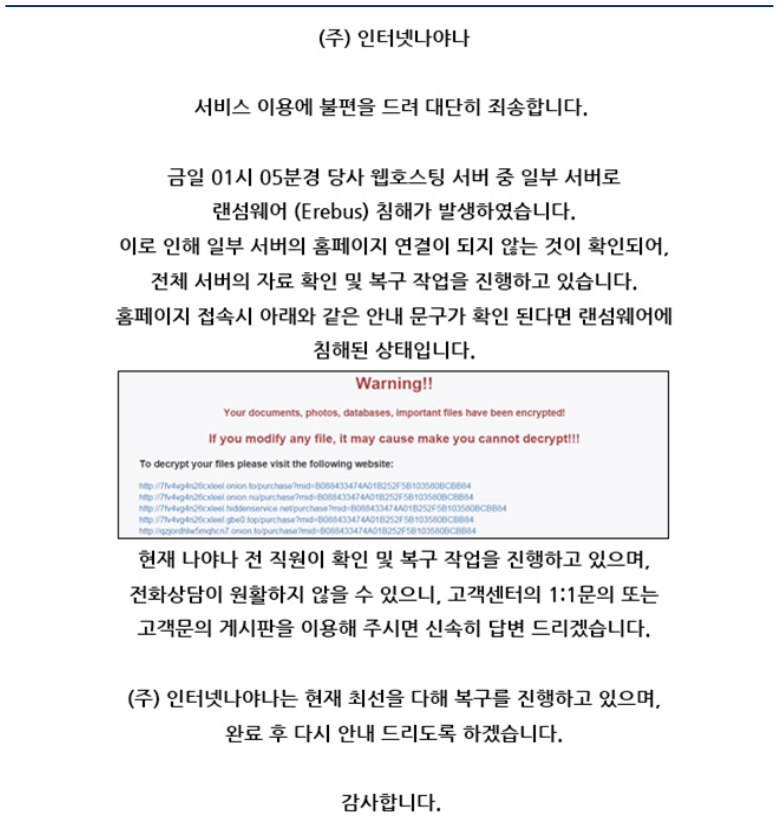
그림 2-20 | 전 세계를 강타한 워너크립터(WannaCryptor)

그림 2-21 | 워너크립터(WannaCryptor)의 등장

5월 13일과 15일에 워너크립터의 동작을 종료시킬 수 있는 킬스위치(Kill-Switch)가 연이어 발견되면서 랜섬웨어의 활동은 어느 정도 마무리되었다. 국내에서도 피해 사례가 발견되어 외국어 시험 진행이 취소되거나 유명 영화 상영관의 광고 서버가 감염되어 광고 상영이 중단되는 사례도 발생했다.

10) 국내 기업을 파산 위기로 몰고간 에레버스 랜섬웨어

지난 2017년 6월 10일에 국내 웹호스팅 업체인 '인터넷나야나'의 웹 서버와 백업 서버가 에레버스(Erebus) 랜섬웨어에 감염되는 사태가 발생했다. 153대의 서버가 감염되어 암호화되었고, 이로 인해 해당 웹호스팅 업체의 서비스를 받고 있던 약 3천여 업체의 홈페이지가 마비되는 피해를 입었다. 해당 업체는 결국 공격자에게 거액의 복구 비용을 지불하기로 협상하였으나, 이로서 파산 직전의 위기에 몰렸다.


(주) 인터넷나야나

서비스 이용에 불편을 드려 대단히 죄송합니다.

금일 01시 05분경 당사 웹호스팅 서버 중 일부 서버로
랜섬웨어 (Erebus) 침해가 발생하였습니다.
이로 인해 일부 서버의 홈페이지 연결이 되지 않는 것이 확인되어,
전체 서버의 자료 확인 및 복구 작업을 진행하고 있습니다.
홈페이지 접속시 아래와 같은 안내 문구가 확인 된다면 랜섬웨어에
침해된 상태입니다.

Warning!!

Your documents, photos, databases, important files have been encrypted!

If you modify any file, it may cause make you cannot decrypt!!!

To decrypt your files please visit the following website:

현재 나야나 전 직원이 확인 및 복구 작업을 진행하고 있으며,
전화상담이 원활하지 않을 수 있으니, 고객센터의 1:1문의 또는
고객문의 게시판을 이용해 주시면 신속히 답변 드리겠습니다.

