

ASEC REPORT

VOL.80

August, 2016

ASEC REPORT

VOL.80 August, 2016

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

2016년 8월 보안 동향

Table of Contents

1	01 악성코드 통계	4
보안 통계	02 웹 통계	6
STATISTICS	03 모바일 통계	7
2	01 '아이폰 7' 관련 문서로 위장한 악성코드 주의	10
보안 이슈	02 '포켓몬 고(Pokemon Go)' 위장 랜섬웨어 등장	13
SECURITY ISSUE		
3	01 DLL 형태로 돌아온 록키(Locky) 랜섬웨어	17
악성코드 상세 분석		
ANALYSIS-IN-DEPTH		

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

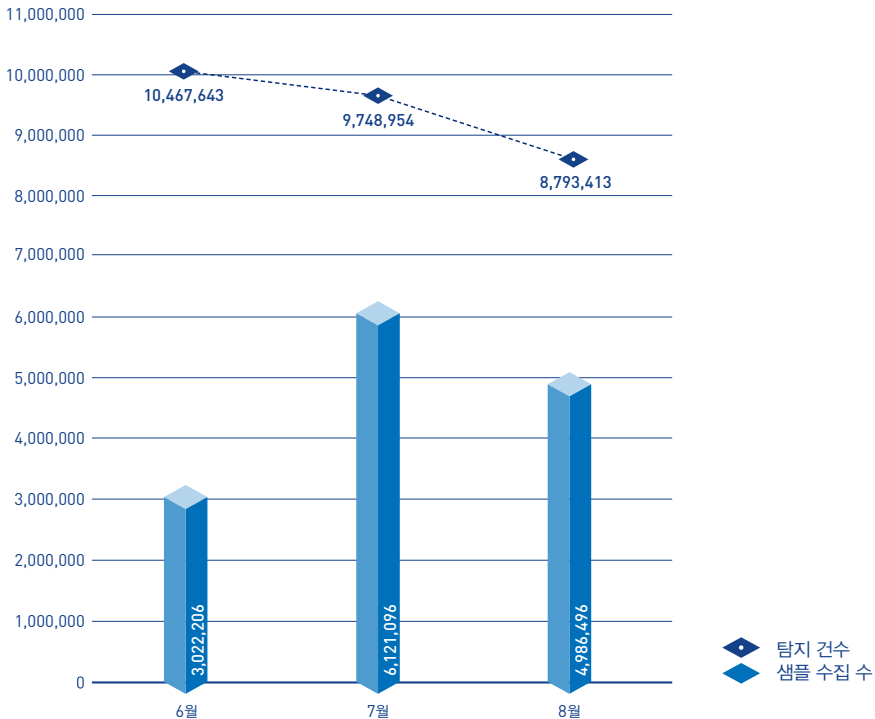
03 모바일 통계

보안 통계

01

악성코드 통계

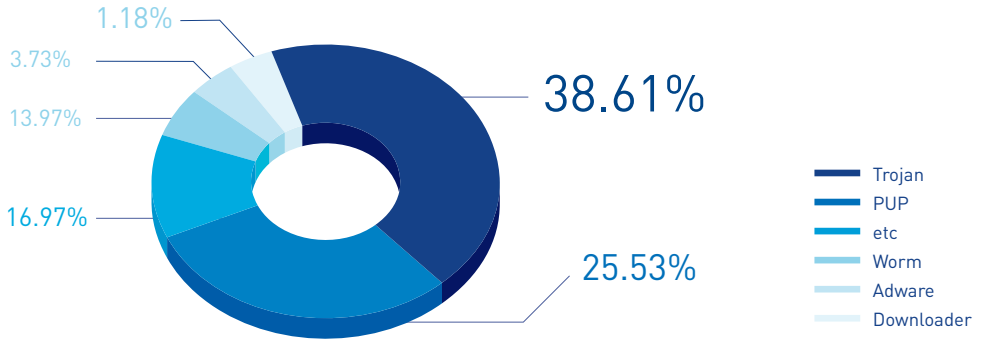
ASEC이 집계한 바에 따르면, 2016년 8월 한 달간 탐지된 악성코드 수는 879만 3,413건으로 나타났다. 이는 전월 974만 8,954건에 비해 95만 5,541건 감소한 수치다. 한편 8월에 수집된 악성코드 샘플 수는 498만 6,496건이다.



