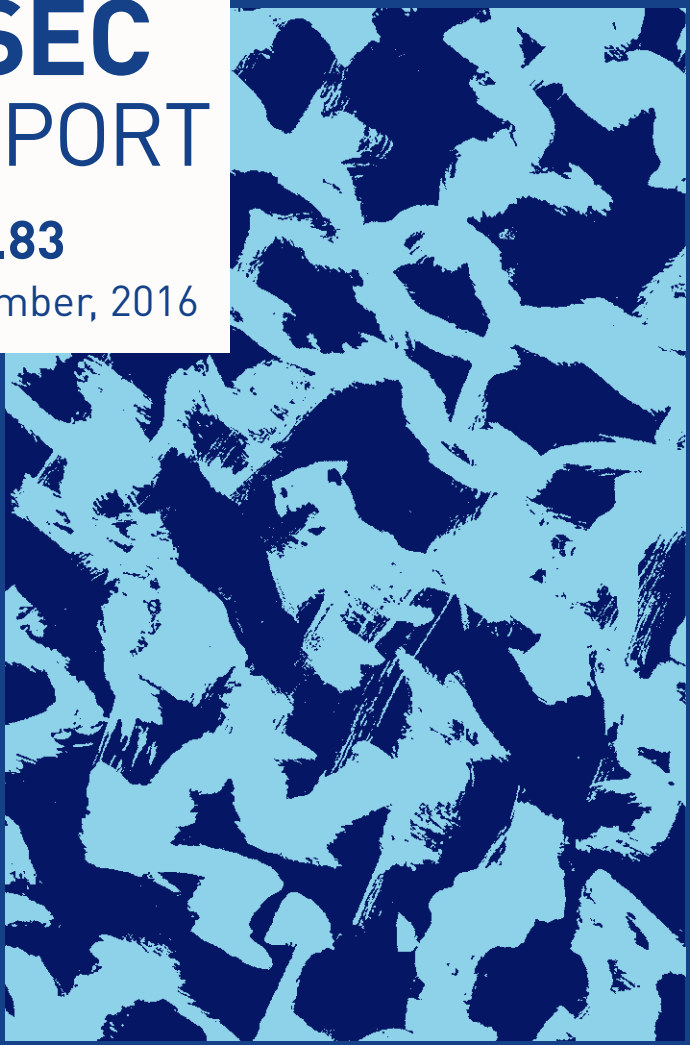
Security Trend

ASEC REPORT

VOL.83

November, 2016



AhnLab

ASEC REPORT

VOL.83 November, 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 11월 보안 동향

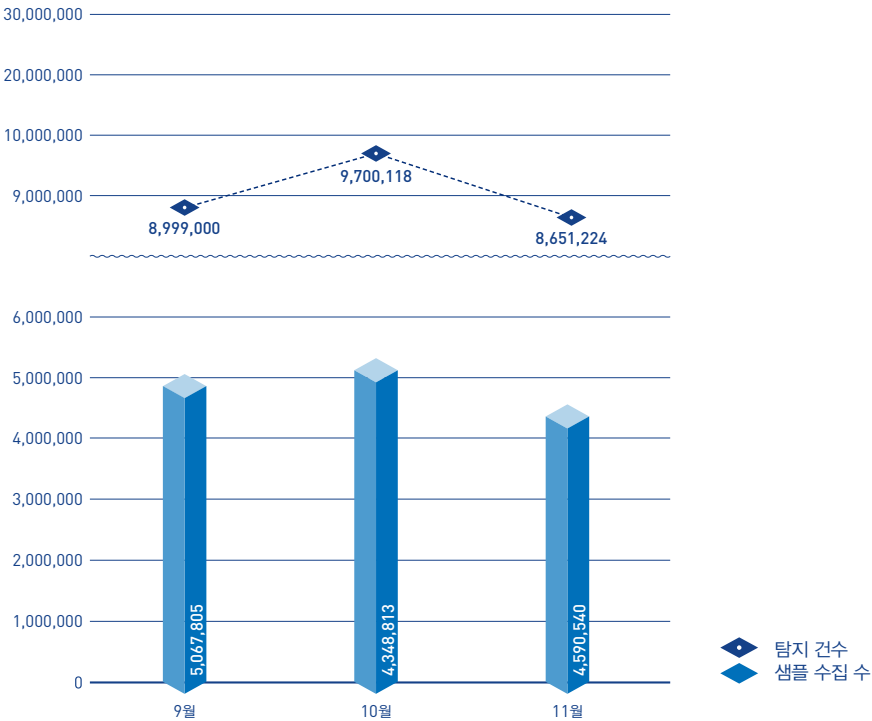
Table of Contents

1

보안 통계
STATISTICS

01 악성코드 통계

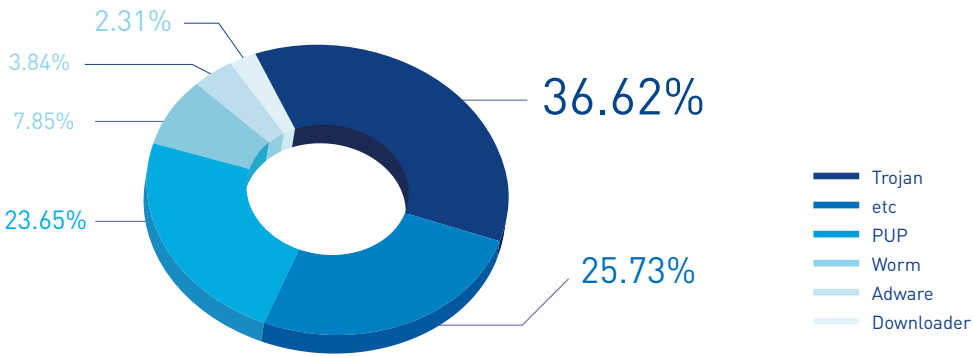
ASEC이 집계한 바에 따르면, 2016년 11월 한 달간 탐지된 악성코드 수는 865만 1,224건으로 나타났다. 이는 전월 970만 118건에 비해 104만 8,894건 감소한 수치다. 한편 11월에 수집된 악성코드 샘플 수는 459만 540건이다.



[그림 1-1] 악성코드 추이(2016년 9월 ~ 2016년 11월)

* '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 11월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이 목마(Trojan) 계열의 악성코드가 36.62%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 23.65%, 웜(Worm)이 7.85%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 11월 주요 악성코드 유형

