Security Trend

ASEC REPORT

VOL.53

May, 2014

AhnLab

ASEC REPORT

VOL.53 May, 2014

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.

2014년 5월 보안 동향

Table of Contents

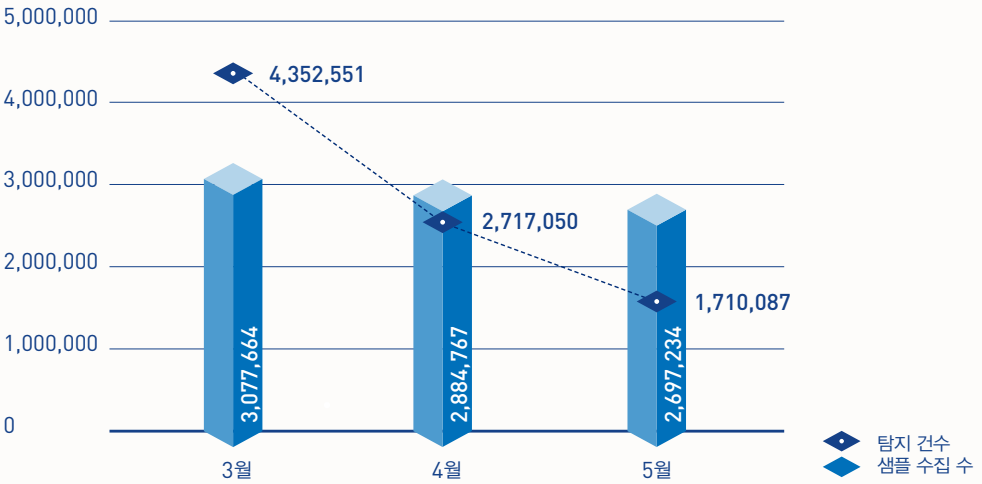
1

보안 통계
STATISTICS

01 악성코드 통계

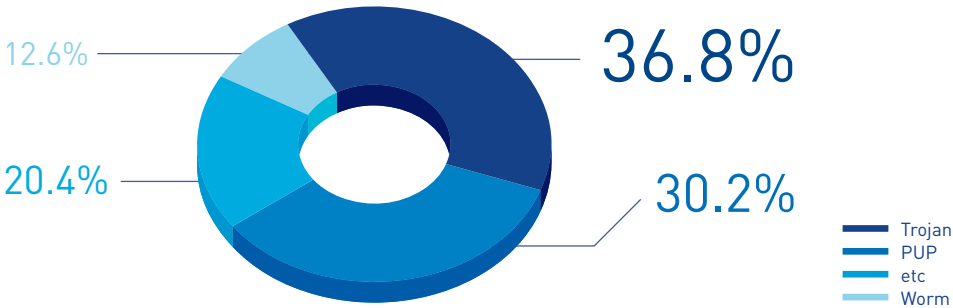
ASEC이 집계한 바에 따르면, 2014년 5월 한달 간 탐지된 악성코드 수는 171만 87건으로 나타났다. 이는 전월 271만 7,050건에 비해 100만 6,963건 감소한 수치다. 한편 5월에 수집된 악성코드 샘플 수는 269만 7,234건이다.

[그림 1-1]에서 '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드 샘플 수를 의미한다.



[그림 1-1] 악성코드 추이

[그림 1-2]는 2014년 5월 한달 간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 36.8%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 30.2%, 웜(Worm)이 12.6%의 비율로 그 뒤를 이었다.



