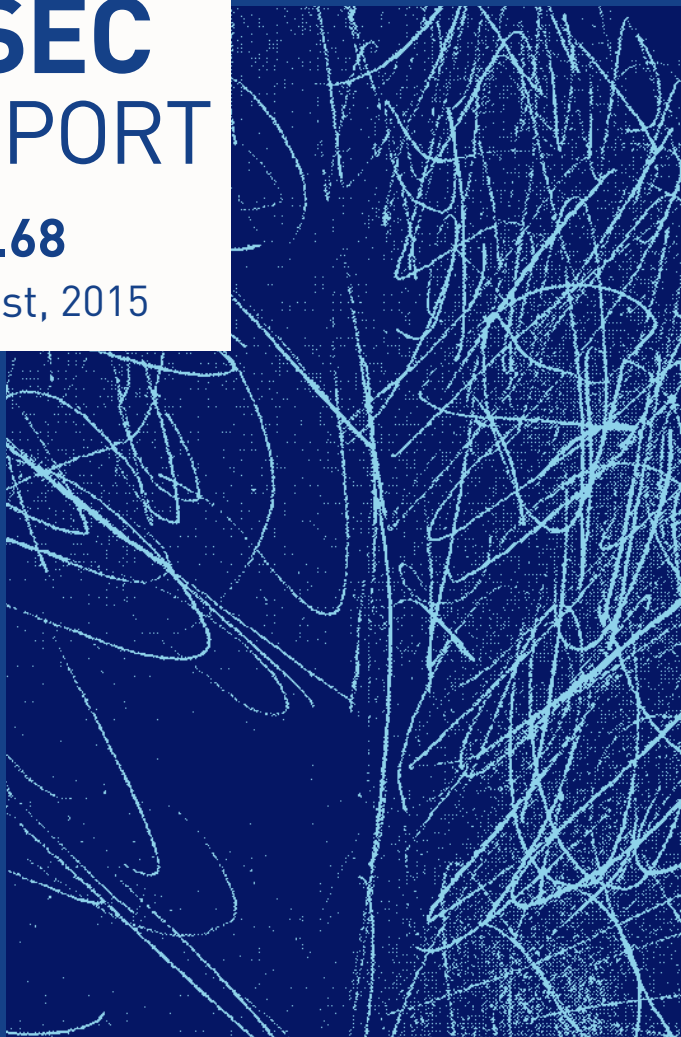


ASEC REPORT

VOL.68

August, 2015



AhnLab

ASEC REPORT

VOL.68 August, 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 8월 보안 동향

Table of Contents

1 보안 통계 STATISTICS	01 악성코드 통계	4
	02 웹 통계	6
	03 모바일 통계	7
2 보안 이슈 SECURITY ISSUE	01 중고나라 안전거래 사이트를 모방한 피싱 사이트 주의	10
	02 사회적 이슈로 클릭 유도하는 PUP 주의	12
3 악성코드 상세 분석 ANALYSIS IN-DEPTH	Windows 10 업데이트로 위장한 랜섬웨어	16

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

03 모바일 통계

보안 통계

01

악성코드 통계

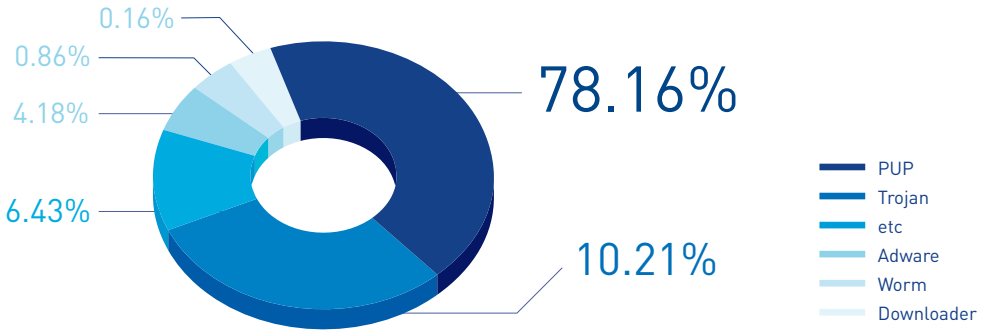
ASEC이 집계한 바에 따르면, 2015년 8월 한 달간 탐지된 악성코드 수는 1,786만 9,127건으로 나타났다. 이는 전월 1,936만 1,841건에 비해 149만 2,714건 감소한 수치다. 한편 8월에 수집된 악성코드 샘플 수는 643만 7,437건이다.