[표 1-1]은 11월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 22만 8,433로 가장 많이 탐지되었고, Trojan/Win32.Banki가 18만 9,681건으로 그 뒤를 이었다.

[표 1-1] 2016년 11월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	228,433
2	Trojan/Win32.Banki	189,681
3	Malware/Win32.Generic	184,113
4	Worm/Win32.IRCBot	141,246
5	Dropper/Win32.Betabot	119,983
6	Unwanted/Win32.HackTool	116,770
7	Trojan/Win32.Cerber	82,922
8	Trojan/Win32.Neshta	75,557
9	Trojan/Win32.Agent	74,760
10	Trojan/Win32.Nitol	66,233

02
웹 통계

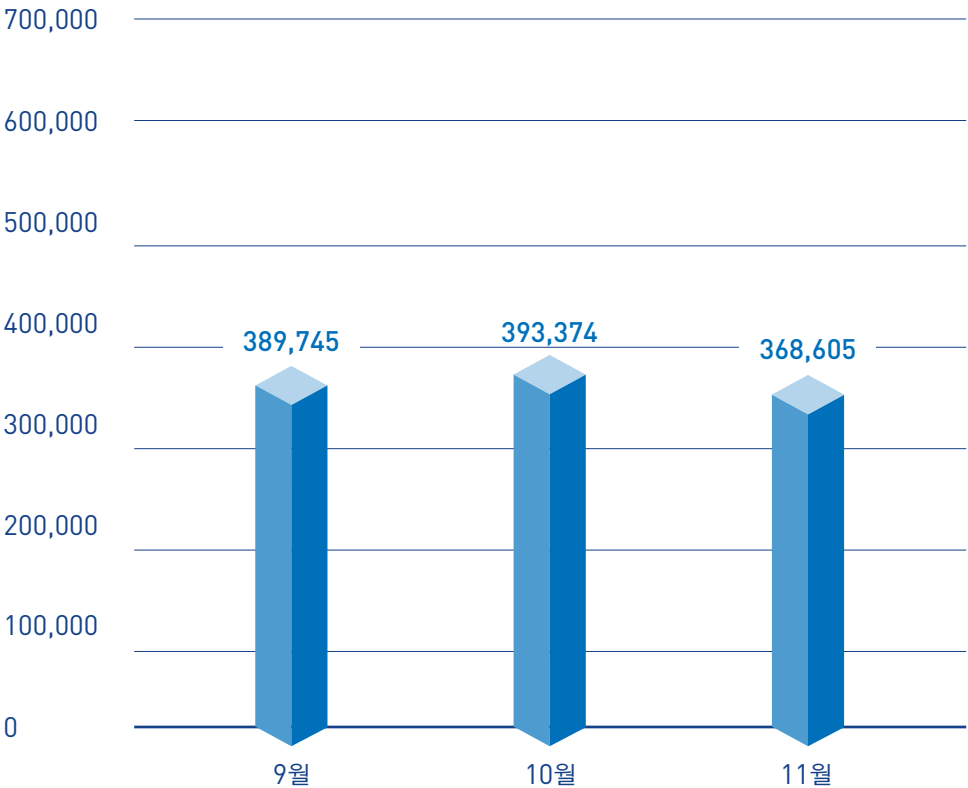
2016년 11월에 악성코드 유포지로 악용된 도메인은 10,193개, URL은 11,165개로 집계됐다([그림 1-3]). 또한 11월의 악성 도메인 및 URL 차단 건수는 총 396만 3,654건이다.