[그림 1-1] 악성코드 추이(2016년 6월 ~ 2016년 8월)

* '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.

[그림 1-2]는 2016년 8월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 38.61%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 25.53%, 웜(Worm)이 13.97%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 8월 주요 악성코드 유형

[표 1-1]은 8월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Malware/Win32.Generic이 총 21만 8,089건으로 가장 많이 탐지되었고, Trojan/Win32.Starter가 18만 3,507건으로 그 뒤를 이었다.

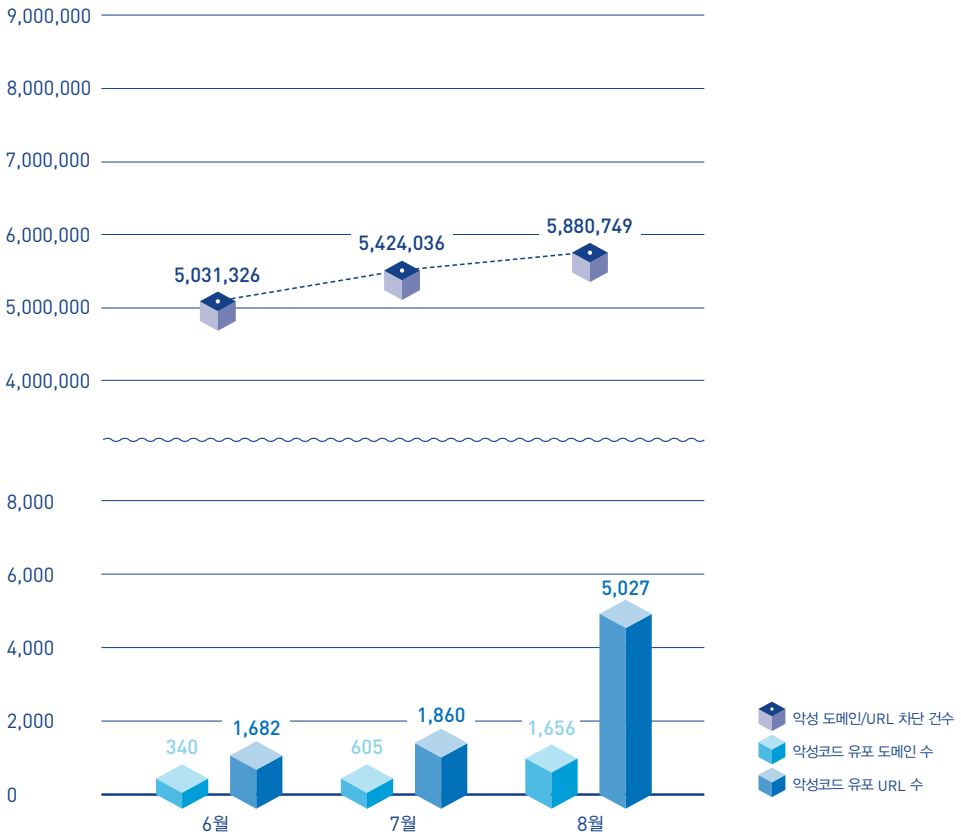
[표 1-1] 2016년 8월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Malware/Win32.Generic	218,089
2	Trojan/Win32.Starter	183,507
3	Unwanted/Win32.HackTool	102,854
4	Trojan/Win32.Neshta	87,818
5	Trojan/Win32.CryptXXX	81,227
6	Trojan/Win32.Banki	80,766
7	Trojan/Win32.Agent	74,148
8	HackTool/Win32.Crack	58,715
9	Adware/Win32.BrowseFox	54,485
10	ASD.Prevention	52,818

보안 통계

02
웹 통계

2016년 8월에 악성코드 유포지로 악용된 도메인은 1,656개, URL은 5,027개로 집계됐다(그림 1-3). 또한 8월의 악성 도메인 및 URL 차단 건수는 총 588만 749건이다.



