Security Trend

ASEC REPORT

VOL.70

October, 2015

AhnLab

ASEC REPORT

VOL.70 October, 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 10월 보안 동향

Table of Contents

1

보안 통계
STATISTICS

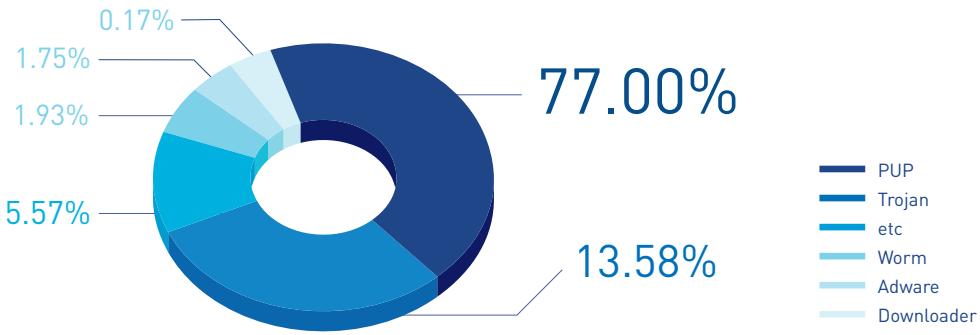
01 악성코드 통계

ASEC이 집계한 바에 따르면 2015년 10월 한 달간 탐지된 악성코드 수는 1,374만 1,322건으로 나타났다. 이는 전월 1,520만 4,993건에 비해 146만 3,671건 감소한 수치다. 한편 10월에 수집된 악성코드 샘플 수는 617만 9,297건이다.

[그림 1-1] 악성코드 추이(2015년 8월 ~ 2015년 10월)

* '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 10월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 77.00%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 13.58%, 웜(Worm)이 1.93%의 비율로 그 뒤를 이었다.



[그림 1-2] 2015년 10월 주요 악성코드 유형

[표 1-1]은 10월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 12만 9,910건으로 가장 많이 탐지되었고, Trojan/Win32.Gen이 11만 4,801건으로 그 뒤를 이었다.

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

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	129,910
2	Trojan/Win32.Gen	114,801
3	Trojan/Win32.Agent	103,522
4	Malware/Win32.Generic	98,757
5	Trojan/Win32.Banki	80,456
6	Trojan/Win32.OnlineGameHack	60,435
7	Unwanted/Win32.Exploit	53,141
8	Worm/Win32.IRCBot	46,705
9	Unwanted/Win32.Keygen	46,642
10	Trojan/Win32.Generic	45,917

02
웹 통계

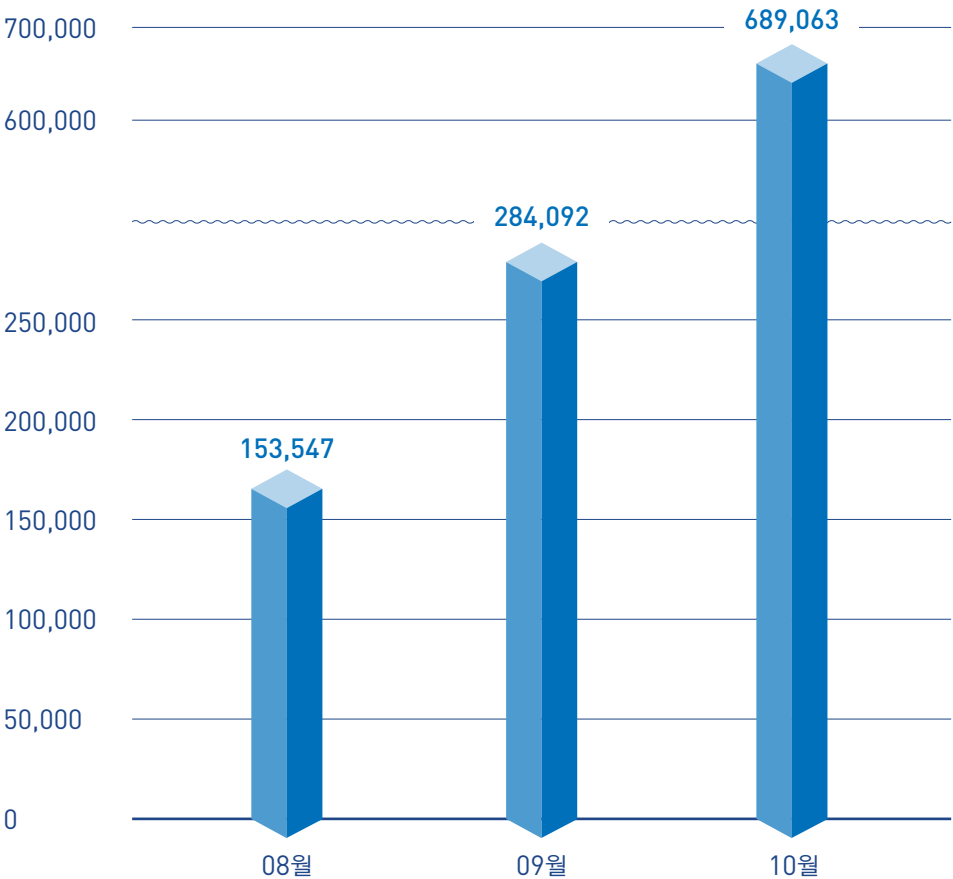
2015년 10월에 악성코드 유포지로 악용된 도메인은 1,535건, URL은 1만 282건으로 집계됐다([그림 1-3]). 또한 10월의 악성 도메인 및 URL 차단 건수는 총 399만 1,443건이다.

