

ASEC REPORT

VOL.71

November, 2015



AhnLab

ASEC REPORT

VOL.71 November, 2015

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

2015년 11월 보안 동향

Table of Contents

1	01 악성코드 통계	4
보안 통계	02 웹 통계	6
STATISTICS	03 모바일 통계	7
2	01 테슬라크립트와 크립토월 비교 분석	10
보안 이슈	02 안드로이드 RAT, 드로이드잭(DroidJack)	13
SECURITY ISSUE		
3	랜섬웨어에 감염되는 이유와 사례	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

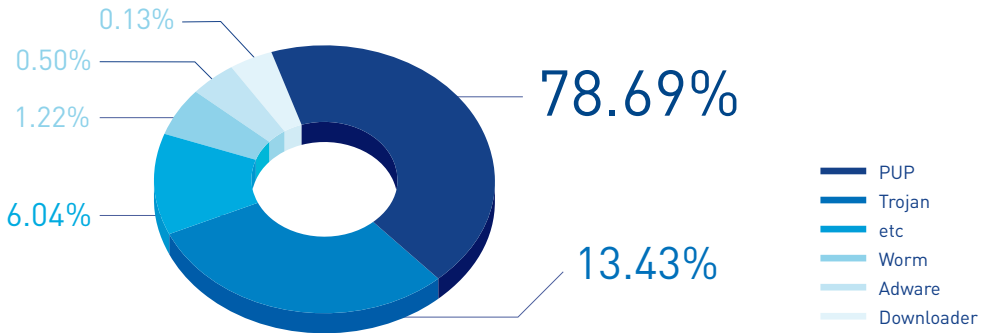
ASEC이 집계한 바에 따르면, 2015년 11월 한 달간 탐지된 악성코드 수는 1,511만 8,864건으로 나타났다. 이는 전월 1,374만 1,322건에 비해 137만 7,542건 증가한 수치다. 한편 11월에 수집된 악성코드 샘플 수는 605만 474건이다.



[그림 1-1] 악성코드 추이(2015년 9월 ~ 2015년 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 2015년 11월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 78.69%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 13.43%, 웜(Worm)이 1.22%의 비율로 그 뒤를 이었다.



[그림 1-2] 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.Starter 가 총 16만 3,725건으로 가장 많이 탐지되었고, Trojan/Win32.Agent가 12만 3,725건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	163,725
2	Trojan/Win32.Agent	123,725
3	Malware/Win32.Generic	112,866
4	Trojan/Win32.Teslacrypt	80,540
5	Trojan/Win32.Gen	77,381
6	ASD.Prevention	68,510
7	Worm/Win32.IRCBot	58,657
8	Trojan/Win32.Neshta	56,148
9	Unwanted/Win32.Exploit	55,902
10	Trojan/Win32.Banki	53,502

보안 통계

02
웹 통계

2015년 11월에 악성코드 유포지로 악용된 도메인은 1,318건, URL은 1만 29건으로 집계됐다(그림 1-3). 또한 11월의 악성 도메인 및 URL 차단 건수는 총 439만 9,439건이다.



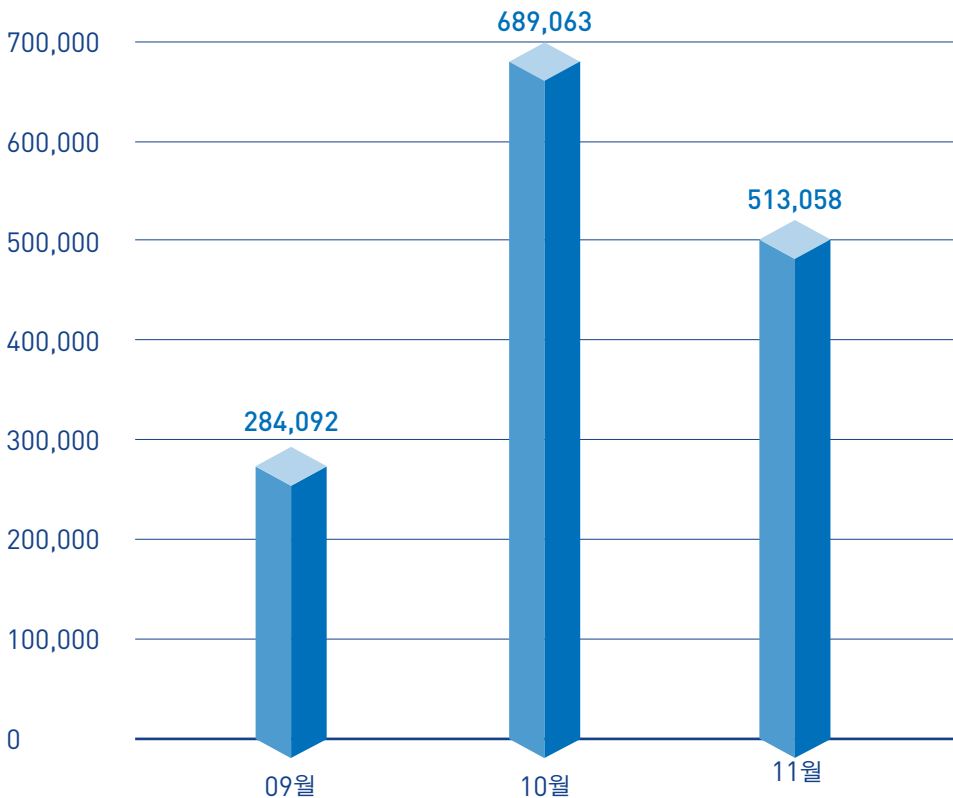
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 9월 ~ 2015년 11월)