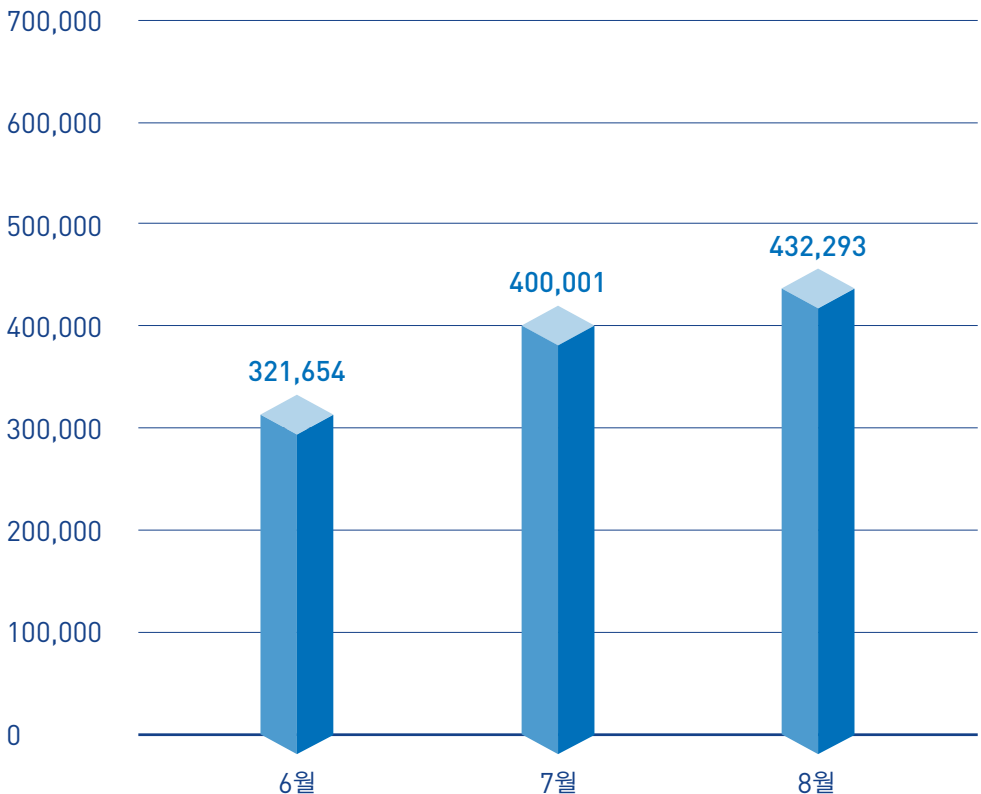
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 6월~2016년 8월)

* 악성 도메인 및 URL 차단 건수란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03

모바일 통계

2016년 8월 한 달간 탐지된 모바일 악성코드는 43만 2,293건으로 나타났다(그림 1-4).



[그림 1-4] 모바일 악성코드 추이(2016년 6월 ~ 2016년 8월)

[표 1-2]는 8월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 8월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	154,907
2	Android-PUP/Shedun	76,665
3	Android-PUP/SmsReg	27,492
4	Android-Trojan/AutoSMS	26,924
5	Android-PUP/Noico	20,143
6	Android-PUP/Zdpay	10,664
7	Android-Trojan/Agent	7,728
8	Android-Trojan/Shedun	7,573
9	Android-Trojan/Hidap	6,006
10	Android-AppCare/Agent	5,030

2

보안 이슈 SECURITY ISSUE

- 01 '아이폰 7' 관련 문서로 위장한 악성코드 주의
- 02 '포켓몬 고(Pokemon Go)' 위장 랜섬웨어 등장

01

‘아이폰 7’ 관련 문서로 위장한 악성코드 주의

최근 아이폰 7 출시와 함께 관련 정보를 담은 문서로 위장하여 사용자를 현혹하는 악성코드가 발견됐다. 악성코드 제작자는 사회적 이슈를 활용하는 전형적인 사회공학기법(Social Engineering)을 이용하여 제품 사양, 디자인 등 출시 전부터 사용자들의 많은 관심을 받은 아이폰 7의 서비스 문서 파일로 위장해 악성코드를 유포시키는 수법을 사용했다.