[그림 1-1] 악성코드 추이(2015년 6월 ~ 2015년 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 2015년 8월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 78.16%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 10.21%, 애드웨어(Adware)가 4.18%의 비율로 그 뒤를 이었다.



[그림 1-2] 2015년 8월 주요 악성코드 유형

[표 1-1]은 8월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Gen이 총 25만 4,208건으로 가장 많이 탐지되었고, Trojan/Win32.Starter가 13만 4,632건으로 그 뒤를 이었다.

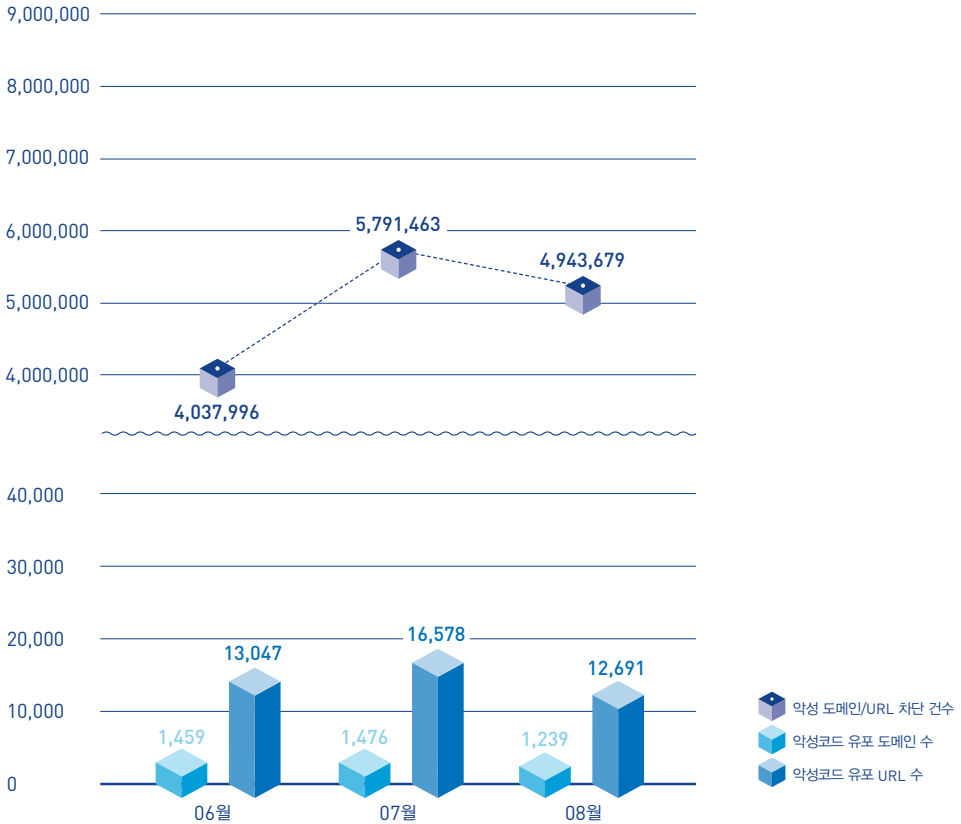
[표 1-1] 2015년 8월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Gen	254,208
2	Trojan/Win32.Starter	134,632
3	Malware/Win32.Generic	126,479
4	Trojan/Win32.Agent	92,959
5	Malware/Win32.SAPE	92,643
6	Unwanted/Win32.Exploit	73,052
7	Trojan/Win32.Banki	53,313
8	Adware/Win32.Agent	49,843
9	Trojan/Win32.Buzus	42,509
10	HackTool/Win32.Crack	42,505

보안 통계

02
웹 통계

2015년 8월에 악성코드 유포지로 악용된 도메인은 1,239건, URL은 1만 2,690건으로 집계됐다([그림 1-3]). 또한 8월의 악성 도메인 및 URL 차단 건수는 총 494만 3,679건이다.