[그림 1-2] 주요 악성코드 유형

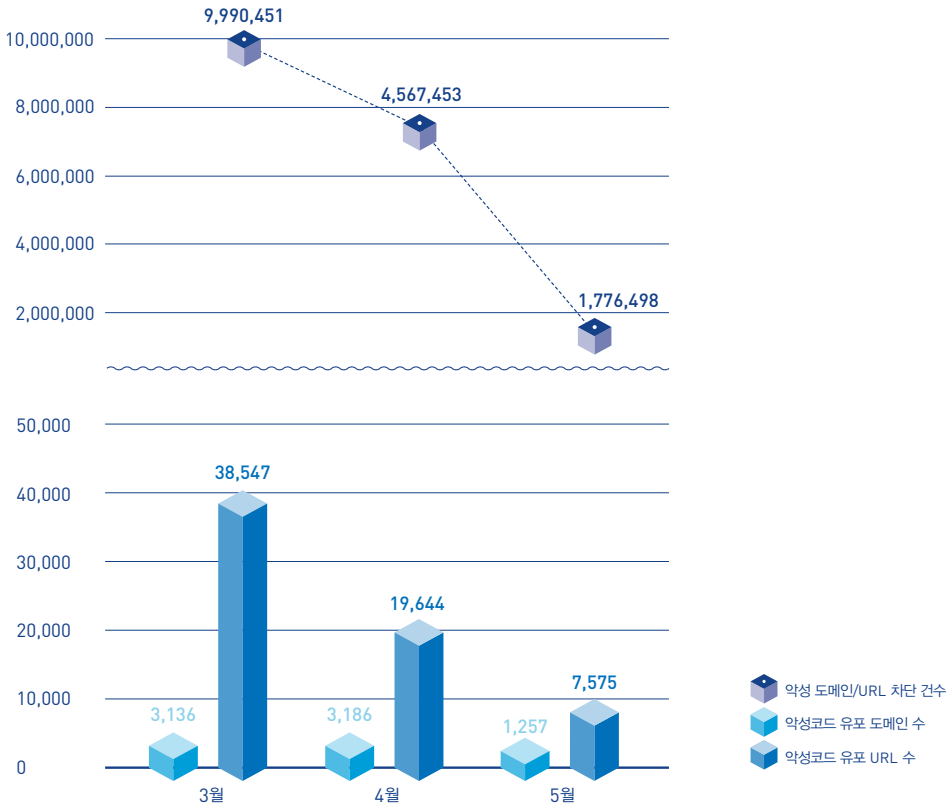
[표 1-1]은 5월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.IntClient 가 총 14만 8,164건으로 가장 많이 탐지되었고, Trojan/Win32.Agent가 8만 7,720건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건 (진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.IntClient	148,164
2	Trojan/Win32.Agent	87,720
3	PUP/Win32.GearExt	56,913
4	PUP/Win32.Kraddare	46,728
5	Trojan/Win32.Hupe	42,543
6	Trojan/Win32.OnlineGameHack	41,662
7	Trojan/Win32.Gen	38,430
8	ASD.Prevention	37,111
9	Unwanted/Win32.Agent	35,405
10	Trojan/Win32.Downloader	34,071

02
웹 통계

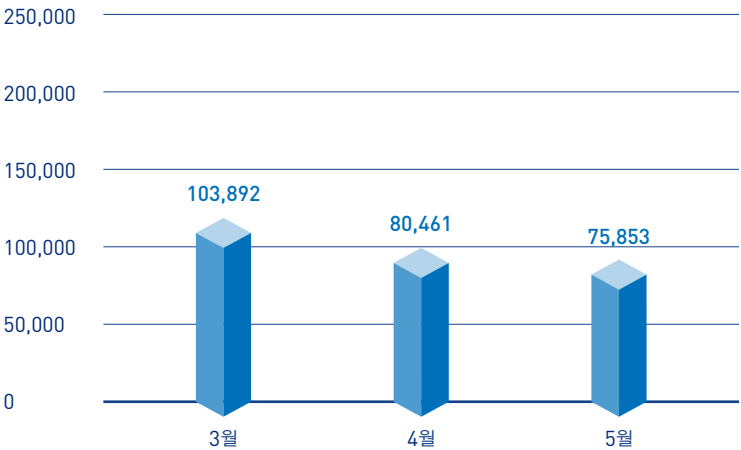
2014년 5월 악성코드 유포지로 악용된 도메인은 1,257개, URL은 7,575개로 집계됐다. 또한 5월의 악성 도메인 및 URL 차단 건수는 총 177만 6,498건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수

03
모바일 통계

2014년 5월 한달 간 탐지된 모바일 악성코드는 7만 5,853건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 5월 한달 간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 애플리케이션 설치 프로그램으로 위장하여 악성코드를 설치하는 악성 앱(Android-Trojan/FakeInst)이 지난 달에 이어 가장 많이 탐지되었다.