자를 속여 동의하도록 유도했다.

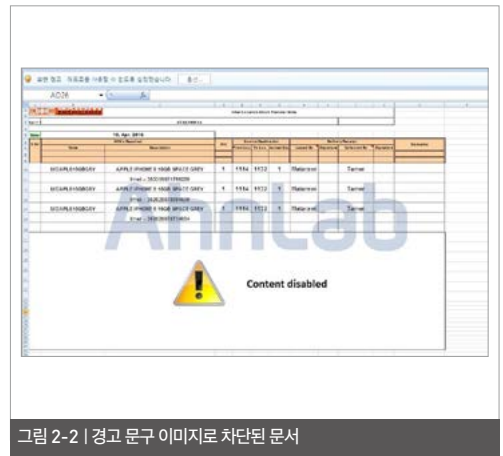


그림 2-2 | 경고 문구 이미지로 차단된 문서

[그림 2-2]의 경고 문구는 이미지로 제작되어 있으며, 해당 이미지를 드래그하면 뒤에 있는 문서 내용을 확인할 수 있다. 따라서 사용자가 매크로 실행 동의를 하지 않아도 실제로는 내용 확인이 가능하다. 악성코드 제작자는 문서 내용 위에 내용이 제한되었다는 경고 이미지를 덮어쓰는 방법으로 사용자가 매크로 실행을 동의하도록 유도한 셈이다.

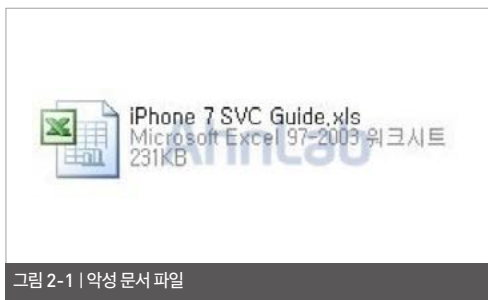


그림 2-1 | 악성 문서 파일

엑셀 파일로 위장한 해당 악성코드는 [그림 2-1]과 같이 사용자들의 호기심을 자극하는 파일명을 사용하고 있다. 해당 파일을 열면 경고 문구와 함께 문서의 일부 내용이 보이지 않는다. 매크로 실행을 동의해야만 문서의 전체 내용을 확인할 수 있는 것처럼 사용

표 2-1 | 네트워크 연결 정보

```
hxxp://217.65.97.52/get/0/9854596/GSX.exe
```

악성 매크로가 실행되면 [표 2-1]의 URL 주소에 연결되며, 네트워크 연결이 이뤄지면 해당 주소에서 악성코드를 다운로드한다.

표 2-3 | 변경된 레지스트리 항목

```
HKCU\Software\Microsoft\Windows NT\
CurrentVersion\Windows\Load
```

```
"C:\Documents and Settings\administrator\Local
Settings\Temp\FolderN\name.exe"
```

변경된 레지스트리 항목은 시스템이 시작될 때마다 레지스트리 값에 해당하는 경로의 악성 파일이 자동으로 실행될 수 있도록 한다.

이번 사례와 같이 많은 사람들이 관심을 갖는 사회적 이슈나 사용자들의 호기심을 이용한 사회공학기법 (Social Engineering)은 공격자들이 선호하는 기법 중 하나다. 앞으로도 이를 이용한 악성 메일, 악성 URL 링크, 악성 동영상 등이 꾸준히 유포될 가능성이 있어 사용자들의 주의가 필요하다.

또한 정상 문서 파일로 위장한 악성 파일은 주로 메일을 통해 유포되므로 발신자가 불분명한 메일은 가급적 열어보지 않는 것을 권장한다. 메일 혹은 웹에 의심스러운 문서 파일이 첨부되어 있는 경우에는 해당 첨부 파일을 실행하기 전 한 번 더 확인하는 등 각별히 주의해야 한다.