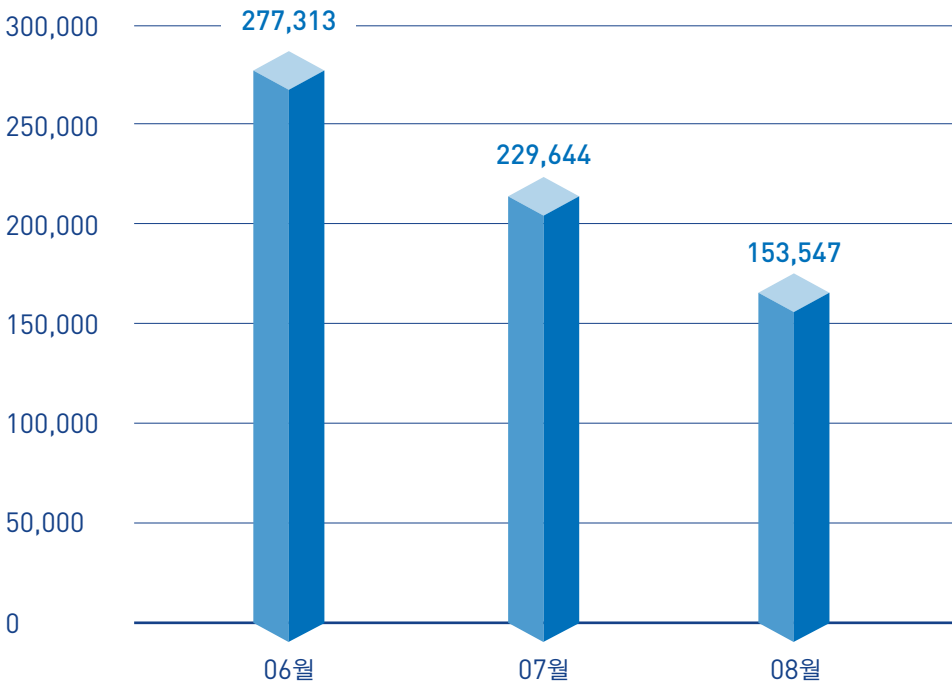
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 6월 ~ 2015년 8월)

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

03

모바일 통계

2015년 8월 한 달간 탐지된 모바일 악성코드는 15만 3,547건으로 집계됐다(그림1-4).



[그림 1-4] 모바일 악성코드 추이(2015년 6월 ~ 2015년 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] 2015년 8월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	47,217
2	Android-PUP/SmsReg	19,437
3	Android-PUP/Zdpay	8,579
4	Android-PUP/Dowgin	7,259
5	Android-Trojan/FakeInst	7,019
6	Android-Trojan/Slocker	6,007
7	Android-PUP/Noico	5,952
8	Android-Trojan/SmsSpy	3,843
9	Android-PUP/Chepa	3,240
10	Android-Trojan/SMSAgent	3,205

2

보안 이슈 SECURITY ISSUE

- 01 중고나라 안전거래 사이트를 모방한 피싱 사이트 주의
- 02 사회적 이슈로 클릭 유도하는 PUP 주의

01

중고나라 안전거래 사이트를 모방한 피싱 사이트 주의

국내 최대 규모의 온라인 직거래 장터인 '중고나라'. 그 규모만큼이나 사기 사건 피해가 끊이지 않고 발생한다. 대부분의 사기 피해 사례들은 판매자와 구매자 간 직접 물품을 매매하는 직거래 방식에서 많이 일어나고 있으며, 판매자가 물품 대금을 받는 순간 잠적해 버리는 경우가 가장 많았다.

판매자와 구매자 간의 직거래 중 발생할 수 있는 사기 피해를 방지하기 위한 대안으로는 안전거래 방식이 있다. 안전거래란, 제3자가 개입하여 구매자의 결제 대금을 예치하고 있다가 상품 배송이 완료된 후 대금을 판매자에게 지급하는 시스템이다. 그러나 이러한 안전거래 사이트를 교묘하게 모방한 피싱 사이트가 지속적으로 발견되고 있어 이용자들의 주의가 필요하다.

다음 [그림 2-1]은 안전거래 피싱 사이트 제작자가 중고나라에 올린 가짜 상품 판매 게시글이다. 보통 상품권이나 인기 있는 스마트폰, 노트북과 같은 전자제품을 판매 대상으로 하고 있다.