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

03

모바일 통계

2015년 11월 한 달간 탐지된 모바일 악성코드는 51만 3,058건으로 집계됐다(그림 1-4).



[그림 1-4] 모바일 악성코드 추이(2015년 9월 ~ 2015년 11월)

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

[표 1-2] 2015년 11월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	127,427
2	Android-PUP/SmsReg	125,621
3	Android-Trojan/FakeInst	66,462
4	Android-PUP/Noico	27,590
5	Android-Trojan/Opfake	19,403
6	Android-Trojan/SMSAgent	13,043
7	Android-PUP/Zdpay	10,381
8	Android-PUP/Dowgin	9,925
9	Android-Trojan/SmsSend	7,727
10	Android-Trojan/SmsSpy	6,687

2

보안 이슈 SECURITY ISSUE

01 테슬라크립트와 크립토월 비교 분석

02 안드로이드 RAT, 드로이드잭(DroidJack)

01

테슬라크립트와 크립토월 비교 분석

테슬라크립트(TeslaCrypt)와 크립토월(CryptoWall)은 11월 한 달 동안 국내에서 가장 많은 감염을 발생시킨 것으로 확인되는 랜섬웨어다. 크립토월은 2013년에 등장하여 꾸준히 업데이트되고 있는 랜섬웨어로, 지불을 유도하는 안내 메시지에 기재되어 있는 것과 같이 RSA Key로 파일을 암호화한다.

에서 'RSA Key로 암호화한다'고 한 것과 달리 AES Key를 사용하여 파일을 암호화한다.

초창기 테슬라크립트의 경우, 크립토락커(CryptoLocker)의 감염 후 메시지를 차용하기도 했으며, 테슬라크립트 2.0 이후에는 크립토월의 감염 후 메시지(html 파일)를 그대로 사용하고 있는 것으로 확인된다. 이에 따라 사용자들은 테슬라크립트에 감염되었음에도 크립토월에 감염된 것으로 착각하는 경우가 많으며, 해외에서는 이를 테슬라크립트가 크립토월로 '위장(disguise)'하고 있다고 표현하기도 한다.



그림 2-1 | 크립토월 감염 후 사용자에게 노출하는 html 파일
(위에서부터 2014년 11월 / 2015년 1월 / 2015년 11월 확인)

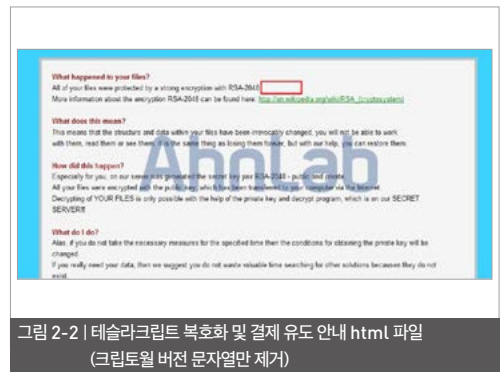


그림 2-2 | 테슬라크립트 복호화 및 결제 유도 안내 html 파일
(크립토월 버전 문자열만 제거)

이와 비교하여 테슬라크립트는 2015년 2~3월경 처음 등장했는데, 감염 후 사용자에게 노출하는 메시지

최근 확인되는 테슬라크립트는 파일을 암호화한 후 확장자를 '*.ccc'로 설정하는 것으로 확인되어, 국내에서는 CCC 랜섬웨어로 악명을 떨치고 있다.

jpg에 갑자기 ecc 붙었는데 바이러스인가요?