(주) 인터넷나야나는 현재 최선을 다해 복구를 진행하고 있으며,
완료 후 다시 안내 드리도록 하겠습니다.

감사합니다.

그림 2-22 랜섬웨어에 의해 피해를 입은 웹호스팅 업체
(*출처: 인터넷나야나 홈페이지)

이번에 발견된 랜섬웨어는 지난 2월 발견된 에레버스 랜섬웨어의 리눅스 버전 변종이다. 때문에 리눅스 서버를 주로 사용하는 웹호스팅 업체가 피해를 입은 것이다. 문제는 해당 웹호스팅 업체가 중소 규모의 업체로, 백업 서버를 망분리 환경이 아닌 일반 서버와 동일한 네트워크 상에서 운영하고 있었다는 점이다. 이로 인해 복구에 필요한 백업 데이터 마저 암호화되었고, 관련 기관의 도움에도 불구하고 피해를 복구할 수 없었다.

4. 결론

2016년이 랜섬웨어의 성장기였다면 2017년은 성숙기라고 해도 과언이 아닐 정도로 올해 상반기에는 새로운 랜섬웨어가 등장하는 동시에 기존 랜섬웨어도 변종을 통해 활동을 재개했다. 워너크립터나 국내 사용자를 대상으로 하는 비너스락커 등과 같이 언론에서 다뤄진 랜섬웨어도 있지만 이들은 빙산의 일각에 불과하다. 최근 국내에 큰 피해를 남긴 에레버스 랜섬웨어의 경우에도 이미 2월에 발견된 적이 있는 랜섬웨어의 변종이다.

한편 2017년 상반기 동향을 통해 알 수 있듯이 랜섬웨어 유포 방식에 있어서는 더 이상 새로울 것이

없었다. 주로 스팸 메일과 익스플로잇 킷(Exploit Kit)을 통해 랜섬웨어가 유포되었으며, 작년에 비해 스팸 메일을 통한 유포는 더욱 증가했다. 이는 이미 20년이 넘도록 악성코드 제작자에게 꾸준히 활용되던 방식이다.

새로운 방법이 아니라는 것은 바꿔 말하면 충분히 예방 가능하다는 것이다. 기본적인 보안 수칙을 준수하는 '한 끗 차이'만으로도 내 파일의 운명을 바꿀 수 있다. 따라서 의심스러운 이메일은 열지 않고, 이메일에 첨부된 파일은 실행하기 전에 백신을 통해 검사하는 등 꼼꼼히 확인해야 한다. 윈도우 및 주요 응용 프로그램의 보안 업데이트를 꾸준히 설치하고 백신 프로그램의 엔진을 항상 최신으로 유지하는 것도 랜섬웨어 피해 예방에 상당한 효과를 볼 수 있다.

갈수록 고도화되는 랜섬웨어 위협은 여전히 적색 경보 수준이다. 계속되는 랜섬웨어 위협에 대비하기 위해 무엇보다도 개개인의 주의와 노력이 필요한 시점이다. 또한 기업 및 기관에서도 보안 솔루션 운영은 물론 프로세스와 내부 임직원의 관리에 대한 실효성 있는 보안 대책 마련이 시급하다.