[표 1-2] 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-Trojan/FakeInst	18,801
2	Android-PUP/Dowgin	16,830
3	Android-PUP/Wapsx	4,625
4	Android-Trojan/Opfake	3,713
5	Android-Trojan/SMSAgent	1,685
6	Android-Trojan/Mseg	1,233
7	Android-Trojan/SmsSend	1,129
8	Android-PUP/SMSreg	1,094
9	Android-PUP/Kuguo	1,074
10	Android-PUP/Admogo	1,060

2

보안 이슈
SECURITY ISSUE

01

국가 재난을 악용한 스미싱과 피싱

최근 발견된 스미싱은 세월호와 같은 사회적 이슈를 악용한 사례가 많다. 이는 악성코드 제작자가 단기간에 사람들의 관심을 유도하여 많은 감염자를 확보하기 위해서이다.

세월호 관련 스미싱 문자는 “실시간 속보…”, “침몰 그 진실..”, “생존자 확인…” 등과 같은 문구를 사용했다. 또 “세월호 사칭 스미싱 대처 방법” 처럼 사람들의 심리를 이용하여 관심을 끌기 위한 어휘를 사용하기도 했다. [표 2-1]은 실제 원문으로, 다양한 문구를 확인할 수 있다.

스미싱 발송 날짜	원문
5월 01일 목요일	세월호기부상황 조회 3**.net/y7A
4월 23일 수요일	23일 9시경 실종자6명 구조성공이다.ㅊㅋㅊㅋ http://goo.gl/**mMVX
4월 22일 화요일	[속보]세월호 3호창 생존자 2명 발견 http://goo.gl/**Wgnd
4월 21일 월요일	단원고 학생 • 교사 78명 생존 확인 http://ww.tl/**m
4월 21일 월요일	세월호 사칭 스미싱 문자 추가 발견..주의 당부 스미싱 대처방법 t.**t99.info
4월 20일 일요일	세월호 침몰 그 진실은... http://ww.tl/**so
4월 20일 일요일	믿기 어려운 세월호 침몰 관련 충격 영상 공개 !! http://goo.gl/**kuii
4월 20일 일요일	세월호 침몰 그 진실 ... http://goo.gl/**uX6D[FW]
4월 19일 토요일	세월호 사칭 스미싱 문자 추가 발견…주의 당부 스미싱 대처방법http://goo.gl/**X4r1
4월 19일 토요일	[GO! 현장] 세월호 구조된 6살 어린이 http://126.107.**.204/
4월 19일 토요일	*실시간속보[세월호]침몰사망자55명더늘어*동영상보기 hosisting.**fo
4월 18일 금요일	[여객선침몰] 청해진해운 "승선자 명단 없는 사망자명단 kowa.**rtit.com
4월 18일 금요일	세월호 침몰 그 진실은...~http://ztc.me/**d
4월 18일 금요일	세월호 침몰 그 진실은...http://ww.tl/**ws
4월 18일 금요일	[연합뉴스]여객선 (세월호)침몰사고 구조현황 동영상 http://goo.gl/**buRb
4월 18일 금요일	*(실시간속보) 세월호침몰 사망자 25명으로 늘어..검색더보기 www.sto**paint**.net
4월 18일 금요일	*실시간속보세월호침몰 사망자 25명 늘어 더보기 http://psm8060.h**web.net/ADT.apk

표 2-1 | 세월호 관련 스미싱

스미싱은 문자메시지에 포함된 인터넷 주소를 클릭하면 악성 앱(apk)이 다운로드 된다. 이 앱을 스마트폰 사용자가 설치 및 실행하면, 사용자의 개인정보와 금융정보가 유출된다. 악성 앱의 아이콘은 구글 마켓과 세월호 사진 등이 이용됐다([그림 2-1]).

그림 2-1 | 악성 앱이 사용한 아이콘

이러한 세월호 관련 스미싱 악성 앱은 사용자의 연락처 정보, 디바이스 정보, 금융 정보를 탈취하여 외부 서버로 전송한다.

이번 세월호 사건을 악용한 스미싱 제작자는 지난 2014년 1월 카드사 정보유출 사건을 악용하기도 했다. 당시 사용된 메시지와 아이콘은 [그림 2-2]와 같다.