2016. 10. 9. 갑자기 jpg, doc, ppt등이 사라졌는데 바이러스일까? 아니면 악성코드일까? ecc 붙었더니 바이러스일까? 아니면 악성코드일까? ecc 붙었더니 바이러스일까? 아니면 악성코드일까?

ecc 랜섬웨어 - 랜섬웨어

2016. 10. 9. 갑자기 jpg, doc, ppt등이 사라졌는데 바이러스일까? 아니면 악성코드일까? ecc 붙었더니 바이러스일까? 아니면 악성코드일까?

ecc 랜섬웨어 - 랜섬웨어

2016. 10. 9. 갑자기 jpg, doc, ppt등이 사라졌는데 바이러스일까? 아니면 악성코드일까? ecc 붙었더니 바이러스일까? 아니면 악성코드일까?

파일들의 확장자가 ecc로 바뀌었는데 랜섬웨어 맞나...

2016. 10. 9. 갑자기 jpg, doc, ppt등이 사라졌는데 바이러스일까? 아니면 악성코드일까? ecc 붙었더니 바이러스일까? 아니면 악성코드일까?

그림 2-3 | 'CCC' 랜섬웨어 구글 검색 결과



그림 2-5 | 테슬라크립트(왼쪽) / 크립토월 3.0(가운데) / 크립토월 4.0(오른쪽) 이미지 파일 및 html 파일

표 2-3 | 레지스트리 확인

테슬라크립트 2.0	크립토월 3.0	크립토월 4.0
X	(감염 후, 암호화된 파일 목록을 HKCU\Software\[\PC별 특정ID]\[랜섬 문자열]에 저장)	X

표 2-1 | 감염 후 암호화된 파일명

테슬라크립트 2.0	크립토월 3.0	크립토월 4.0
1.jpg.ccc (확장자 : .ecc, .exx, .ezz, .aaa 등)	1.jpg (암호화된 파일을 생성한 후, 원본 파일명으로 덮어씌움)	[랜섬문자열].[랜섬문자열]

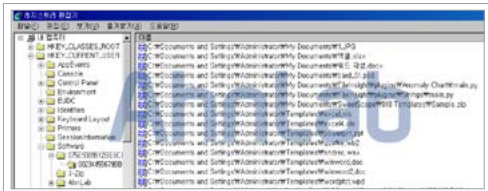


그림 2-6 | 크립토월 3.0 감염 후 레지스트리에 저장된 암호화 파일 목록



그림 2-4 | 테슬라크립트(왼쪽) / 크립토월 3.0(가운데) / 크립토월 4.0(오른쪽) 감염 후 파일명

표 2-2 | 감염 후, 복호화 및 결재 안내 파일

테슬라크립트 2.0	크립토월 3.0	크립토월 4.0
howto_recover_file_txt howto_recover_file_html howto_recover_file_[랜섬문자열].bmp 또는 HOWTO_RESTORE_FILES.htm HOWTO_RESTORE_FILES.txt HOWTO_RESTORE_FILES.bmp	HELP_DECRYPT.HTML HELP_DECRYPT.PNG HELP_DECRYPT.TXT	HELP_YOUR_FILES.HTML HELP_YOUR_FILES.PNG HELP_YOUR_FILES.TXT

테슬라크립트와 크립토월 이외에도 매우 다양한 종류의 랜섬웨어가 있지만, 결과적으로 파일을 암호화하여 인질로 사용한다는 개념은 같다. 랜섬웨어에 감염될 경우 암호화를 수행하는 악성코드가 제거되더라도 이미 암호화된 파일로 인해 사용자들의 피해가 극심한데, 최근 나타난 랜섬웨어는 자기 자신의 감염 흔적을 지우기 위해 파일 암호화가 완료되면 자기 스스로를 삭제하는 경우가 많다. 따라서 랜섬웨어 감염 PC에서 실행된 랜섬웨어가 확인되지 않는 경우도 비밀비재하다.