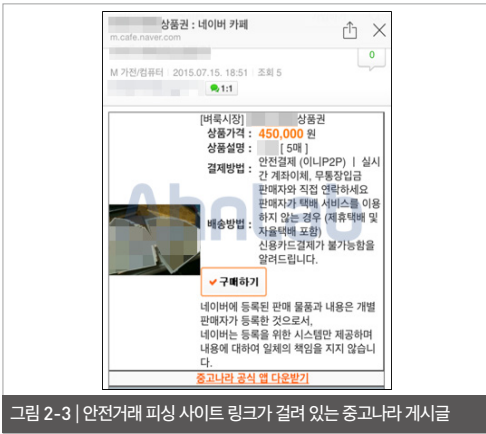


그림 2-1 | 중고나라 가짜 상품 판매 게시글



그림 2-2 | 사기 거래 대화 내용

판매자로 위장한 피싱 사이트 제작자는 직거래가 불가능하다는 여러 가지 이유를 들어 안전거래 방식으로 거래하기를 유도한다.

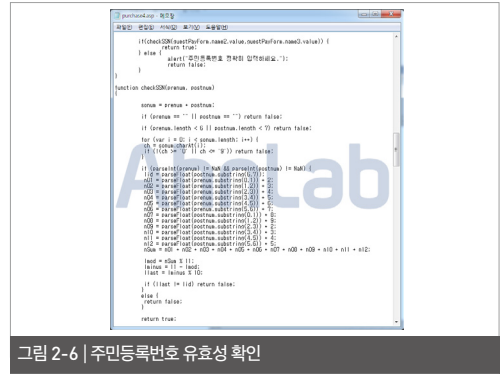


이후 안전거래 URL을 포함한 게시글을 다시 중고나라에 게시하는데, 확인해보면 안전거래 사이트를 모방한 피싱 사이트로 연결된다.

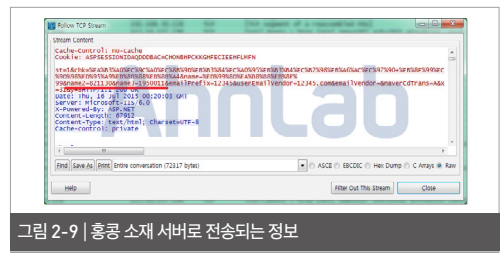


The figure illustrates a security audit finding on a personal website. On the left, a user interface shows a '비밀번호 찾기' (Forgot Password) link and a '로그인' (Login) button. On the right, the same interface is shown after a security audit, with the '로그인' button disabled and a message indicating that the password is not correct.

안전거래 업체 사이트를 모방한 피싱 사이트는 물품 배송을 이유로 이름, 주민등록번호, 주소 등의 개인정보를 요구한다. 주민등록번호의 경우에는 정상적인 주민등록번호를 입력했는지 유효성까지 확인한다.



이렇게 입력된 정보는 홍콩 소재의 서버 [113.**.
***.196]로 전송한다.



현재는 해당 도메인이 유효하지 않아 더 이상 접근이 되지 않는다. 그러나 이러한 피싱 사이트는 동일한 수법으로 URL 주소만을 변형하여 계속 생성할 수 있으므로 이용자들의 절대적인 주의가 필요하다.

02

사회적 이슈로 클릭 유도하는 PUP 주의

최근 연예인 관련 동영상이나 사회적 이슈와 관련된 동영상상을 이용해 불필요한 파일, PUP(Potentially Unwanted Program)를 유포한 사례가 발견됐다. 사용자가 삭제하기 어렵게 제작된 PUP가 유포된 데 이어 주로 악성코드 유포 시에 이용되던 사회 공학적 기법까지 이용하는 PUP가 나타남에 따라 PUP가 나날이 교묘해지고 있음을 알 수 있다.

PUP는 악성코드는 아니지만 PC를 느려지게 하거나 광고창을 반복적으로 노출하는 등 사용자에게는 악성코드 못지 않게 달갑지 않은 존재임이 틀림없다. 이번에 발견된 PUP는 다음 표와 그림과 같이 연예인 동영상 또는 폭탄 테러 등 사회적인 이슈와 관련된 동영상상을 이용해 유포되었다.