[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 9월~2016년 11월)

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

03
모바일 통계

2016년 11월 한 달간 탐지된 모바일 악성코드는 36만 8,605건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 11월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/Baogifter 가 가장 많이 발견되었다.

[표 1-2] 2016년 11월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/Baogifter	67,949
2	Android-PUP/SmsPay	43,976
3	Android-Trojan/SmsSpy	28,329
4	Android-PUP/Agent	24,761
5	Android-PUP/Shedun	18,916
6	Android-Trojan/Moavt	18,747
7	Android-PUP/SmsReg	15,548
8	Android-Trojan/SmsSend	13,044
9	Android-Trojan/Agent	11,076
10	Android-PUP/Noico	7,615

2

보안 이슈
SECURITY ISSUE

01 악성 SWF 파일 속 숨겨진 랜섬웨어 주의!

랜섬웨어가 점점 진화된 유포 방식으로 사용자들을 끊임없이 위협하고 있는 가운데, 최근 록키(Locky), 케르베르(Cerber)와 같은 랜섬웨어를 다운로드하여 실행하는 SWF 형식의 플래시 파일(Flash File)이 유포되어 사용자들의 주의가 필요하다.

랜섬웨어 다운로드를 목적으로 하는 악성 플래시 파일의 대다수는 웹 서버에서 동작하는 공격용 소프트웨어인 익스플로잇 킷(Exploit Kit)을 통해 유포되는데, 이번에 발견된 악성 SWF 파일은 내부에 암호화된 플래시 파일을 가지고 있는 유형이다.

먼저 해당 악성 SWF 파일의 내부 구조를 살펴보자. [그림 2-1]과 같은 파일 구조로 되어 있으며, 스크립트 코드를 살펴보면 플래시 파일에서 사용하는 스크립트 언어인 액션스크립트(ActionScript)를 사용하고 있다.

그림 2-1 | 플래시 파일 구조와 스크립트 코드

해당 스크립트 코드는 파일 실행 시 [그림 2-2]와 같은 일련의 과정을 통해 내부에 암호화된 데이터를 복호화하는데, 내부 데이터 복호화 과정 중 특이 사항은 '③ 복호화'에 해당하는 스크립트 코드가 정상적으로 파싱(parsing)되지 않는다는 점이다.

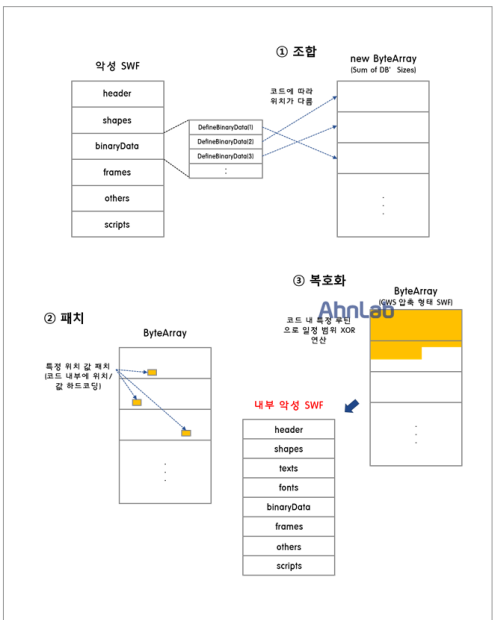


그림 2-2 | 내부 데이터 복호화 과정

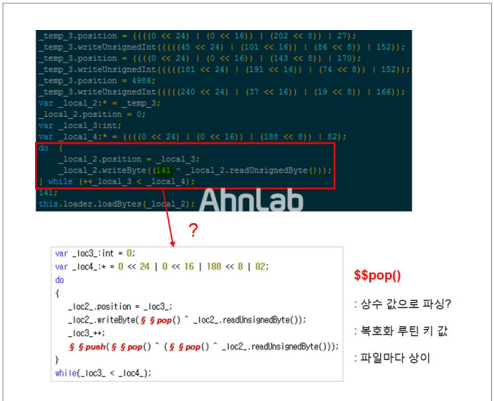


그림 2-3 | 정상 파싱이 되지 않은 스크립트 코드

[그림 2-3]과 같이 정상 파싱이 되지 않은 해당 스크립트 코드는 [그림 2-4]와 같은 XOR 연산을 거쳐 복호화된다. 복호화가 완료되면 압축된 형태의 플래시 파일을 확인할 수 있다. 이때 압축 라이브러리인 'zlib'을 사용하여 압축된 해당 플래시 파일의 시그니처는 'CWS'다.