또한, 랜섬웨어가 등장한 초기에는 Windows의

VSC(Volumn Shadow Copy) 기능을 통해 암호화된 파일 중 일부 파일을 복구할 수 있었지만 최근 랜섬웨어는 VSC 기능을 이용한 백업 파일도 'vssadmin.exe delete' 명령을 통해 삭제하여 복구가 어렵다. 이로 인해 백업의 중요성이 그 어느 때보다도 강조되고 있다.

한동안 랜섬웨어에 대한 국내 유포는 끊이지 않을 것으로 보이며, 관련 변종도 꾸준히 등장할 것이다. 국내 최대 이슈였던 파밍 악성코드가 사용자들에게 많이 알려지면서 악성코드에 감염되더라도 이전처럼 쉽게 모든 개인 정보를 입력하는 사용자는 많이 줄었기 때문에 악성코드 유포자들이 랜섬웨어에 눈을 돌렸을 것으로 추정된다.

따라서 확인되지 않은 메일의 첨부 파일은 바로 삭제하고, 다운로드 실행(Drive-by-Download) 방식으로 유포되는 악성코드 감염 예방을 위해 항상 최신 보안 패치를 적용하고, 사용 중인 백신을 최신 엔진 버전으로 유지해야 한다. 또한, 파일 공유 사이트 혹은 P2P를 통해 다운로드한 파일도 위험성이 있으므로 이러한 파일의 실행은 권장하지 않는다. 만약 불가피하게 실행해야 한다면, 반드시 사용 중인 백신으로 정밀 검사한 후 주의하여 실행할 수 있도록 하자.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Teslacrypt (2015.11.07.02)

Trojan/Win32.CryptoWall (2015.11.11.00)

02

안드로이드 RAT, 드로이드잭(DroidJack)

영국 경찰은 ‘드로이드잭(DroidJack)’으로 불리는 스마트폰 악성코드를 통해 28세의 남자를 체포했다. 영국 국가범죄수사국(UK's National Crime Agency)은 유럽의 5개국(독일, 프랑스, 벨기에, 스위스, 영국)과 미국에서 드로이드잭을 통해 범죄자를 검거한 것으로 확인됐다. 드로이드잭(DroidJack)은 원격 접속이 가능한 트로이목마 바이러스 혹은 ‘랫(RAT)’으로, 안드로이드 단말만 감염시킨다. 또한 사용자가 전혀 모르게 스마트폰 데이터의 트래픽을 감시하고 대화를 도청한다. 카메라에 찍힌 정보를 가로챌 수도 있다. 다음은 드로이드잭 검거 관련 BBC NEWS의 소식이다.

드로이드잭은 다음과 같은 기능을 제공하며 가격은 \$210이다. 온라인 구매 시 [그림 2-8]과 같이 사용자 정보를 요구한다.

* 주요 기능

- apk 파일 빌드
- 스마트폰에 저장된 파일 탈취
- 스마트폰으로 파일 전송
- 스마트폰의 SMS 탈취
- 스마트폰에서 SMS 보내기
- 통화내역 탈취
- 주소록 탈취
- 스마트폰의 마이크를 이용하여 도청 및 녹음
- 스마트폰 인터넷 방문 기록 및 북마크 정보 탈취
- 위치 정보 탈취
- 스마트폰의 앱 실행, 실행 중인 앱 정보 탈취
- IMEI, MAC, 통신사 정보 탈취 및 루팅 여부 확인 등



그림 2-7 | BBC NEWS 2015.10.30 (드로이드잭 관련 검거 소식)

[illegible]

그림 2-11 | GPS 위치 정보 확인 기능

The screenshot shows a Windows XP desktop environment. A web browser window is open, displaying a text message log. The log has a table with columns: No., Message, Name, Number, and Date. The messages are numbered 1 through 12. Below the table, there is a 'Full Message' section with a text input field containing 'Great, very tomorrow (pm) (Friday)' and a 'Send' button. To the right of the browser window, there is a separate application window titled 'SMS'. This window has a menu bar with 'Backup', 'SMS', 'Record', 'View', 'History', and 'Live'. It also features a search bar with a magnifying glass icon and a 'Refresh' button. The main area of the 'SMS' window is currently empty.