[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 8월 ~ 2015년 10월)

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

03
모바일 통계

2015년 10월 한 달간 탐지된 모바일 악성코드는 68만 9,063건으로 집계됐다([그림 1-4]).



[그림 1-4] 모바일 악성코드 추이(2015년 8월 ~ 2015년 10월)

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

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

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	330,240
2	Android-Trojan/FakeInst	56,645
3	Android-PUP/SmsReg	34,608
4	Android-PUP/Noico	29,980
5	Android-PUP/Dowgin	21,709
6	Android-PUP/Zdpay	21,324
7	Android-PUP/Downloader	20,501
8	Android-Trojan/Opfake	16,596
9	Android-PUP/Mmsreg	15,523
10	Android-Trojan/SMSAgent	11,645

2

보안 이슈
SECURITY ISSUE

01 인터넷 우체국을 사칭한 스팸 메일 주의

최근 '인터넷 우체국'을 사칭하는 스팸 메일이 유포되고 있어 인터넷 사용자들의 주의가 요구된다. '소포의 배송 주소가 잘못되어 있으니 확인하라'는 내용으로 사용자들을 유도하여 악성코드 다운로드를 시도한다. 해당 악성코드는 사용자의 키보드 입력 값을 탈취하거나 사용하고 있는 프로그램의 정보를 외부로 전송하는 것으로 확인됐다.

스팸 메일은 여전히 효과적인 악성코드 유포 수단이다. 물론 그간 다수의 보안 침해 사례와 보안 업계의 적극적인 행보로 사용자들의 보안 의식이 높아진 것이 사실이다. 그러자 공격자들은 [그림 2-1]과 [그림 2-2]와 같이 사람들의 호기심이나 일상 생활에 관련이 있을 법한 내용으로 사용자들을 유도하는 사회공학적 기법을 이용하고 있다. 특히 이번에 발견된 우체국 사칭 메일은 최근의 스팸 메일과 달리 영어가 아닌 한국어로 작성되어 있어 스팸 공격이 나날이 고도화되고 있음을 짐작하게 한다.

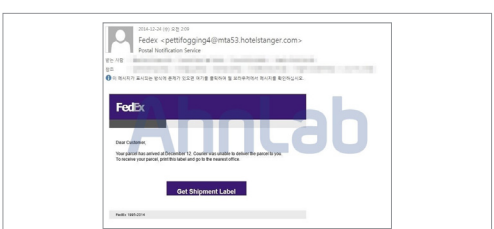


그림 2-1 | 허위 배송 정보 스팸 메일

그림 2-2 | 허위 영수증 스팸 메일

[그림 2-3]은 최근 유포된 우체국 사칭 메일이다. 메일 내에 우체국 로고를 사용하고 있을 뿐만 아니라 어색한 문장이기는 하지만 한국어로 작성되어 사용자의 관심을 유도하고 있다.