참고자료

1. CISCO - http://www.cisco.com/c/dam/m/digital/en_us/Cisco_Annual_Cybersecurity_Report_2017.pdf
2. Microsoft Technet - https://blogs.technet.microsoft.com/mmpc/2017/01/23/exploit-kits-remain-a-cybercrime-staple-against-outdated-software-2016-threat-landscape-review-series
3. Microsoft Technet - https://blogs.technet.microsoft.com/mmpc/2017/01/23/exploit-kits-remain-a-cybercrime-staple-against-outdated-software-2016-threat-landscape-review-series
4. 보안뉴스 - http://www.boannews.com/media/view.asp?idx=54228
5. MalwareBytes - https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf
6. Check Point - http://blog.checkpoint.com/2017/03/22/ransomware-not-file-encryption
7. Bleeping Computer - https://www.bleepingcomputer.com/news/security/the-locky-ransomware-is-back-and-still-adding-osiris-to-encrypted-files
8. IBM Security Intelligence - https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam
9. Bleeping Computer - https://www.bleepingcomputer.com/news/security/spam-accounts-for-two-thirds-of-all-email-volume-and-its-still-going-up/
10. MalwareBytes - https://blog.malwarebytes.com/threat-analysis/2017/03/exploit-kits-winter-2017-review/
11. The Hacker News - http://thehackernews.com/2017/04/swift-banking-hacking-tool.html
12. Bleeping Computer - https://www.bleepingcomputer.com/news/security/mongodb-apocalypse-is-here-as-ransom-attacks-hit-10-000-servers/
13. Bleeping Computer - https://www.bleepingcomputer.com/news/security/mongodb-hijackers-move-on-to-elasticsearch-servers/
14. Bleeping Computer - https://www.bleepingcomputer.com/news/security/database-ransom-attacks-hit-couchdb-and-hadoop-servers/
15. Security Affairs - http://securityaffairs.co/wordpress/56660/cyber-crime/mysql-databases-ransom-attacks.html
16. Bleeping Computer - https://www.bleepingcomputer.com/news/government/ransomware-hits-pennsylvania-senate-democrats/
17. Bleeping Computer - https://www.bleepingcomputer.com/news/security/ransomware-incident-shuts-down-countys-government-infrastructure/
18. Security Affairs - http://securityaffairs.co/wordpress/55810/malware/washington-dc-cctv-ransomware.html
19. The Hacker News - http://thehackernews.com/2017/01/ransomware-hotel-smart-lock.html
20. Bleeping Computer - https://www.bleepingcomputer.com/news/security/police-department-loses-years-worth-of-evidence-in-ransomware-incident/
21. ESET - http://www.welivesecurity.com/2017/01/20/ransomware-attack-hits-st-louis-public-library/
22. Security Affairs - http://securityaffairs.co/wordpress/55228/malware/los-angeles-community-college-district.html
23. FireEye - https://www.fireeye.com/blog/threat-research/2017/05/dridex_and_lockyret.html
24. IBM Security Intelligence - https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/
25. Bleeping Computer - https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-adds-ddos-feature/
26. Bleeping Computer - https://www.bleepingcomputer.com/news/security/shadow-brokers-now-selling-windows-exploits-antivirus-bypass-tools/
27. Bleeping Computer - https://www.bleepingcomputer.com/news/security/shadow-brokers-announce-retirement-after-failed-attempts-to-sell-their-hacking-tools/
28. Security Affairs - http://securityaffairs.co/wordpress/55454/hacking/smb-zero-day-exploit.html
29. The Hacker News - http://thehackernews.com/2017/04/nsa-hacking-tools.html
30. Security Affairs - http://securityaffairs.co/wordpress/58025/hacking/shadow-brokers-windows-exploits.html
31. Security Affairs - http://securityaffairs.co/wordpress/58217/hacking/doublepulsar-nsa-massive-attacks.html
32. Security Affaris - http://securityaffairs.co/wordpress/58615/intelligence/nsa-statement-surveillance-activities.html
33. ESET - http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
34. EMSISOFT - http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/
35. Bleeping Computers - https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/
36. Trend Micro - http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-changes-course-triple-checks-security-software/
37. Trend Micro - http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/
38. Bleeping Computer - https://www.bleepingcomputer.com/news/security/rensenware-will-only-decrypt-files-if-victim-scores-2-billion-in-th12-game/
39. Bleeping Computer - https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-using-nsa-exploit-leaked-by-shadow-brokers-is-on-a-rampage/
40. Microsoft Technet - https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
41. Kaspersky - https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
42. The Hacker News - http://thehackernews.com/2017/05/wannacry-ransomware-windows.html
43. MalwareTech - https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
44. Bleeping Computer - https://www.bleepingcomputer.com/news/security/wannacry-ransomware-version-with-second-kill-switch-detected-and-shut-down/
45. Bleeping Computer - https://www.bleepingcomputer.com/news/security/aes-ni-ransomware-dev-claims-hes-using-shadow-brokers-exploits/
46. Trend Micro - http://blog.trendmicro.com/trendlabs-security-intelligence/wannacry-uiwix-ransomware-monero-mining-malware-follow-suit/
47. 디지털데일리 - http://www.ddaily.co.kr/news/article.html?no=156951

ASEC REPORT Vol.87

2017년 2분기

AhnLab

집필 안랩 시큐리티대응센터 (ASEC)

편집 안랩 콘텐츠기획팀

디자인 안랩 디자인팀

발행처 주식회사 안랩

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901