No.	Message	Name	Number	Date
1	You have 1 missed call.	Apple	+91 888212155	2009/01/11 09:01
2	There is the biggest risk.	Apple	+91 888212155	21/09/2010 11:37 AM
3	Oh look it's Thursday.	Apple	+91 888212155	2009/01/11 09:02
4	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:03
5	Offices W or you will do it.	Apple	+91 888212155	2009/01/11 09:03
6	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
7	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
8	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
9	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
10	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
11	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04
12	Don't forget, we're all in.	Apple	+91 888212155	2009/01/11 09:04

Full Message
Great, very tomorrow (pm) (Friday)
Send

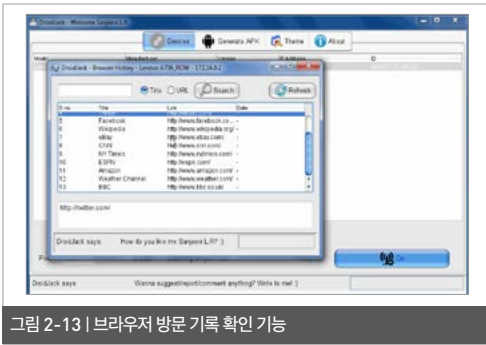


그림 2-13 | 브라우저 방문 기록 확인 기능

안드로이드 악성 앱은 주로 구글(Google)이나 유틸리티, 유명 게임 등의 아이콘을 이용하여 제작되는 경우가 많은데 이는 사용자가 의심하지 않고 설치하도록 유도하기 위해서다. 안랩에서는 드로이드책과 관련된 수많은 악성 앱을 진단하고 있다. 그 중 아이콘 몇 가지를 살펴보면 [그림 2-14]와 같다. 일부는 테스트를 위해 제작한 앱도 포함되어 있었다.



그림 2-14 | 드로이드책 악성 앱

유명 게임인 'Agar.io'의 아이콘으로 위장한 악성 앱을 설치한 화면을 살펴보면 [그림 2-15]와 같다. 설치 과정에서 필요한 권한을 획득한다. 설치 완료 후 실행되면 자신의 아이콘을 제거하여 사용자 스마트폰

폰에 설치되어 있지 않은 것처럼 위장하고 있다.



그림 2-15 | 권한 획득(왼쪽) / 설치 아이콘(가운데) / 설치 및 실행 후 아이콘이 사라진 화면(오른쪽)

이러한 스파이 앱은 각종 악성 앱의 악의적인 기능의 총 집합체로 스마트폰에 저장된 거의 모든 정보를 조작하거나 탈취할 수 있기 때문에 특히 주의해야 한다. 따라서 앱은 공식 마켓에서 다운로드하여 설치하는 것이 상대적으로 안전하지만, 공식 마켓에도 악성 앱이 등록되어 있을 수 있으므로 평판 정보를 확인하고 설치하는 습관을 가져야 한다. 무심코 문자에 포함된 URL을 클릭하다 보면 악성 앱이 설치될 수도 있기 때문에 안전성이 확인되지 않은 URL이나 앱은 설치하지 않도록 주의해야 한다. 또한, 세계 1위의 모바일 전용 보안 앱(V3 모바일 등)이나 스미싱 탐지 앱(안랩 안전한 문자 등)을 설치하고, 자동 업데이트 설정으로 항상 최신 엔진을 유지하여 보다 안전한 스마트폰 환경을 만들어야 한다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Android-Trojan/Sandrorat

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

랜섬웨어에 감염되는 이유와 사례

랜섬웨어에 감염되는 이유와 사례

최근 사용자 PC에 있는 문서 파일과 이미지 파일들을 암호화하고 금전을 요구하는 랜섬웨어에 감염되는 사례가 많아지고 있다. 과거 2010년 초반에 유행했던 온라인 게임 핵 악성코드와 그 이후 유행한 파밍 악성코드에 이어 이제는 랜섬웨어가 주요 트렌드가 된 상황이다.

초기에는 주로 메일의 첨부 파일을 이용한 유포 방식이 대부분이었지만, 최근에는 보안이 취약한 웹사이트를 통해 악성코드를 유포하는 다운로드 실행(Drive-by-download) 방식을 주로 사용하고 있다. 이에 따라 대부분의 사용자들은 자신도 모르는 사이에 랜섬웨어에 감염되어 파일들이 암호화되는 피해를 입고 있다. 다운로드 실행(Drive-by-download) 방식을 통해 악성코드를 유포하는 방법은 다음과 같다.

1. 보안이 취약한 웹사이트에 악성 스크립트를 삽입한다.