그림 2-8 | 사회적 이슈로 위장한 파일명

다음 [표 2-1]의 파일 생성 일자에서 알 수 있는 것처럼 PUP 파일 제작자는 파일 제작 당시 뉴스에 자주 보도되는 이슈를 이용했다. 파일의 생성 일자와 유포

일자는 해당 이슈가 발생한 시기와 일치한다. 이 시기는 관련 이슈의 뉴스 기사가 집중적으로 확산되며 사회적인 관심이 고조되는 때이다.

표 2-1 | PUP 파일 생성 일자

[PUP 파일 정보]	
파일명	파일 생성 일자
(연예인A)_태도논란_동영상.exe	2015.08.11 14시
(연예인B)_티저영상.exe	2015.08.11 15시
(방송인A)_동영상.exe	2015.08.18 16시
방콕폭탄테러_동영상.exe	2015.08.18 12시

사회적 이슈로 위장한 파일을 실행할 경우, 다음과 같이 경로 'C:\Windows'에 파일 'snbsetup.exe'를 생성한 후 실행한다.

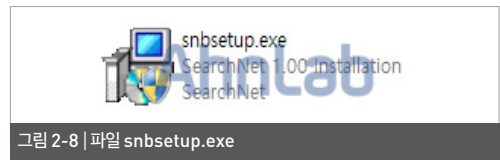


그림 2-8 | 파일 snbsetup.exe

파일 'snbsetupe.exe'가 실행되면, 다음 경로에 불필요한 프로그램이 설치된 후 실행된다.

표 2-2 | 생성 파일 정보

[생성 파일 정보]

C:\WProgram Files\SearchNet\searchnet.exe
 C:\WProgram Files\SearchNet\usearchnet.exe
 C:\WProgram Files\SearchNet\Uninstall.exe
 C:\WProgram Files\SearchNet\utildownload.exe

또한, [표 2-3]과 같이 시작프로그램 영역에 등록되어 시스템 시작 시 불필요한 프로그램을 자동으로 실행하게 한다.

표 2-3 | 시작프로그램 정보

[생성 파일 정보]

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\searchnet
 → "C:\WProgram Files\SearchNet\searchnet.exe"
 HKCU\Software\Microsoft\Windows\CurrentVersion\Run\usearchnet
 → "C:\WProgram Files\SearchNet\usearchnet.exe"

이후 생성된 파일 'utildownload.exe'가 실행되어 다음과 같은 화면을 출력한다. 프로그램의 좌측 하단에는 불필요한 프로그램의 이용약관이 표시되며, 우측 하단에는 파일 열기 버튼이 표시된다.

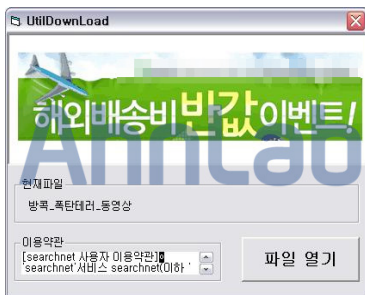


그림 2-10 | 파일 'UtilDownLoad' 실행 화면

사용자가 파일 열기 버튼을 클릭할 경우, 파일 'UtilDownLoad.exe'가 인터넷 익스플로러를 실행하여 해당 이슈의 동영상 페이지를 연결한다. 다음 동영상 페이지는 정상 페이지이며 이슈와 관련된 내용을 담고 있으므로 사용자는 시스템에 불필요한 프로그램이 설치된 사실을 인지하기 어렵다.



그림 2-11 | 관련 이슈의 동영상 페이지

이렇게 설치된 불필요한 프로그램의 주목적은 광고를 통한 금전적 이득이다. 불필요한 프로그램은 사용자가 방문하는 페이지 주소를 감시하고 있다가 사용자가 [표 2-4]와 같은 페이지에 연결할 경우, 광고를 삽입한다.

표 2-4 | 감시되는 페이지 정보

[페이지 주소]

http://search.*****.net/search
 http://www.google.co.kr/search
 http://search.*****.net/*****
 http://search.*****.com/search
 http://search.*****.co.kr/search
 http://search.*****.co.kr/search/search
 http://search.*****.co.kr/SearchPrdAction

이러한 불필요한 프로그램의 주목적은 배포 자체에 있으므로 프로그램이 제작된 후에는 관리가 이루어지지 않는다. 즉, 이렇게 탄생한 불필요한 프로그램들 이러한 불필요한 프로그램의 주목적은 배포 자체에 있으므로 프로그램이 제작된 후에는 관리가 이루어지지 않는다. 즉, 이렇게 탄생한 불필요한 프로그램들은 다수의 사용자에게 배포되며, 이후에는 보안 관리가 전혀 이루어지지 않는다. 따라서 악성코드 제작자로 하여금 훌륭한 악성코드 유포지로 표적이 될 수 있으므로 주의해야 한다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