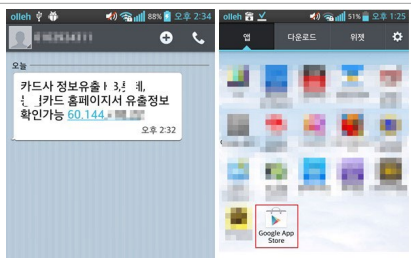


그림 2-2 | 카드사 정보 유출 스미싱(좌)과 악성 앱 아이콘(우)

악성 앱은 스마트폰에서 사용중인 은행 앱을 체크하여 해당 은행 앱으로 위장한 악성 앱을 다운로드 받는다(카드사 정보유출 사건). 대상이 되는 패키지명(은행 앱)은 동일하며 정보를 탈취 및 전송하는 서버 주소의 매개 변수 값도 동일하게 구성되어 있다. 또한 C&C 서버를 통해 명령을 수행하도록 설계되어 있다.

그림 2-3 | 대상 패키지 및 정보 탈취 서버정보의 일부 코드, 카드사 정보유출 사건(좌) / 세월호 사건(우)

스미싱 피해를 예방하려면 의심스러운 문자메시지의 URL 클릭을 자제하고, 스마트폰의 백신 앱은 항상 최신 버전으로 유지해야 한다. 또한 "안전한 문자"와 같은 스미싱 예방에 도움이 되는 앱을 설치하면 좀더 안전하게 스마트폰을 사용할 수 있다. 안전한 문자는 구글 플레이(https://play.google.com/store/apps/details?id=com.ahnlab.safemessage)에서 무료로 다운로드 받아 이용할 수 있다.

한편, 스미싱 뿐만 아니라 세월호 사건을 악용한 피싱 사이트도 발견되었다. [그림 2-4]와 같이 SNS에 수많은 사용자의 이름으로 해당 내용이 게시된 것을 확인 할 수 있다.

그림 2-4 | 세월호 사건의 허위 SNS 내용

해당 피싱 사이트는 유명 커뮤니티에서도 발견되었다([그림 2-5]).

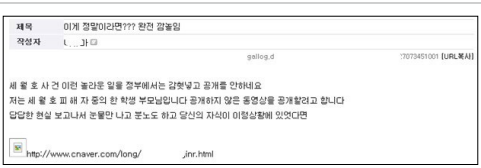


그림 2-5 | 세월호 사건을 악용한 피싱 사이트

작성자의 다른 글도 [그림 2-6]과 같이 세월호 사건을 언급하고 있다.

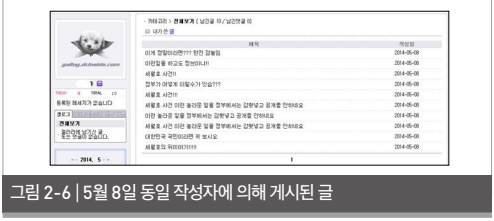


그림 2-6 | 5월 8일 동일 작성자에 의해 게시된 글

해당 피싱 사이트는 포털 사이트 로그인 페이지로 위장되었으나, 확인한 결과 로그인 형식(FORM)과 위치가 맞지 않았다.

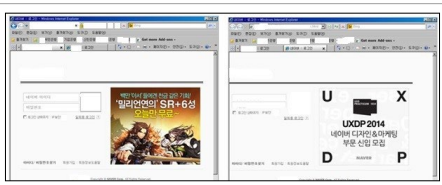


그림 2-7 | 정상적인 로그인 페이지(좌) / 악의적인 피싱 사이트(우)

[그림 2-8]과 같이 사용자가 입력한 아이디와 패스워드는 대만에 위치한 서버(피싱 사이트)로 전송한 후 정상적인 포털 사이트 페이지에 접속 한다.

그림 2-8 | 사용자가 입력한 ID/PW를 피싱 사이트로 전송하는 페이지 소스코드

해당 데이터 패킷을 보면 [그림 2-9]와 같이 아이디와 패스워드가 전송되는 것을 확인할 수 있다.