2. 사용자가 해당 웹사이트 접속 시 악성 스크립트가 동작한다.

3. 사용자의 PC에 설치된 프로그램의 버전을 확인하여 취약점이 존재하는지 체크한다. 주로 인터넷 익스플로러, 자바(Java), 플래시 플레이어 프로그램 등의 취약점이 자주 악용된다.



4. 사용자의 PC에 해당 취약점이 존재하는 경우, 취약점을 유발시키는 코드를 실행한다.

5. 취약점을 유발시키는 코드를 통해 악성코드를 다운로드하고 실행하여 사용자 PC를 감염시킨다.



이러한 악성코드 유포 방식은 굉장히 익숙한 유포 방식이다. ‘익숙한’이라는 표현을 쓰는 이유는, 앞서 언급한 온라인 게임 핵 악성코드와 파밍 악성코드 유포에 사용된 것과 동일한 방식으로 악성코드를 유포하고, 최종적으로 사용자 PC에 다운로드되는 악성코드만 바뀐 형태이기 때문이다. 랜섬웨어는 주로 인터넷 익스플로러, 자바, 플래시 플레이어 프로그램의 취약점을 악용하기 때문에 안랩에서는 사용자들에게 윈도우 보안 업데이트와 인터넷 익스플로러, 자바, 플래시 플레이어 프로그램의 최신 버전 유지 등을 안내하고 있다.

그러나 과거 온라인 게임 핵과 파밍 악성코드가 유행할 때에도 많은 사람들이 피해를 입었고, 최근 랜섬웨어 악성코드도 마찬가지로 다수의 피해자를 양산하고 있다. 분명 과거와 같은 방식으로 유포하고 있는데 감염자가 줄지 않는 이유는 무엇일까?

가장 큰 원인은 바로 사용자의 ‘무분별한 인터넷 사용’에 있다. 특히 사용 목적과 관련이 없는 PC 사용은 악성코드 감염의 지름길이다. 즉, 업무 PC에서 업무와 관련 없는 무분별한 인터넷 사용은 악성코드 감염

으로 이어질 수 있다는 것이다. 특히 각종 소규모 쇼핑몰 사이트와 유명 커뮤니티 사이트 등은 보안에 취약한 경우가 많아 악성코드 유포에 자주 악용되므로 유의해야 한다. 지난 4월에 유포된 한글 랜섬웨어 악성코드 역시 유명 커뮤니티 사이트를 통해 다수의 사용자들이 감염되었던 것이다. 그리고 사용자들이 보안 업체에서 안내하는 윈도우 보안 업데이트, 인터넷 익스플로러, 자바, 플래시 플레이어 프로그램의 최신 업데이트 등을 소홀히 여기는 것도 악성코드 감염의 큰 원인 중 하나다.



아크로벳 리더, 플래시 플레이어, 자바 등의 프로그램이 설치되어 있을 경우, 업데이트 메시지가 출력되는 것을 볼 수 있다. 많은 사람들이 귀찮다 혹은 시간이 없다는 이유로 ‘설치 안함’을 클릭하거나 창을 닫아 버리고 지나가는 경우가 많은데, 설치 시간이 오래 걸리지 않으므로 업데이트를 꼭 설치해야 한다. 프로그램을 최신 상태로 유지하면 취약점들을 조치할 수 있고 악성코드 감염을 사전에 예방할 가능성이 높아진다.

사내에서 사용하고 있는 업무 인프라가 인터넷 익스플로러나 자바와 같은 프로그램의 특정 버전에만 동작하도록 되어 있어 최신 버전을 설치하기 어려운 경우도 있다. 이런 경우는 더욱 간단하게 해결할 수 있다. 그것은 바로 '업무 사이트 외에는 사용하지 않는 것'이다. 업무 PC는 업무 목적으로만 사용하고, 개인적인 용도로 사용하지 않으면 악성코드 감염은 상당히 예방할 수 있다.



그림 3-5 | 실시간 동영상 스트리밍 서비스 제공 페이지

그리고 자주 감염되는 경로 중 하나는 메일의 첨부 파일이다. 의심되는 메일임에도 불구하고 발신자나 제목, 내용 등을 확인하지 않고 첨부 파일부터 여는 경우가 있는데 이는 매우 위험한 행동이다. 출처를 알 수 없거나 의심이 되는 제목의 메일은 읽지 않고 삭제하는 것이 좋다. 또한 발신자를 아는 경우에도 첨부 파일은 바로 실행하지 않고 PC에 저장 후 백신으로 검사하는 습관을 가지는 것이 좋다.