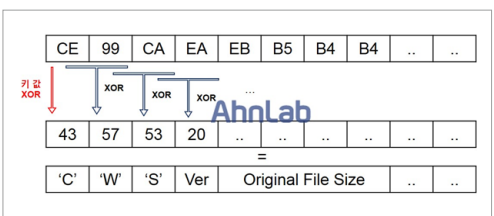


그림 2-4 | XOR 연산 과정

실제 악성코드 실행 과정에서는 내부 파일이 메모리 내에서 복호화되어 실행되기 때문에 파일로 생성되지 않아 직접 확인이 불가능하하다. 그러나 메모리 덤프를 통해 [그림 2-5]와 같이 복호화 후 생성된 플래시 파일을 확인할 수 있다.

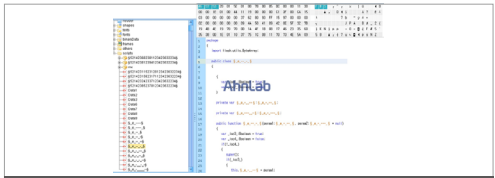


그림 2-5 | 복호화 후 생성된 플래시 파일 구조 및 스크립트

최근 익스플로잇 킷을 통해 유포된 플래시 파일은 내부에 쉘코드(Shellcode)나 또 다른 악성 파일을 가지고 있는 경우가 많다. 또한 파라미터를 통해 악성코드 다운로드 URL을 전달받아 랜섬웨어를 다운로드하는 기능을 가지고 있다.

이번에 발견된 악성 SWF 파일을 또한 동일한 기능을 가지고 있으며, 추가로 플래시 파일 내부에 암호화된 데이터가 존재하여 복호화 시 또 다른 악성 플래시 파일을 확인할 수 있다.

이번 사례와 같이 주요 응용 프로그램 취약점을 이용하는 익스플로잇 킷의 공격으로 인한 피해를 예방하기 위해서는 확인되지 않은 사이트나 불필요한 사이트 이용을 자제하는 것이 바람직하다. 또한 OS 및 주요 응용 프로그램의 최신 보안 패치를 적용하고 V3 등 백신 프로그램의 엔진을 항상 최신 버전으로 유지하는 것이 중요하다.

V3 제품에서는 해당 유형의 악성 플래시 파일을 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

SWF/Exploit (2016.09.02.00)

02
워드 폼 개체를 활용한 악성코드: VBA 매크로 주의보

마이크로소프트 오피스 워드(Microsoft Office Word) 파일을 이용한 보안 위협은 지속적으로 발견되고 있는 위협 중 하나다. 사용자 수가 많은 만큼 워드 파일을 이용한 보안 위협이 꾸준히 증가하고 있는 가운데, 최근에는 사회공학기법(Social Engineering)을 이용하여 스팸 메일을 통해 유포된 악성 워드 파일이 발견되어 사용자들의 각별한 주의가 필요하다.

공격자는 [그림 2-6]과 같이 워드 프로그램의 사용자 정의 폼 기능을 악용하여 악성코드를 유포했다. 해당 악성코드는 응용 프로그램의 확장을 위한 프로그래밍 언어인 VBA(Visual Basic for Applications) 매크로를 이용하고 있다. 사용자 정의 폼 내부에 암호화된 쉘코드(Shellcode)와 숨겨진 악성 실행 파일을 통해 정상 프로세스에 인젝션(Injection)되어 악성 행위를 수행하는 방식이다.

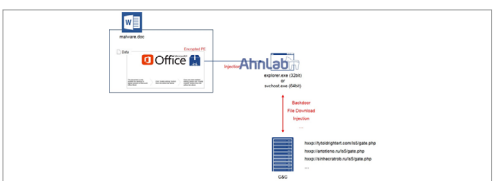


그림 2-6 | 악성 행위 수행 과정

해당 악성 워드 파일은 먼저 [그림 2-7]과 같은 본문 이미지를 통해 사용자의 매크로 실행을 유도한다.

그림 2-7 | 본문 이미지

공격자가 악용한 사용자 정의 폼 기능은 '체크 박스', '라디오 버튼', '텍스트 박스' 등과 같이 응용 프로그램과 사용자의 상호 작용을 위해 필요한 컨트롤들을 사용자가 직접 작성하는 기능이다. [그림 2-8]과 같이 VBA 편집기 내부의 VBA 프로젝트에서 확인할 수 있다.