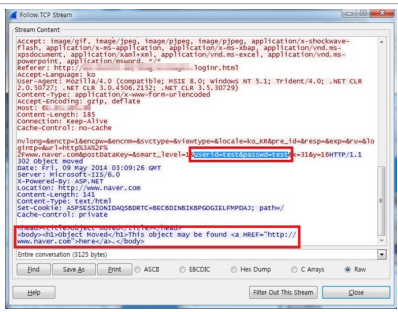


그림 2-9 | 사용자의 계정정보가 전송되는 네트워크 패킷

한편, 스미싱 범죄는 '정보통신망이용 촉진 및 정보보호 등에 관한 법률'에 의거하여 처벌 받을 수 있으며, 개인정보 무단 수집의 경우 5년 이하의 징역 또는 5,000만원 이하의 벌금형에 처할 수 있다.

02

공유기 DNS 변조 주의!

DNS 변조를 통해 금융정보를 탈취하는 악성코드가 꾸준히 발견되고 있다. [그림 2-10]은 악성 DNS 주소가 설정된 공유기를 통하여 정상적인 사이트에 접근한 화면이다.

그림 2-10 | DNS 변조를 통한 악성 앱 다운로드 유도

이처럼 DNS가 변조된 공유기를 통하여 접속할 경우 악성 앱을 다운로드 받게 된다. 어떤 과정을 통하여 악성 앱을 다운로드 받게 되는지 살펴보자.
[그림 2-11]은 악성 행위의 흐름을 나타낸 것이다.

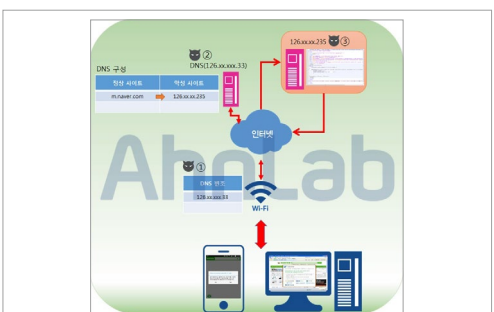


그림 2-11 | 악성 행위 흐름도

① 공유기 DNS 변조
A. 악의적인 DNS 주소로 접근하도록 변조한다.
② DNS 서버 구성
A. 사용자가 접근할 정상 사이트에 매핑되는 악성 사이트가 설정되어 있다.
③ 악성 스크립트 배포
A. 변조된 DNS 정보로 악성 사이트에 접속하게 된다.
B. 개인정보를 탈취 당하거나, 악성코드가 다운로드 될 수 있다.

[그림 2-12]와 같이 PC(Windows) 사용자가 접속하면 금융감독원을 사칭한 팝업 화면을 볼 수 있다.

그림 2-12 | 금융감독원을 사칭한 피싱(가짜) 사이트

[그림 2-12]의 팝업 화면에서 특정 은행을 선택하면 악성코드 제작자는 [그림 2-13]과 같이 "전자금융사기 예방 시스템" 관련 공지에 대한 글을 보여주고 사용자에게 정상 사이트로 인식시킨 후 금융정보 탈취를 시도한다.

그림 2-13 | 금융 정보를 탈취하려는 악성 사이트

스마트폰에서 살펴보면 사용자는 정상 사이트에 접속했지만 [그림 2-14]와 같은 스크립트에 의해 126..xx.xx.235 주소로 연결되며 악성 앱을 다운로드 받게 된다.

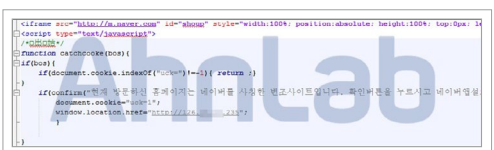


그림 2-14 | 악성 앱 다운로드 스크립트

그림 2-15 | 스마트폰에서 접속한 화면 (좌) / 악성 앱 다운로드 (우)

다운로드받은 악성 앱을 설치하면 [그림 2-16]의 (좌)처럼 권한을 요청한다. 정상 앱과 악성 앱의 아이콘은 동일하며 앱 이름만 다르게 나타난다(우).

그림 2-16 | 악성 앱의 권한정보 (좌) / 정상 앱과 악성 앱의 아이콘 (우)

악성 앱을 실행하면 정상적인 포털 사이트 페이지가 열리고 악성 앱의 아이콘은 삭제된다. 사용자는 악성 앱이 설치되어 있는지 인지하기 어렵다. 이런 경우에는 [환경설정] - [애플리케이션] 항목에서 설치된 앱을 확인하고 삭제할 수 있다.