그림 2-3 | 우체국 사칭 스팸 메일

만일 사용자가 이 메일의 첨부 파일을 실행하면 <C:₩Documents and Settings₩[사용자 계정]₩Application Data₩랜덤문자열₩> 경로에 "랜덤문자열.exe" 파일이 자가 복제한다. 또한 시스템 시작 시 자동실행되도록 하기 위해 레지스트리에 등록한다(HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩).

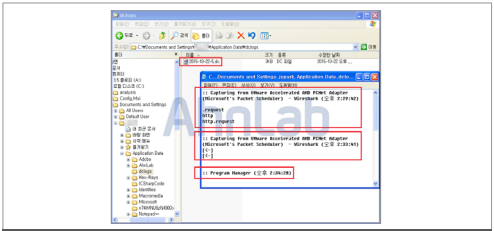


그림 2-4 | 시스템 내 실행 되는 프로그램 및 입력되는 문자열 값 저장

해당 악성코드는 .Net Framework로 제작된 후, 난독화된 실행 파일이다. 이 악성코드는 액세스 토큰에 특권(SeSecurityPrivilege, SeShutdownPrivilege, SeDebugPrivilege 등)을 부여하여 시스템 권한을 획득한 후 사용자가 실행하는 프로그램 및 키보드 입력값을 탈취하여 <C:₩Documents and Settings₩[사용자 계정]₩Application Data₩dclogs₩> 경로에 "Y(년)-M(월)-D(일)-H(시간).dc"라는 로그를 저장한다.

그림 2-5 | AES in CBC mode 암호화 코드

또한 특정 IP 주소로 접속을 시도하는데, 해당 서버와 통신이 이루어지면 감염된 시스템에서 수집한 정보를 AES 암호화한 후 전송하는 것으로 보인다. 이를 통해 C&C 서버로부터 추가 악성코드를 다운받거나 RAT류 악성코드를 이용해 공격자가 감염된 시스템을 원격 제어할 수도 있다.

스팸 메일을 통한 악성코드 유포는 매우 고전적인 수법이지만 사라지지 않고 지속적으로 발생하는 것으로 보아 여전히 유효한 수법임이 틀림없다. 게다가 그 수법이 나날이 지능화되고 있으며, 이번 사례처럼 특정 지역의 사용자를 노리는 '맞춤형 스팸'으로 진화하고 있음을 알 수 있다. 번역기로 돌린 듯 매우 어색한 한국어 문장이지만, 보이스 피싱의 진화처럼 조만간 정확한 한국어 스팸으로 진화할지도 모를 일이다.

따라서 사용자들은 메일 이용 시 아래와 같이 '메일 보안 기본 수칙'에 준수하여 더욱 주의를 기울여야겠다. 아울러 백신 사용 및 최신 엔진 버전 유지, 윈도우 및 각종 응용프로그램의 최신 보안 패치 적용 등 기본적인 부분도 잊지 말아야 하겠다.

[메일 보안 기본 수칙]

1. 출처가 확인되지 않은 메일의 첨부 파일을 함부로 열어보지 않는다.
2. 메일 본문을 꼼꼼히 읽어서 스팸 메일 여부를 확인한다.
3. 폴더 옵션 항목 중 "알려진 파일 형식의 파일 확장명 숨기기" 기능을 해제하여 확장명을 확인할 수 있도록 한다. 확장명 숨기기 옵션을 이용 중인 사용자의 경우 문서 파일 아이콘 등으로 위장한 공격에 노출되기 쉽다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Win-Trojan/FCN.140610 (2015.10.19.06)

02
‘블루스크린’으로 위장한 피싱 사이트

오랫동안 Windows를 사용한 사용자라면 파란 바탕화면에 하얀색 글씨가 나타나는 블루스크린(Blue Screen)을 한 번도 경험하지 않은 사람은 없을 것이다. 블루스크린은 ‘Blue Screen of Death’를 줄여서 부르는 용어로 앞 글자만 따서 ‘BSOD’라고도 부른다. 최근 블루스크린이 발생한 것처럼 위장한 악성 사이트가 발견됐다. 실제로는 사용자를 속여 금품을 갈취하기 위한 피싱 사이트이다.