표 2-2 | 파일 생성 정보

```
C:\Documents and Settings\administrator\Local
Settings\Temp\svhost.exe
```

```
C:\Documents and Settings\administrator\Local
Settings\Temp\FolderN\name.exe
```

악성 파일이 생성된 이후에는 [표 2-3]과 같이 레지스트리를 변경한다.



그림 2-3 | 다운로드된 악성 파일

시스템에 다운로드된 악성 exe 파일은 사용자의 의심을 피하기 위해 [그림 2-3]과 같이 애플사의 로고와 유사한 이미지를 사용하고 있다. 이 악성 파일을 실행하면 [표 2-2]와 같은 추가 파일이 생성된다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

X97M/Downloader (2016.07.27.00)

Trojan/Win32.Injector (2016.08.02.04)

02

‘포켓몬 고(Pokemon Go)’ 위장 랜섬웨어 등장

랜섬웨어 유포 방식이 점점 고도화되고 있는 가운데, 최근 증강현실(Augmented Reality, AR) 기술을 접목하여 전세계적으로 인기를 끌었던 모바일 게임 ‘포켓몬 고(Pokemon Go)’로 위장한 랜섬웨어가 등장하여 사용자들을 위협하고 있다.

표 2-4 | 파일 생성 정보

C:\Documents and Settings\Administrator\시작 메
뉴\프로그램\시작프로그램\87121.exe

Drive Root:\PokemonGo.exe

파일이 실행되면 [표 2-4]와 같이 시작 프로그램 경로에 추가 악성 파일을 생성하고, 감염 시스템 내 모든 드라이브 루트에 자기 자신을 복사한 랜섬웨어 실행 파일을 생성한다.

Action Entry	Description	Publisher	Image Path	Timestamp
HKCU\Software\Microsoft\Windows\CurrentVersion\W				2016-08-18 오후 2:07
87121.exe	PokemonGo		c:\PokemonGo.exe	2016-08-12 오후 5:28
C:\Users\Administrator\AppData\Local\Temp\87121.exe			c:\Users\Administrator\AppData\Local\Temp\87121.exe	2016-08-18 오후 2:03

그림 2-5 | 자동 실행 프로그램

이번에 발견된 랜섬웨어는 [그림 2-4]와 같이 게임의 대표 캐릭터를 아이콘으로 사용하여 사용자가 정상적인 게임을 실행하는 것처럼 인식하도록 위장했다. 그러나 실제로는 시스템 내 문서 파일을 암호화하는 랜섬웨어다.

이때 생성된 악성 파일은 시스템이 다시 시작될 때마다 자동 실행되며, [표 2-5]와 같이 시스템의 레지스트리 항목을 변경한다. UserList 항목에 ‘Hack3r’ 레지스트리를 추가하여 시스템에 ‘Hack3r’의 이름

으로 관리자 계정을 생성한다.

표 2-5 | 변경된 관리자 계정 레지스트리 항목

HKLM\Software\Microsoft\Windows NT\
CurrentVersion\Winlogon\SpecialAccounts\
UserList

Hack3r = "0"

또한 레지스트리 추가 시, 값을 0으로 설정해 사용자
에게 해당 계정이 보이지 않게 했다. 실제로는 [그림
2-6]과 같이 'Hack3r'의 이름으로 관리자 계정이 생
성되어 있다.

표 2-6 | 네트워크 연결 정보

10.25.0.169:80



그림 2-7 | 랜섬웨어 감염 시 화면

랜섬웨어에 감염된 시스템의 화면은 [그림 2-7]과 같
이 변경된다. 게임 캐릭터와 함께 보이는 아랍어 메시
지로 보아, 아랍어 사용자를 공격 대상으로 했음을 알
수 있다. 해당 메시지는 PC 내 파일들이 암호화되었
으며, 암호화된 파일을 복구하려면 메일로 연락하라
는 내용이다. 랜섬웨어가 암호화한 대상 파일의 확장
자는 [표 2-7]과 같다.