해당 악성 앱은 금융정보 탈취를 목적으로 제작되었다. 다음과 같은 정보를 탈취하여 특정서버 (vvcn9.xxxx.cc)로 전송한다.

① IMEI (국제모바일기기 식별코드 [international mobile equipment identity])
② 전화번호
③ 통신사
④ 사용 중인 은행 앱
⑤ 주소록의 전화번호
⑥ 문자메시지(송신자번호, 수신일시, 문자내용)
⑦ 추가 악성 앱 다운로드

악성 앱 설치 후 네트워크 패킷을 살펴보면 [그림 2-17]과 같이 스마트폰의 정보를 탈취하는 것을 확인할 수 있다.

그림 2-17 | 악성 앱에 의한 네트워크 패킷(정보 탈취 부분의 일부 패킷)

또한 악성 앱에는 10개의 금융사를 사칭한 악성 앱을 다운로드 받는 코드가 존재한다.

그림 2-18 | 10개 금융사 사칭 앱 리스트

추가로 다운로드 받는 악성 앱에는 공인인증서를 탈취하는 코드가 존재한다.

그림 2-19 | 공인인증서 탈취 코드 일부

지금까지 DNS 변조로 인하여 감염될 수 있는 악성코드에 대해서 살펴봤다. 그 외에도 변조된 DNS가 발견되고 있다. [그림 2-20]과 같이 "ahnlab.com"으로 접근할 때 1.1.1.1로 연결되도록 설정하여 실제 안랩 접속을 차단하고 있는 사례도 발견되었다.

그림 2-20 | 변조된 DNS로 인하여 "ahnlab.com" 접속 차단

공유기는 DNS 주소가 변경되는 취약점이 발생될 수 있다. DNS 변조가 의심되면 공유기의 DNS 및 PC의 DNS 설정이 정상적으로 되어 있는지 확인하면 된다. 또한 이 같은 취약점을 예방하려면 반드시 공유기 제조사를 통해 최신 버전의 펌웨어로 업그레이드 해야 한다.

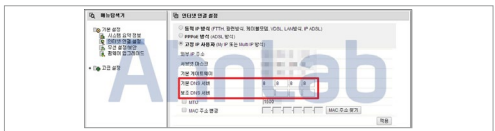


그림 2-21 | 공유기 DNS 설정 화면

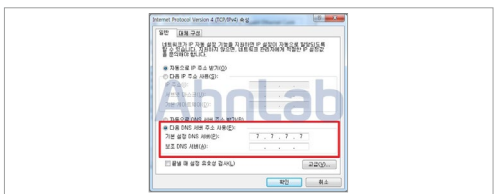


그림 2-22 | PC DNS 설정 화면

공유기 또는 PC의 DNS 주소가 변경되었다면 다음과 같이 변경하거나 자동으로 설정하면 된다.
참고로 기본 DNS 서버 주소는 아래와 같다.

KT : (기본 DNS 서버) 168.126.63.1
(보조 DNS 서버) 168.126.63.2

SK 브로드밴드 : (기본 DNS 서버) 210.220.163.82
(보조 DNS 서버) 219.250.36.130

LG U+ : (기본 DNS 서버) 164.124.101.2
(보조 DNS 서버) 203.248.252.2

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>
Trojan/Win32.Banki (2014.05.29.00)
Android-Trojan/Bankun (2014.05.28.04)

03

돈벌이 수단으로 이용되는 랜섬웨어

랜섬웨어(Ransomware)는 PC나 휴대전화 등 사용자 기기의 가용성을 다양한 방법으로 제한하여 사용자 스스로 금전을 지불하게 만드는 악성코드이다.

이번에 발견된 랜섬웨어 '크립토월(CryptoWall)'은 이메일로 전파되어 지금도 많은 사용자의 파일을 암호화한 후 금전을 요구하고 있다.