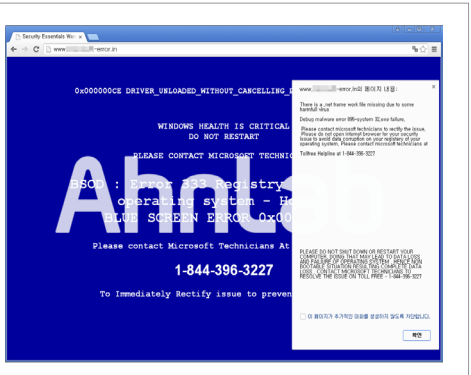


그림 2-6 | 블루스크린 화면으로 위장한 악성 사이트

[그림 2-6]은 최근 발견된 블루스크린 화면으로 위장한 피싱 사이트이다. ‘윈도우에 심각한 문제가 발생하였으며 해결을 위해 마이크로소프트 기술지원센터에 문의하라’는 내용을 담고 있다. 또한 수신자 부담 전화번호를 제공하고 있는데, 이 번호로 전화를 하면 마이크로소프트 직원을 사칭하며 복구 비용을 요구하는 것으로 알려져 있다.

원래 블루스크린은 윈도우(Windows) 이용 시 메모리 액세스 위반, 하드웨어 및 소프트웨어 오류 등 치명적인 시스템 오류가 발생하여 복구될 수 없을 때 나타난다. 오류의 원인을 알려주는 일종의 메시지이지만, PC 사용 중에 갑자기 등장하여 화면 전체를 파랗게 압도하는 탓에 누구든 당황하게 된다. 예컨대 한창 작업 중이던 파일을 미처 저장하지 못했을 때 블루스크린이 나타나 가슴이 철렁했던 순간을 경험한 사용자들이 많을 것이다. 이번에 발견된 피싱 사이트는 바로 이러한 사용자들의 당혹스러움을 이용했다.

물론 컴퓨터 사용에 익숙한 사용자라면 [그림 2-6]과 같은 화면이 나타났을 때 정상적인 블루스크린이 아니라는 것을 알아차릴 수도 있다. 그런데 이 피싱 사이트는 [그림 2-7]과 같이 소스 코드 일부에 사용자가 발생시킨 이벤트를 막는 스크립트가 삽입돼 있어 PC의 ‘Windows 작업 관리자’를 통해 프로세스 자체를 종료하지 않으면 인터넷 브라우저가 종료되지 않는다. 그렇기 때문에 대부분의 사용자들은 순간 당황하여 조작된 거짓 화면과 가이드임을 눈치채지 못할 수도 있다.

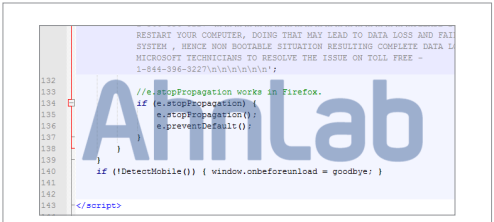


그림 2-7 | 악성 사이트 html 소스 코드 일부

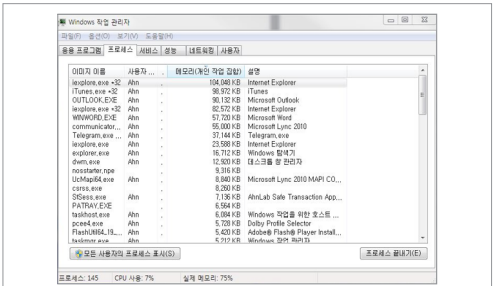


그림 2-8 | 'Windows 작업 관리자'를 통한 프로세스 종료

이 피싱 사이트는 구글의 '광고' 링크를 이용해 불특정 다수의 사용자 접속을 유도한 것으로 확인되었다. 사용자들이 특정 검색어를 입력하였을 때 [그림 2-9]와 같이 검색 결과 링크의 상단 또는 하단에 표시되는 광고 링크를 이용한 것이다.

그림 2-9 | 구글의 광고 링크를 이용한 사용자 클릭 유도

동일한 IP 주소로 조회해봤을 때 다음과 같이 근래에만 다양한 URL이 확인되었음을 알 수 있다.

그림 2-10 | 동일 IP 주소로 조회되는 URL 목록

현재 구글은 관련 이슈를 보고받고 해당 피싱 사이트 링크를 삭제한 상태다. 그러나 공격자들은 URL의 단어 한 두 개만 살짝 바꾸는 등의 수법을 통해 지속적으로 악성 사이트를 유포하기 때문에 사용자들의 각별한 주의가 필요하다.