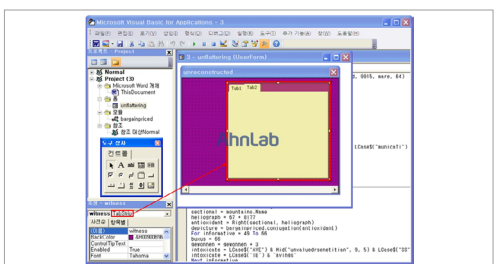


그림 2-8 | 매크로와 사용자 정의 폼

매크로는 사용자 정의 폼 내부에 암호화된 쉘코드를 복호화한 후 실행하기 위해 [그림 2-9]와 같이 사용자 정의 폼 내의 탭스트립(TabStrip) 컨트롤에 접근한다.

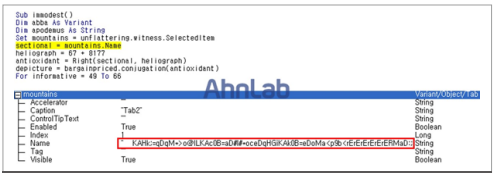


그림 2-9 | 탭스트립(TabStrip) 컨트롤을 이용하는 매크로

이때 쉘코드에 해당하는 데이터는 워드 파일을 압축 해제할 때 생성되는 바이너리 파일 내부에서도 확인 가능하다.

그림 2-10 | 암호화된 쉘코드

매크로 코드는 [그림 2-9]에서 가져온 데이터를 복호화하는 작업을 수행하는데, 해당 복호화 작업을 도식화하면 [그림 2-11]과 같다.

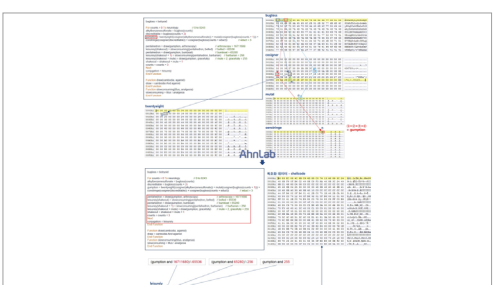


그림 2-11 | 쉘코드 복호화 과정

매크로는 모듈 내부의 'RtlMoveMemory', 'VirtualAllocEx', 'EnumTimeFormatsW' API를 사용하여 복호화된 쉘코드를 실행시킨다. 이때 쉘코드는 [그림 2-12]와 같이 워드 프로그램의 프로세스 메모리 영역 안에서 특정 마커(Marker)를 비교하는 루틴을 통해 암호화된 악성 실행 파일의 위치를 찾게 된다.

에그 헌팅(egg hunting)이라고 부르는 이와 같은 기법은 최초 쉘코드를 통해 특정 마커와 동일한 태그를 가진 실제 메인 코드를 찾아 실행시키는 일련의 과정을 의미한다.

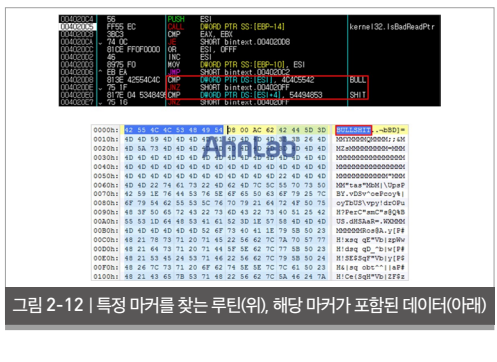


그림 2-12 | 특정 마커를 찾는 루틴(위), 해당 마커가 포함된 데이터(아래)

쉘코드가 특정 마커를 가진 메모리 영역을 발견하면 [그림 2-13]과 같은 코드를 통해 마커 뒷부분에 존재하는 데이터를 1차 복호화한다.

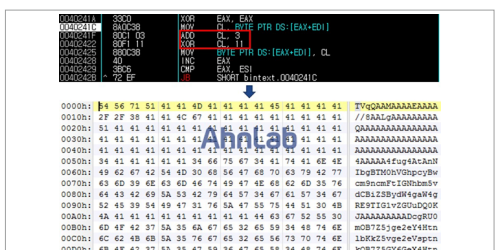


그림 2-13 | 1차 복호화(위), 복호화 후 생성되는 데이터(아래)

1차 복호화 후 생성된 데이터를 Base64 디코딩 과정을 거쳐 2차 복호화하면 [그림 2-14]와 같이 실제 악성 행위를 수행하는 실행 파일을 확인할 수 있다. 이후 쉘 코드는 정상 프로세스에 생성된 실행 파일을 인젝션하기 위한 준비를 한다.