PUP/Win32.Toolbar (2015.08.18.05)

Trojan/Win32.Infostealer (2015.08.20.08)

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

Windows 10 업데이트로 위장한 랜섬웨어

Windows 10 업데이트로 위장한 랜섬웨어

마이크로소프트사(이하 MS)의 마지막 OS가 될 Windows 10이 8월 29일 출시됐다. 출시 후 며칠이 지나지 않아 Windows 10 업데이트 파일로 위장한 랜섬웨어가 메일로 유포된 것으로 볼 때, Windows 10의 출시는 일반 사용자뿐만 아니라 악성코드 제작자들의 흥미 또한 유발한 것으로 보인다.



그림 3-2 | Windows 10 파일로 위장한 악성코드

악성코드를 실행하면 기대하던 Windows 10 업데이트가 아닌 랜섬웨어가 실행되어 사용자 시스템 내 파일을 암호화한다. 실행된 랜섬웨어 악성코드는 <C:\WDCOME~1W\사용자 계정\WLOCALS~1WTempW> 경로에 파일명 'lrxxjii.exe'로 자가 복제하고, 레지스트리를 통해 서비스에 등록되어 시스템이 시작할 때마다 실행된다.

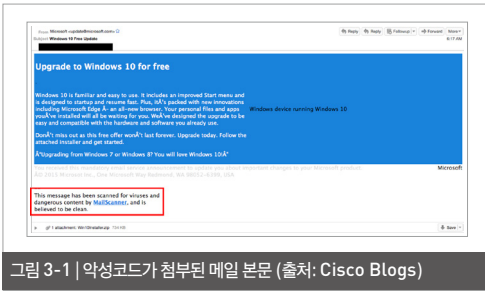


그림 3-1 | 악성코드가 첨부된 메일 본문 (출처: Cisco Blogs)

공격자는 발신인, 본문 내용과 더불어 ‘악성코드 스캔 후 이상 없다’는 마지막 문장을 [그림 3-1]과 같이 첨부하여, 수신자가 해당 메일을 읽은 후 아무 의심 없이 첨부 파일을 다운로드하고 실행하도록 유도했다. 심지어 메일 내 첨부된 악성 파일의 아이콘이 [그림 3-2]와 같이 Windows 로고를 사용함으로써, 평소 보안 의식이 강한 사용자가 아니라면 분명 거부감 없이 해당 파일로 마우스 포인터를 옮길 것이다.



그림 3-3 | 랜섬웨어에 감염된 후 바탕화면

[그림 3-3]과 같이 파일 복호화 안내를 바탕화면에 표시한다. 기존의 다른 랜섬웨어들과 크게 다른 특징은 없지만, 이번 사례에서 이용된 사회 공학 기법은 악성코드 유포 방법이 점차 지능화되고 있으며 결국 사람이 가장 큰 취약점이란 것을 새삼 느끼게 해준다.

지난 4월 국내 대형 커뮤니티 웹사이트를 통해 드라이브 바이 다운로드(Drive-by Download)로 유포되었던 랜섬웨어의 경우, 시스템의 취약점을 노린 공격이었으므로 평소 Windows 보안 패치 및 응용 프로그램(Adobe, java 등)의 업데이트를 성실히 수행해 온 사용자라면 악성코드 감염을 피할 수 있었을 것이다.

하지만 이번 사례와 같이 메일로 유포된 악성코드를 다운로드하여 실행하는 것은 사용자 스스로의 판단에 따른 행동이다. 보안 패치로 굳게 닫혀있는 시스템

을 악성코드의 노크에 직접 문을 열어주는 것은 사용자의 판단 부재에 따른 것이다. “절대로 메일 내 첨부 파일을 함부로 다운로드하거나 실행해서는 안 된다”는 가장 기초적이고 중요한 안전 수칙을 수없이 강조하게 되는 이유가 바로 이 때문이기도 하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.CTBLocker (2015.08.03.03)

AhnLab

ASEC REPORT VOL.68 August, 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.