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

PDF 파일을 악용한 악성코드 사례

PDF 파일을 악용한 악성코드 사례

#사례1: PDF를 악용한 뱅커(Banker)류

A씨는 거래처 영업대표로부터 이메일을 받았다. 메일 제목을 보니 이번 달 제품 단가에 대한 업데이트 문서를 첨부한 것 같았다. 매달 비슷한 내용의 메일을 받기 때문에 별다른 의심 없이 메일에 첨부된 PDF 파일을 열었다. 그런데 PDF 문서 안에는 dd라는 두 글자만 쓰여 있을 뿐이고 다시 첨부 파일을 열라는 팝업창이 나타났다. '문서 포맷이 바뀐 건가?'라고 생각하며 팝업창의 OK 버튼을 눌렀다. 그러자 MS 워드 파일이 열리며 문서가 표시되는데, 역시 아무 내용이 없다. 그리고는 문서 상단에 '매크로를 실행할 수 없다'는 표시가 나타났다. 무슨 문서를 이렇게 복잡하게도 만들었나 싶었지만 어쨌든 매크로를 실행했다. 그런데 또 다시 아무 내용도 안 보인다. 순간 짜증이 났지만 나중에 업체에 연락해야겠다고 생각하며 그 문서를 닫고 다른 업무를 처리했다.

그날 오후, 다른 거래처에 거래 대금을 송금하기 위해 A씨가 인터넷 뱅킹 사이트에 접속하자 보안카드 번호 전체를 입력하라는 팝업창이 나타났다. 뭔가 느낌이 좋지 않다.

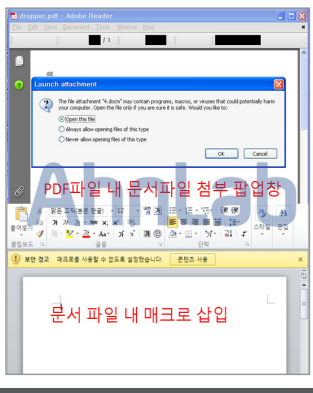


그림 3-1 | 내부에 다른 포맷의 문서 파일 및 EXE 파일을 포함하고 있는 악성 PDF 파일

이와 같이 최근 악성 PDF 파일을 이용한 공격 사례가 잇따르고 있다. 특히 업무 내용으로 위장한 메일의 첨부 파일 형태로 유포되고 있어 더욱 주의가 요구된다.

앞서 언급한 사례는 거래처 영업대표의 메일 계정이 탈취되어 주소록에 포함된 사람들에게 악성 PDF 파일을 첨부한 메일이 전송된 사례를 재구성한 것이다. 그나마 위의 사례에서는 의심 징후를 찾아볼 수 있다. 우선 PDF 문서에 아무 내용이 없었던 점도 이상하

지만 ▲PDF 파일에 MS 워드 문서가 내장되어 있다는 점 ▲MS 워드 파일에도 아무 내용이 없고 매크로가 포함되어 있다는 점 등은 의심해볼 필요가 있다. 대다수의 공격에서는 위와 같은 징후를 알아차리기 쉽지 않다. 위의 사례를 중심으로 PDF 파일을 이용한 최신 공격 방식을 상세히 살펴보고 예방법은 없는지 알아본다.

공격은 어떻게 이루어졌나

우선 메일에 첨부된 해당 PDF 파일에서 문자열을 추출하여 특정 키워드를 검색하는 툴을 이용해 분석했다. 그 결과, PDF 파일 내부에 자바스크립트가 포함되어 있으며, 또 다른 파일이 내장(embedded)되어 있었다.

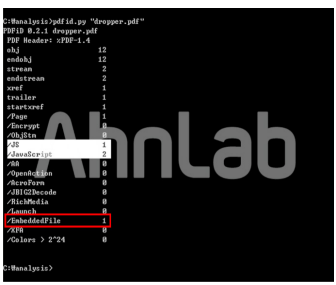


그림 3-2 | PDF 파일 문자열 검색 결과

파일이 내장된 부분은 의심스러우나 자바스크립트 코드는 정상일 수도 있다. 삽입된 자바스크립트는 어떤 기능을 갖는지, 내장된 파일은 어떤 파일인지 확인해보자. [그림 3-3]은 PDF 파일 속에 내장된 파일의 헤더인데, 이처럼 PK 혹은 50 4B를 헤더로 갖는 파일의 종류는 ZIP, JAR, MS 오피스, Open Document 등이다.