그림 2-6 | Hack3r 관리자 계정

이후 악성코드는 [표 2-6]의 주소로 네트워크 연결을
시도한다. 분석 당시에는 네트워크 연결로 인한 추가
악성 행위는 이뤄지지 않았다.

표 2-7 | 암호화 대상 파일 확장자

*.txt, *.rtf, *.doc, *.pdf, *.mht, *.docx, *.xls,
*.xlsx, *.ppt, *.pptx, *.png, *.odt, *.jpg, *.png,
*.csv, *.sql, *.mdb, *.sln, *.php, *.asp, *.aspx,
*.html, *.xml, *.psd, *.htm, *.gif

이번에 발견된 랜섬웨어는 교육용으로 제작된 히든 티어(Hidden-Tear) 랜섬웨어의 소스코드를 활용하여 제작된 랜섬웨어로 밝혀졌다. 교육용으로 공개된 소스코드까지 악성 행위에 이용되어 사용자들에게 피해를 주는 만큼, [표 2-8]의 랜섬웨어 예방법을 참고하여 랜섬웨어에 감염되지 않도록 각별히 주의하자.

V3 제품에서는 해당 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Ryzerlo (2016.08.17.00)

Trojan/Win32.Ransom (2016.08.18.04)

표 2-8 | 랜섬웨어 예방법

- 의심스러운 메일의 첨부 파일 열람 금지
- 콘텐츠 불법 다운로드 금지
- 문서(doc, ppt, pdf, hwp), 사진 파일 등 중요 파일의 백업
- 운영체제 및 응용 프로그램의 보안 업데이트 수시 적용: 상당수의 랜섬웨어는 응용 프로그램의 취약점을 통해 드라이브 바이 다운로드(Drive-by-download) 방식으로 유포됨

3

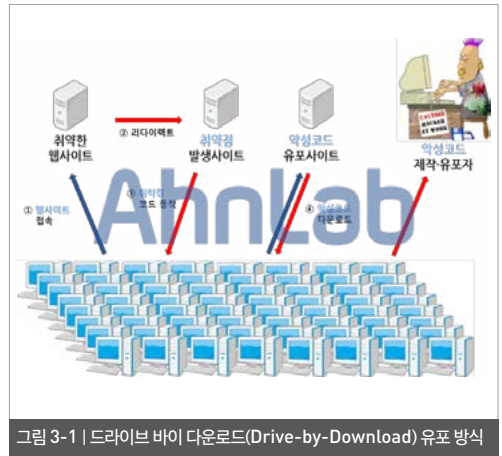
악성코드 상세 분석 ANALYSIS-IN-DEPTH

01 DLL 형태로 돌아온 록키(Locky) 랜섬웨어

01

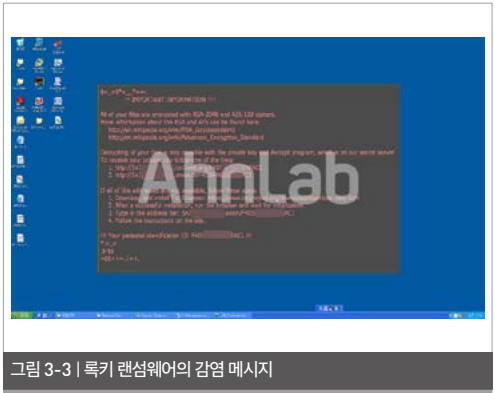
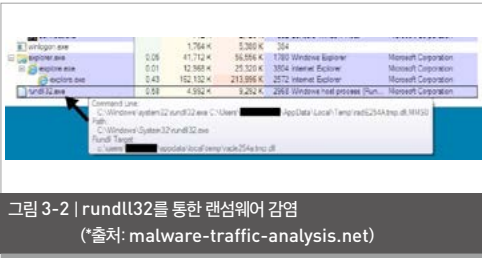
DLL 형태로 돌아온 록키(Locky) 랜섬웨어