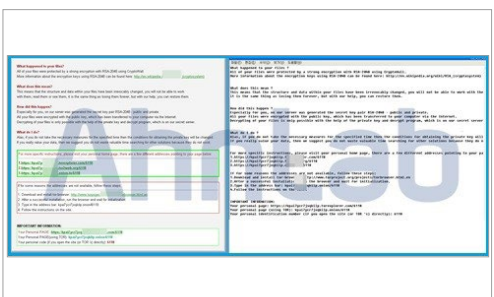


그림 2-23 | 크립토월 감염 시 나타나는 창

해당 악성코드는 감염 시 다양한 확장자 파일(*.doc, *.docx, *.xls, *.ppt, *.psd, *.pdf, *.eps, *.ai, *.cdr, *.jpg, etc.)을 RSA-2048 알고리즘을 이용하여 암호화하고 [그림 2-23]과 같은 창을 사용자에게 보여준다. 해당 문서에는 RSA-2048 알고리즘이 무엇인지, 복구 방법은 무엇인지, 파일을 정상화하기 위해 어떻게 해야 하는지에 대해 자세히 설명해준 후 그 대가로 사용자에게 금전을 요구한다.

기업이나 개인이 중요 문서를 저장하고 있는 PC가 크립토월에 감염되었을 경우 심각한 피해가 우려된다. 이 때문에 악성코드 제작자는 금전을 지불하면서까지 파일을 복구하려는 사람들의 심리를 교묘하게 이용하고 있다.

크립토월에 감염되면 암호화된 파일이 있는 모든 경로에 [그림 2-24]와 같이 3개의 파일이 공통으로 생성된다.

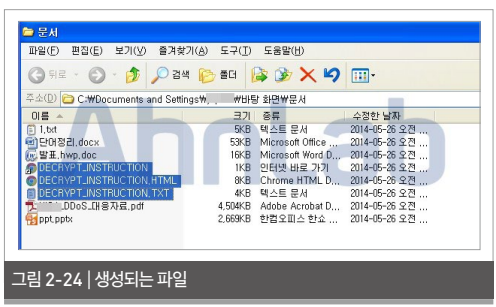


그림 2-24 | 생성되는 파일

생성된 3개의 파일은 [그림 2-23]과 같이 감염 시 나타나는 창과 동일한 내용이다.

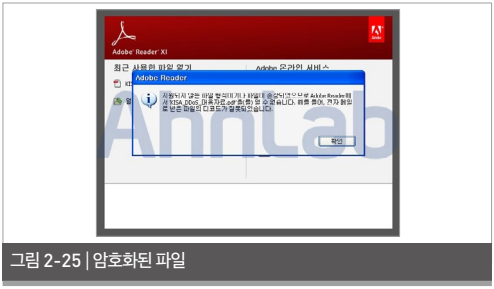


그림 2-25 | 암호화된 파일

악성코드가 실행되면 암호화된 파일은 [그림 2-25]와 같이 파일이 손상되었다는 메시지가 팝업되거나 파일이 열리더라도 알 수 없는 내용으로 가득 차 있다.

그림 2-26 | 암호화 된 PDF 파일(좌) / 정상 PDF 파일(우)

파일의 내부를 살펴보면 정상적인 PDF 파일 구조와는 전혀 다르게 모든 데이터가 RSA 알고리즘에 의해 암호화 되어 있다. 따라서 암호화 키를 알지 못하면 파일만으로는 해독이 불가능하다.

그림 2-27 | 비트코인을 요구하는 페이지

크립토월은 여느 랜섬웨어처럼 제한시간을 정해두고 시간 내에 돈을 지불하지 않으면 요구 금액을 인상한다. 그리고 복호화 키를 삭제하여 아예 복구할 수 없게 만든다는 메시지를 사용자에게 보여준다. 이를 통해 사용자의 판단을 흐리게 하고 결제를 유도한다. 금전 취득을 위해 시간을 제한함으로써 사용자의 불안한 심리를 이용하고 있는 것이다.

또한 샘플로 파일 1개를 통해 복호화가 가능하다는 것을 보여주고 500달러만 지불하면 모든 파일을 복호화할 수 있는 것처럼 사용자들을 유혹하고 있다.