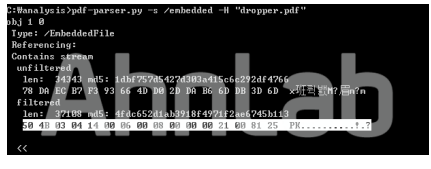


그림 3-3 | PDF 내장 파일의 파일 헤더

앞서 [그림 3-1]의 팝업창에 나타난 파일명이 "4.docm"라는 점에서 해당 PDF에 내장된 파일은 매크로가 포함된 MS 오피스 파일 형식(.DOCM)이라는 것을 유추할 수 있다.

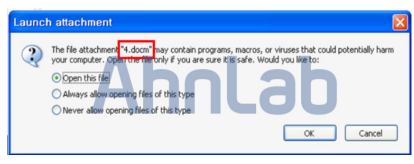


그림 3-4 | 그림 1의 팝업 확대

또한 해당 PDF 파일 내 삽입된 자바스크립트 코드는 특정 객체를 추출하여 실행시키는 명령으로, PDF 파일에 내장된 DOCM 파일을 임시 폴더에 추출하여 실행하기 위한 목적임을 알 수 있다.

그림 3-5 | PDF 파일 내 자바스크립트 코드

이제 자바스크립트를 통해 실행되는 PDF 내의 DOCM 파일이 어떤 행위를 하는지 알아보자. [그림 3-6]은 "4.docm" 파일의 OLE 데이터 스트림을 문자열로 변환한 결과다. A3 스트림에서 매크로를 이용하여 ceece.exe를 다운로드하여 실행하는 것을 확인할 수 있다.

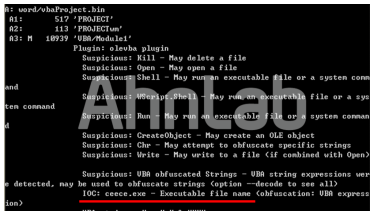


그림 3-6 | 매크로에 의한 EXE 파일 실행

ceece.exe는 파밍 공격에서 주로 사용되는 뱅커(Banker)류의 악성코드로 확인되었다. A3 스트림을 통해 확인한 이 악성코드의 다운로드 경로는 다음과 같다.

http://kons****au.re****ika.pl/07jhnb4/0kn7b6gf.exe

악성 PDF 파일에 의한 피해, 어떻게 예방할 것인가

악성 PDF 자체는 Adobe Reader의 '신뢰 관리자(Trust Manager)' 기능을 통해 피해를 예방할 수 있다. [그림 3-6]과 같이 [편집] > [기본설정] > [신뢰 관리자] 경로에서 'PDF가 아닌 첨부 파일을 외부 응용 프로그램으로 열기 허용' 기능을 해제하면 된다.

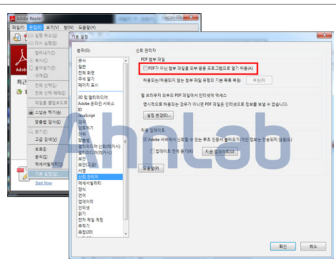


그림 3-7 | Adobe Reader의 신뢰 관리자 화면

위의 기능을 선택 해제하면 PDF 파일 내부에 탑재된 파일에 대해 실행 여부를 묻지 않고 [그림 3-8]과 같이 바로 실행을 차단한다.

그림 3-8 | 외부 응용 프로그램 열기 허용 기능 사용 시(왼쪽)와 기능 해제 시(오른쪽)

사용자가 많은 기업의 경우에는 '액티브 디렉터리'를 통해 다음과 같은 레지스트리 값을 배포하는 것도 방법이다.