인터넷 스트리밍 서비스를 제공하는 업체에서는 동영상 재생할 때 광고창을 삽입하여 광고 수익을 얻는다.



그림 3-6 | 재생 버튼 클릭 시 생성되는 광고창(오른쪽)

지금까지 랜섬웨어에 감염되는 이유를 살펴보았다. 그렇다면 실제 감염 과정은 어떤지 확인해 보자.

최근에는 인터넷 스트리밍 서비스를 통해 파일을 다운로드하지 않고 대용량 미디어 파일을 이용할 수 있다. 인터넷만 연결되어 있으면, 시간과 장소에 구애받지 않고 원하는 TV 프로그램, 영화, 음악 등을 감상할 수 있어 많은 사람들이 이용하고 있다.

사용자는 생성되는 광고창을 종료하거나 무시하고 동영상을 시청하게 되는데, 동영상 시청을 마치면 다음과 같이 랜섬웨어에 감염되었다는 알림창을 보게 된다.



그림 3-7 | 랜섬웨어에 감염되었음을 알리는 알림창

원인은 광고 사이트 내부에 삽입되어 있는 스크립트에 있다. [그림 3-8]은 광고 사이트의 내부 정보다. 악성코드 제작자는 악성코드 유포 도구(Exploit Kit)를 이용하여 내부에 악의적인 스크립트를 삽입했다.



그림 3-8 | 사이트 내부에 삽입된 악성 스크립트

악성코드 유포 도구(Exploit Kit)는 탐지되는 것을 피하기 위해 URL을 [표 3-1]과 같이 리다이렉트 시킨다.

표 3-1 | 변조된 부분

[접속 경로]

```
http://*****.info/topic.php?forum=48&topic=58526&p
otid=1447350054
>http://pb6kq.*****.pw/viewforum.php?f=07b4c&si
d=k4c.6661hvg53122q7
```

최종적으로 연결된 사이트의 내부 정보는 [그림 3-9]와 같다. 이전과 마찬가지로 탐지 및 분석을 방지하기 위해 난독화된 코드로 구성되어 있다.

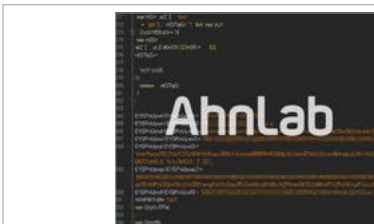


그림 3-9 | 난독화된 악성 스크립트

악성 스크립트가 실행되면 보안 제품 및 가상 머신 설치 여부와 시스템에 존재하는 취약점을 탐지한 후, 악성코드를 실행시킨다.

표 3-2 | 악성코드 생성 정보

[파일 정보]

C:\Windows\[랜덤문자].exe

[레지스트리 정보]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"C:\Windows\[랜덤문자].exe"

그렇다면 광고창이 생성되지 않는 사이트면 안전할까? 그렇지 않다.

다음은 랜섬웨어가 유포되는 인터넷 언론 사이트이다. 포털 사이트의 뉴스 기사 검색을 통해서 해당 사이트에 접속할 수 있다.



그림 3-10 | 연결된 인터넷 언론 사이트(오른쪽)

접속된 사이트에는 별도의 광고창이 생성되지 않는다. 하지만 사이트 내부에 악성 스크립트가 삽입되어 있어 뉴스 기사를 보던 중 랜섬웨어 경고 알림창을 확인할 수 있다.

[illegible]

그림 3-11 | 사이트 내부에 삽입된 악성 스크립트

하여 다운로드 실행 (Drive-by-download) 공격을 막고, 백신 제품의 엔진을 최신으로 유지하는 사용자의 올바른 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

이렇게 악성코드 제작자에 의한 공격은 인터넷 사용 환경에 깊숙이 침투해 있다. 랜섬웨어 감염을 예방하기 위해서는 보안 업데이트(운영체제, 인터넷 익스플로러, 자바, 플래시 플레이어)를 최신 버전으로 설치

<V3 제품군의 진단명>

Trojan/Win32.Teslacrypt

Trojan/Win32.CryptoWall

Trojan/Win32.CryptoLocker

AhnLab

ASEC REPORT VOL.71 November, 2015

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.