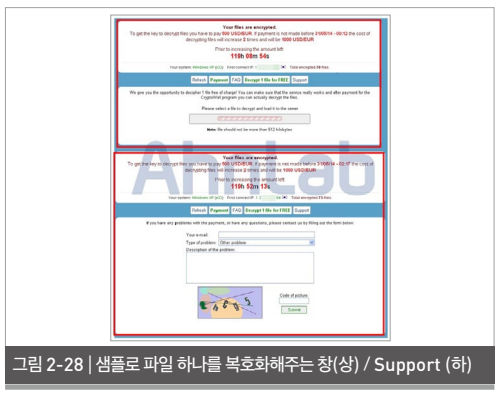


그림 2-28 | 샘플로 파일 하나를 복호화해주는 창(상) / Support (하)

[그림 2-28]을 보면 크립토월은 고객지원 창(Support)이 있어 마치 판매자와 구매자의 관계처럼 대화할 수 있는 페이지가 마련되어 있다(하). 악성코드 제작자는 복호화창(상)을 통해 상세한 내용을 설명해주고 암호화된 파일 한개를 복호화해준다. 사용자에게 신뢰를 얻음으로써 금전적인 이득을 취하기 위해서이다.

ASEC 대응팀은 이 방법으로 악성코드 제작자와 접촉을 시도했으나 응답이 오지 않았다.

랜섬웨어는 중요한 문서를 암호화한 후 복구 대가를 요구하지만 한번 암호화 되면 대가를 제공하지 않고서는 복구 가능성이 매우 희박하다. 또 대가를 지불한다고 해도 모든 파일을 복구할 수 있다는 보장도 없다.

하지만 대가를 지불하지 않고도 암호화된 파일을 복구할 수 있는 방법이 전혀 없는 것은 아니다. 평소 중요한 문서나 파일에 대해 백업해 두는 습관을 들이면 피해를 예방할 수 있다. 윈도의 사용자 파일 백업 기능을 이용하면 된다. 복원지점을 설정해 두었거나 사용자 파일을 백업해 두었다면 해당 악성코드에 감염되더라도 감염 전으로 돌아가 복구할 수 있다.

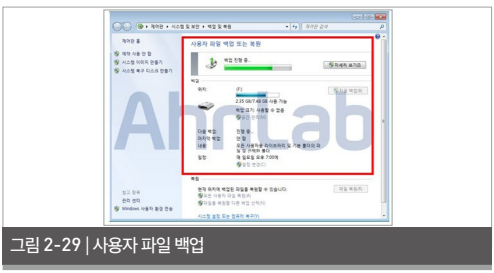


그림 2-29 | 사용자 파일 백업

이때 사용자는 반드시 윈도가 설치된 로컬 디스크가 아닌 다른 저장매체에 저장해야 백업이 가능하다. 로컬 디스크는 백업파일이 저장될 경로에 표시되지 않으며 로컬 디스크에서 백업할 파일이나 폴더를 사용자가 지정할 수 있다.

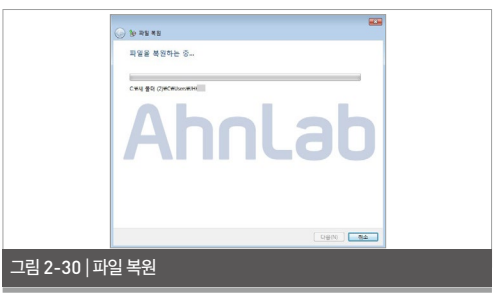


그림 2-30 | 파일 복원

파일 복원을 진행하면 사용자가 백업을 설정한 파일을 원본 파일에 덮어씌워 복원하거나 기존 경로 외에 다른 경로에 저장할 수 있다.

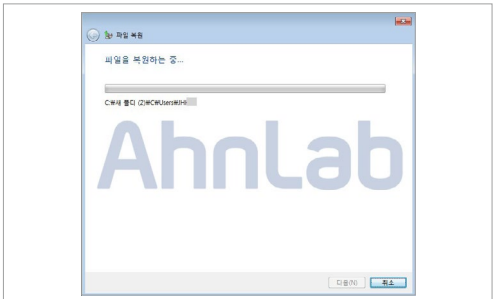


그림 2-31 | 복원 후 파일

[그림 2-31]과 같이 지정된 경로에 백업했던 파일이 복원되고 정상적으로 실행되는 것을 확인할 수 있다.

악성코드 감염에 있어 가장 중요한 것은 대처가 아닌 예방이다. 의심되는 메일이나 첨부파일은 열어보지 않고 중요한 파일은 백업해두는 습관만으로도 악성코드로부터 PC를 지킬 수 있다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Agent (2014.05.27.00)

AhnLab

ASEC REPORT

VOL.53
May, 2014

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 UX디자인팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901