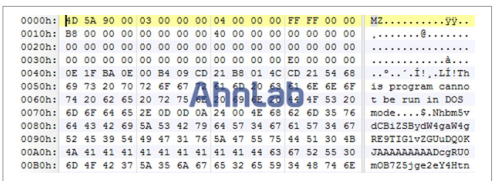


그림 2-14 | Base64 디코딩 과정을 통해 생성된 실행 파일 (일부)

[그림 2-15]와 같이 현재 실행되고 있는 운영체제 환경에 따라 인젝션 대상 프로세스가 달라지는데, 32비트 계열에서는 '%windir%\explorer.exe' 파일을, 64비트 계열인 경우에는 '%windir%\SysWOW64\svchost.exe' 파일을 절전모드(Suspend Mode)로 실행하여 인젝션 행위를 수행한다.

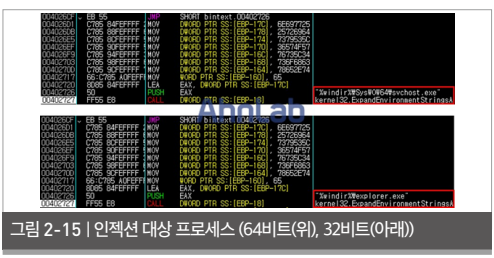


그림 2-15 | 인젝션 대상 프로세스 (64비트(위), 32비트(아래))

정상 프로세스로 위장하기 위한 인젝션이 완료되면 [그림 2-16]과 같이 감염 PC 의 사용자 및 시스템 정보 등을 C&C 주소로 전송한다. 또한 해당 주소로부터 명령을 받아 악성 파일을 다운로드하고 추가 인젝션 행위 등을 수행한다.

그림 2-16 | 인젝션된 파일이 수행하는 악성 행위

이번 사례처럼 VBA 매크로와 사용자 정의 폼을 이용한 악성 워드 파일은 사회공학적 기법을 이용한 스팸 메일을 통해 유포되는 경우가 많다. 또한 문서 파일 내부의 이미지를 통해 사용자로 하여금 큰 의심없이 매크로를 실행시키도록 유도하기 때문에 주의해야 한다. 따라서 사용자는 출처를 알 수 없는 메일의 첨부 파일 실행을 되도록 삼가고 확인되지 않은 문서 파일 내부의 매크로를 실행할 때에는 각별한 주의가 필요하다.

V3 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

W97M/Hancitor (2016.11.24.07)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

01 변화를 거듭하는 록키 랜섬웨어 변종 3종 분석

록키(Locky) 랜섬웨어의 변신은 끝이 없다. 2016년 2월 처음 등장한 이후 현재까지 활발하게 발견되고 있을 뿐만 아니라 지속적으로 신 • 변종으로 진화하고 있다. 록키 랜섬웨어는 봇넷을 통해 스팸 메일의 첨부 파일로 대량 유포되는 것이 특징이며, 위장하는 첨부 파일의 형식 또한 기존 DOCX 형태의 문서 파일을 시작으로 JS(Java Script), WSF(Windows Script File), HTA(Hyper-Text Application), 그리고 최근에는 윈도우 바로가기 형식의 LNK까지 등장했다.

사용자 PC의 파일들을 암호화한 후 변경하는 파일의 확장자명도 지속적으로 변화해왔다. 초기의 '.locky'를 시작으로 '.zepto', '.odin', '.shit', '.thor'에 이어 '.aesir'라는 확장자명을 가진 변형까지 최근 새롭게 발견됐다. 유포 방식은 기존 록키 랜섬웨어와 동일하게 스팸 메일에 포함된 첨부 파일 형식이며, 사용자가 메일에 첨부된 다운로더를 실행하면 실제 랜섬웨어 행위를 수행하는 악성 실행 파일이 다운로드되는 방식이다.

확장자명을 변경하며 끊임없이 변화를 거듭하고 있는 록키 랜섬웨어 변종 3종(shit, thor, aesir)을 자세히 살펴보자.

1. 확장자명을 '.shit'으로 변경하는 록키 랜섬웨어

기존 록키 랜섬웨어와 동일하게 JS(Java Script) 파일 형식을 통해 유포된 이 록키 랜섬웨어의 특징은 일반적으로 ZIP 파일 형식으로 압축된 것이다. 사용자가 해당 ZIP 파일의 압축을 해제한 뒤 내부의 JS 파일을 더블 클릭하여 실행하는 순간, [그림 3-1]과 같은 랜섬웨어 다운로더를 통해 감염이 시작된다.

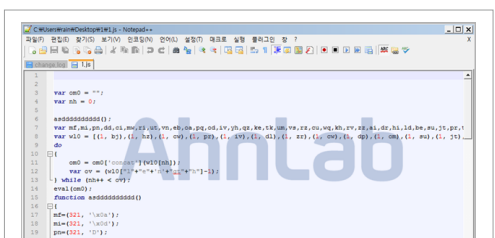


그림 3-1 | 난독화 되어있는 Java Script 형식의 랜섬웨어 다운로더

난독화된 랜섬웨어 다운로더의 스크립트가 실행되면 [표 3-1]의 IP와 URL 주소로 접속하여 악성 DLL 파일을 다운로드한다.