[레지스트리 설정 가이드]

- 경로: HKLM\SOFTWARE₩Policies₩Adobe₩<product name>₩<version>₩FeatureLockDown₩cDefaultLaunchAttachmentPerms
- 레지스트리 이름: tBuiltInPermList
- 레지스트리 값: version:1|.ade:3|.adp:3|.app:3|.arc:3|.arj:3|.asp:3|.bas:3|.bat:3|.bz:3|.bz2:3|.cab:3|.chm:3|.class:3|.cmd:3|.com:3|.command:3|.cpl:3|.crt:3|.csh:3|.desktop:3|.dll:3|.exe:3|.fxp:3|.gz:3|.hex:3|.hlp:3|.hqx:3|.hta:3|.inf:3|.ini:3|.ins:3|.isp:3|.its:3|.job:3|.js:3|.jse:3|.ksh:3|.lnk:3|.lzh:3|.mad:3|.maf:3|.mag:3|.mam:3|.maq:3|.mar:3|.mas:3|.mat:3|.mau:3|.mav:3|.maw:3|.mda:3|.mdb:3|.mde:3|.mdt:3|.mdw:3|.mdz:3|.msc:3|.msi:3|.msp:3|.mst:3|.ocx:3|.ops:3|.pcd:3|.pi:3|.pif:3|.prf:3|.prg:3|.pst:3|.rar:3|.reg:3|.scf:3|.scr:3|.sct:3|.sea:3|.shb:3|.shs:3|.sit:3|.tar:3|.taz:3|.tgz:3|.tmp:3|.url:3|.vb:3|.vbe:3|.vbs:3|.vsmacros:3|.vss:3|.vst:3|.vsw:3|.webloc:3|.ws:3|.wsc:3|.wsf:3|.wsh:3|.z:3|.zip:3|.zlo:3|.zoo:3|.pdf:2|.fdf:2|.jar:3|.pkg:3|.tool:3|.term:3

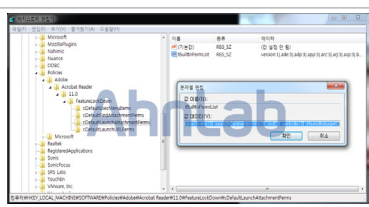


그림 3-9 | 레지스트리 설정

단, Adobe Reader의 메뉴를 통해 '첨부 파일을 외부 응용 프로그램으로 열기 허용' 을 해제하면 생성되는 값이 많은 파일 유형을 포함하기 때문에 주의가 필요하다.

#사례2: PDF를 악용한 피싱 - 배송 업체 사칭

피싱(Pishing)이란, 'private data'와 'fishing'의 합성어로 사용자가 신뢰할 수 있는 유명 기업이나 기관 등으로 속여 사용자 스스로 개인 정보를 입력하도록 유도하여 갈취하는 공격 방법이다. 이 과정에서 사용자의 신뢰를 얻기 위해 다양한 방법을 사용하는데 PDF 문서를 이용해 피싱 사이트로 유도하는 케이스가 발견되었다.

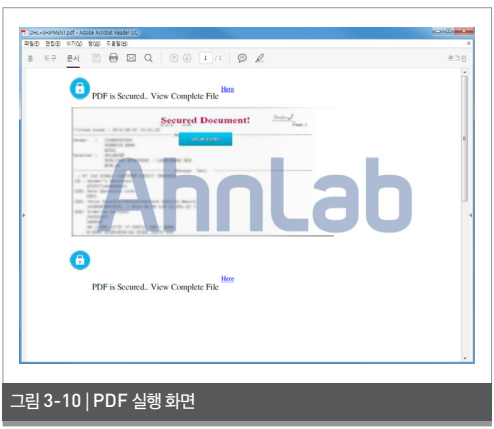


그림 3-10 | PDF 실행 화면

해당 PDF는 해외 유명 운송 업체로 위장하고 있으며, 문서가 암호화되어 있다는 메시지와 함께 피싱 사이트로 접속을 유도한다. 문서가 영어로 되어 있지만, 국내에서도 구매 대행 서비스를 이용해 해외에서 물품을 구매하는 경우가 많기 때문에 국내 이용자들도 주의해야 한다.

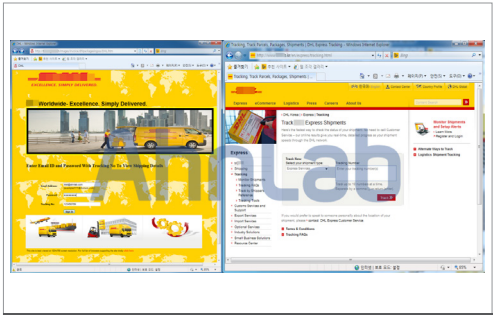


그림 3-11 | 정상 사이트(왼쪽)와 피싱 사이트(오른쪽)

PDF 내부 링크를 클릭하면 피싱 사이트로 연결되며 메일, 비밀번호, 운송 번호를 요구한다. 하지만 정상적인 실제 운송 조회 사이트에서는 운송 조회에 필요한 최소한의 정보만을 요구한다. 따라서 과도한 정보를 요구할 경우 피싱 사이트가 아닌지 의심해봐야 한다.