지난 2016년 2월 처음 발견된 록키(Locky) 랜섬웨어는 시스템에 심각한 피해를 입히며 이슈가 됐다. 발견 당시 암호화된 파일의 확장자 뒤에 '.locky'를 붙이는 것으로 알려졌지만, 이후에는 확장자를 '.zepto'로 변경하는 록키 랜섬웨어도 발견됐다. 더 나아가 유포 방식 또한 문서 파일로 유포하던 방식에서 스크립트 파일로 유포하는 방식으로 발전했다. 그런데 이번에는 기존의 EXE 형태가 아닌 DLL 형태의 록키 랜섬웨어가 새롭게 발견되어 사용자들의 주의가 요구된다. 지속적으로 변종을 유포하며 사용자들을 위협하는 록키 랜섬웨어를 면밀히 살펴보자.



록키 랜섬웨어 이전에 DLL 파일 유포 방식을 최초로 적용한 랜섬웨어는 '크립트XXX(CryptXXX)'다. [그림 3-1]과 같이 보안이 취약한 웹 사이트에 삽입된 광고 모듈의 취약점을 이용한 멀버타이징(Malvertising) 기법을 사용하여, 드라이브 바이 다운로드(Drive-by-download) 형태로 DLL 파일을 유포해 많은 사용자들에게 큰 피해를 입힌 바 있다.

이번에 발견된 DLL 파일을 이용한 록키 랜섬웨어는 스팸 메일 내에 자바스크립트(js) 형태의 다운로드 파일을 첨부하는 방식으로, 악성코드를 유포하는 방식은 이전과 같다. 달라진 점은 다운로드 악성코드 실행 시 DLL 파일이 임시 폴더에 다운로드되고, [그림 3-2]와 같이 rundll32.exe를 통해 실행된다는 점이다.



스팸 메일을 통해 유입된 JS 파일을 실행하면, 유포지인 [표 3-1]의 URL 주소를 통해 파일이 다운로드된다.

표 3-1 | 유포지 URL 정보

sopranolady7.wang/1cntwk5
ihvr.org/txb1n2bm
da-fortunato.de/fqjold5
spir.50webs.com/52sc0

이때 [표 3-2]와 같이 DLL 파일 형태의 랜섬웨어가 임시 폴더인 %Temp% 경로에 다운로드된다.

표 3-2 | 다운로드된 DLL 파일 경로

%Temp%\1o0cGXH9d.dll

다운로드된 DLL 파일을 실행하면 [그림 3-3]과 같이 바탕화면이 록키 랜섬웨어의 감염 안내 메시지로 변경된다.

록키 랜섬웨어에 감염된 후 변경된 파일의 이름과 확장자는 [표 3-3]과 같다.

표 3-3 | 변경된 파일명 및 확장자

C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-8E79-B65E2228C978.zepto

C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-C81F-576C3AC8C83A.zepto

C:\Documents and Settings\Default User\Templates\F4D5F460-96E9-FAC1-8CE8-B5606E7172D3.zepto

C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-3DFD-709222A3B9BD.zepto

C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-8CCB-7E954797747B.zepto

나날이 진화하는 신·변종 랜섬웨어의 위협이 계속되고 있다. 한번 랜섬웨어에 감염되면 암호화된 파일을 복구하는 것은 거의 불가능하다. 따라서 랜섬웨어는 다른 어떤 악성코드보다 사전 예방이 중요하다. 랜섬웨어 피해 예방을 위해서는 평소 운영체제 및 주요 프로그램의 최신 보안 업데이트를 적용하고, 중요한 데이터는 미리 백업해두는 것이 중요하다. 백업은 랜섬웨어 감염에 대한 사전 예방뿐만 아니라 하드디스크 손상, 운영체제 오류 등으로 인해 시스템을 포맷하게

될 경우에도 유연하게 대처할 수 있는 수단이 될 수 있으므로 주기적으로 해두는 것이 바람직하다.

V3 제품에서는 록키 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Locky (2016.08.24.05)

JS/Obfus.S111 (2016.08.25.00)

AhnLab

ASEC REPORT VOL.80

August, 2016

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

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.