표 3-1 | DLL 파일을 다운로드 하는 URL과 IP 정보

coreywallace.com/qjkrlxp 74.220.199.24:80

그 후, [표 3-2]의 경로에 DLL 파일을 생성한 뒤, 기존 록키 랜섬웨어와 마찬가지로 해당 파일을 rundll32.exe를 통해 로드하여 파일 암호화를 진행한다.

표 3-2 | 악성 DLL 파일이 PC에 저장되는 경로

C:\Documents and Settings\Administrator\Local Settings\Temp\VFVGY7may1.dll

결과적으로 해당 랜섬웨어에 감염되면, 사용자 PC 내 파일들은 [그림 3-2]와 같이 암호화되어 파일명과 확장자명이 변경된다. 파일명은 총 32자의 문자열로 변경되며, 앞의 16자의 문자열은 고정되어 있는 것으로 보아 감염된 PC의 고유값인 것으로 추정된다. 또한 확장자명으로 '.shit'이 추가된다. 이전 록키 랜섬웨어의 확장자명은 기존 '.locky'에서 '.zepto'로 변경되는데 4개월, '.zepto'에서 '.odin'으로 변경되는데 3개월 소요된 것에 반해, 이와 같은 '.shit' 확장자명은 약 1달 만에 변경되는 특징을 보였다.

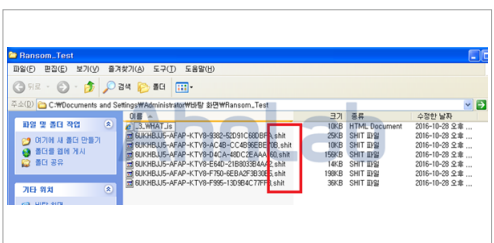


그림 3-2 | 암호화 후 추가되는 확장자명 '.shit'

2. 확장자명을 '.thor'로 변경하는 록키 랜섬웨어

앞서 다룬 확장자명을 '.shit'으로 변경하는 록키 랜섬웨어에 이어, 하루만에 등장한 또 다른 변종은 확장자명을 '.thor'로 변경하는 록키 랜섬웨어다. 전체적인 감염 과정은 앞서 살펴본 확장자명을 '.shit'으로 변경하는 랜섬웨어와 동일하다. [그림 3-3]과 같이 영문으로 된 스팸 메일에 ZIP 파일을 첨부하여 유포하는 특징 또한 동일하다.

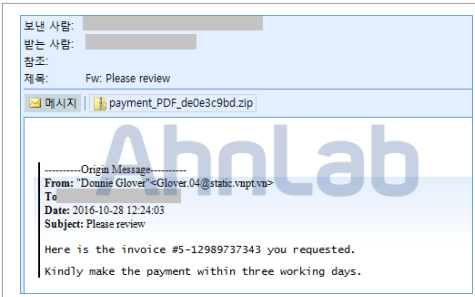


그림 3-3 | 기존 록키 랜섬웨어 유포 방식과 동일한 스팸 메일

단, 확장자명을 '.shit'으로 변경하는 록키 랜섬웨어는 ZIP 파일 내부에 JS(Java Script)가 포함되어 있었던 반면, 이번에 발견된 '.thor' 록키 랜섬웨어는 [그림 3-4]와 같이 VBS(Visual Basic Script) 파일을 포함하고 있다.

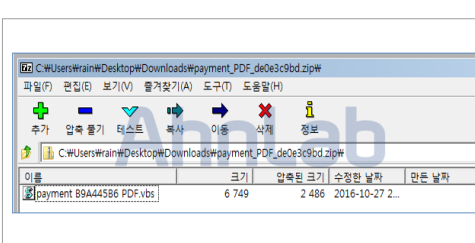


그림 3-4 | ZIP 파일 내부에 포함 된 VBS(Visual Basic Script) 파일

또한, ZIP 파일 내부에 있는 VBS 파일은 [그림 3-5]와 같이 기존 JS와 동일하게 알아보기 어렵도록 난독화 되어 있다.

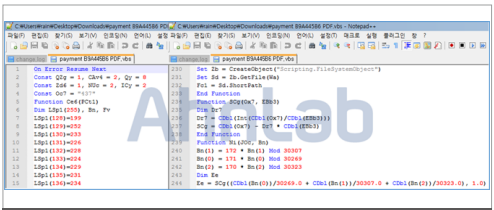


그림 3-5 | 난독화 되어 있는 VBS (Visual Basic Script) 형식의 랜섬웨어 다운로더

암호화가 완료되면 확장자명을 변경하는 록키 랜섬웨어 변종과 마찬가지로 [그림 3-6]과 같이 확장자명을 '.thor'로 변경한다. 그리고 기존 록키 랜섬웨어와 같이 파일명은 총 32자의 문자열로 변경되는데, 앞에 16자는 고정되어 있는 것으로 보아 감염된 PC의 고유값인 것으로 보인다.