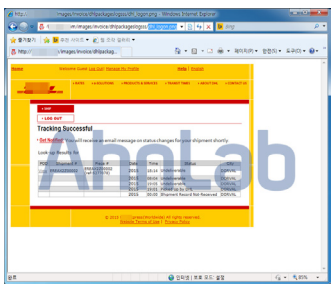


그림 3-12 | 요구 정보 입력 시 나타나는 화면

요구 정보를 모두 입력하면 [그림 3-12]와 같은 화면이 나타난다. 입력 정보와 무관한 그림 파일이기 때문에 어떤 정보를 입력하든 동일하게 이 화면이 나타난다. 입력 정보는 [그림 3-13]과 같이 평문 형태로 배송 업체와 상관없는 서버에 전송되는 것을 확인할 수 있다.

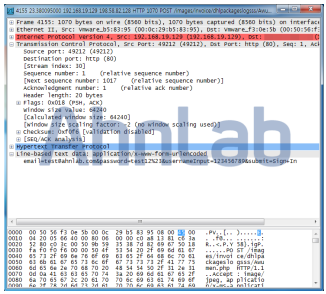


그림 3-13 | 입력 정보 패킷

#사례3: PDF를 악용한 피싱 - 구매 내역 위장

이번 사례 역시 PDF 파일에 피싱 사이트로 접속을 유도하는 링크가 존재하는 경우다. 링크를 클릭하면 [그림 3-14]와 같이 'This PDF is protected' 라는 문구와 함께 사용자의 메일, 비밀번호 정보를 요구한다.

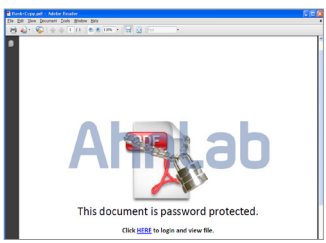


그림 3-14 | PDF 실행 화면

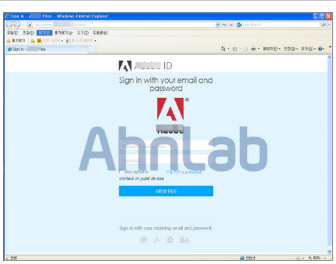


그림 3-15 | 피싱 사이트

사용자 아이디와 비밀번호를 입력하고 'VIEW FILE' 버튼을 클릭하면 정상적인 문서를 브라우저에 보여주며, 동시에 입력된 사용자 개인 정보는 유출된다.

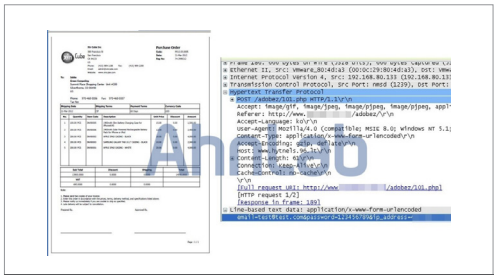


그림 3-16 | 사용자 정보 입력 시 나타나는 문서(왼쪽)와 입력 정보 패킷(오른쪽)

이렇게 공격자에게 개인 정보가 유출될 경우 이를 악용한 추가 피해가 발생할 수 있기 때문에 가급적 출처가 분명하지 않은 메일의 첨부 파일 확인이나 링크 실행 시 주의하길 권장한다. 또한 일반적으로 요청하지 않는 비밀번호, 금융 정보 등과 같은 개인 정보를 요청할 경우, 해당 기관이나 사이트에 진위 여부를 확인해보는 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

PDF/Fakeinvoice (2015.10.15.00)

AhnLab

ASEC REPORT

VOL.70
Octorber, 2015

집필	안랩 시큐리티대응센터 (ASEC)	발행처	주식회사 안랩
편집	안랩 콘텐츠기획팀		경기도 성남시 분당구 판교역로 220
디자인	안랩 디자인팀		T. 031-722-8000
			F. 031-722-8901