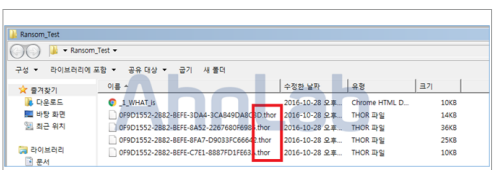


그림 3-6 | 암호화 후 추가되는 확장자명 '.thor'

3. 확장자명을 '.aesir'로 변경하는 록키 랜섬웨어

이번엔 확장자명을 '.aesir'로 변경하는 록키 랜섬웨어 변종을 살펴보자. 해당 랜섬웨어는 전형적인 록키 랜섬웨어 유포 방식처럼 스팸 메일의 첨부 파일로 다운로더가 유포되는데, 이때 다운로더를 실행하면 [그림 3-7]과 같이 실제 랜섬웨어 행위를 수행하는 악성 실행 파일이 다운로드된다.

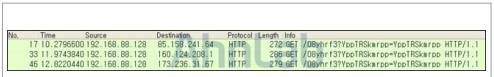


그림 3-7 | 실행 파일 다운로드

유포지의 URL 주소 정보는 [표 3-3]과 같다.

표 3-3 | 유포지 URL 주소

hxxp://ovsz.ru/08yhrf3
hxxp://pppconstruction.co.za/08yhrf3
hxxp://propfisher.com/08yhrf3

다운로더에 의해 실행된 파일은 사용자 PC의 %Temp% 폴더에 암호화된 형태로 생성된다. 해당 파일은 복호화 후 정상적인 동적 링크 라이브러리(DLL) 파일로 변환된 뒤, [그림 3-9]와 같이 윈도우(Windows) 정상 프로세스인 Rundll32.exe에 인젝션되어 실행된다.

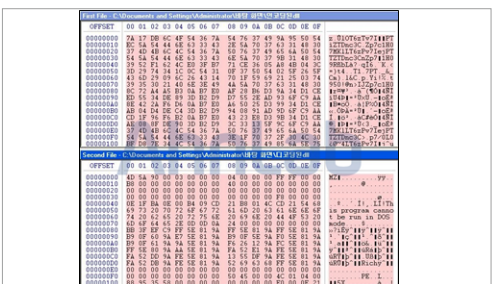


그림 3-8 | 인코딩된 실행 파일 (위) / 디코딩된 실행 파일 (아래)

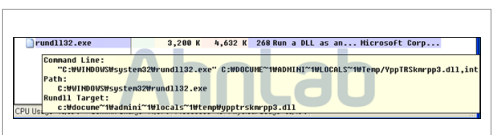


그림 3-9 | Rundll32.exe에 인젝션된 DLL파일

Rundll32.exe가 실행된 후 바로 파일 암호화가 진행되지 않고, 일정 시간이 경과한 다음 파일 암호화가 진행된다. 최종적으로 암호화가 완료되면 -INSTRUCTION.bmp, -INSTRUCTION.html 파일명을 가진 랜섬웨어 감염 알림 메시지가 출력되며, [그림 3-10]과 같이 파일의 확장자명이 '.aesir'로 변경된 것을 확인할 수 있다.

그림 3-10 | 암호화 후 추가되는 확장자명 '.aesir'

그림 3-11 | 암호화 완료 뒤 출력되는 메시지

앞서 살펴본 이들 록키 랜섬웨어 변종에 감염되면 [그림 3-11]과 같은 화면이 나타난다. 출력되는 메시지는 기존 록키 랜섬웨어와 크게 다르지 않다.

랜섬웨어를 이용한 보안 위협은 점점 고도화되고 있다. 일단 랜섬웨어에 감염되어 파일이 암호화되면 거의 복구하기 어렵다. 따라서 다른 어떤 악성코드보다 랜섬웨어는 사전 예방이 중요하다. 랜섬웨어 피해 예방을 위해 평소 OS 및 주요 프로그램의 최신 보안 업데이트를 적용하고, 중요한 데이터는 주기적으로 백업을 해두는 것이 바람직하다.

V3 제품에서는 해당 록키 랜섬웨어 변종을 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Locky (2016.11.24.03)

JS/Obfus.S158 (2016.10.25.05)

JS/Obfus.S166 (2016.11.24.05)

Downloader/VBS.Agent (2016.10.29.00)

AhnLab

ASEC REPORT

VOL.83
November, 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