Security Trend

ASEC REPORT

VOL.82

October, 2016

AhnLab

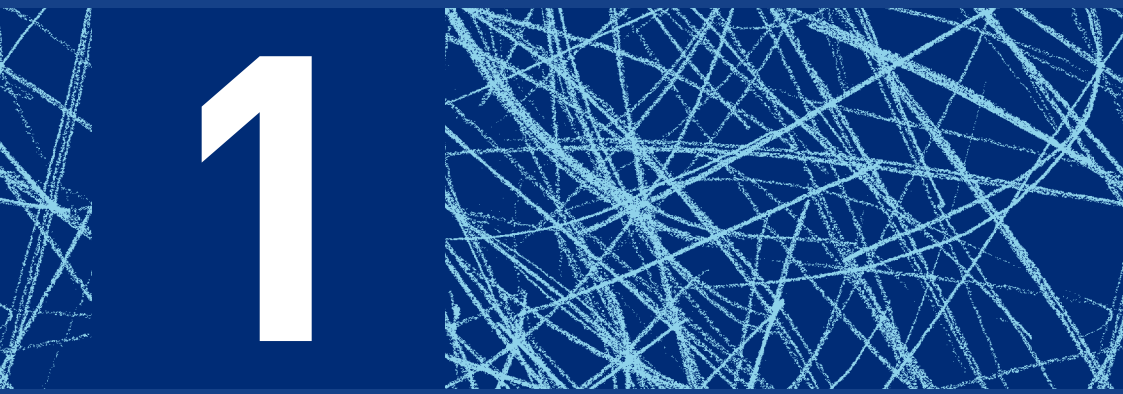
ASEC REPORT

VOL.82 October, 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 10월 보안 동향

Table of Contents

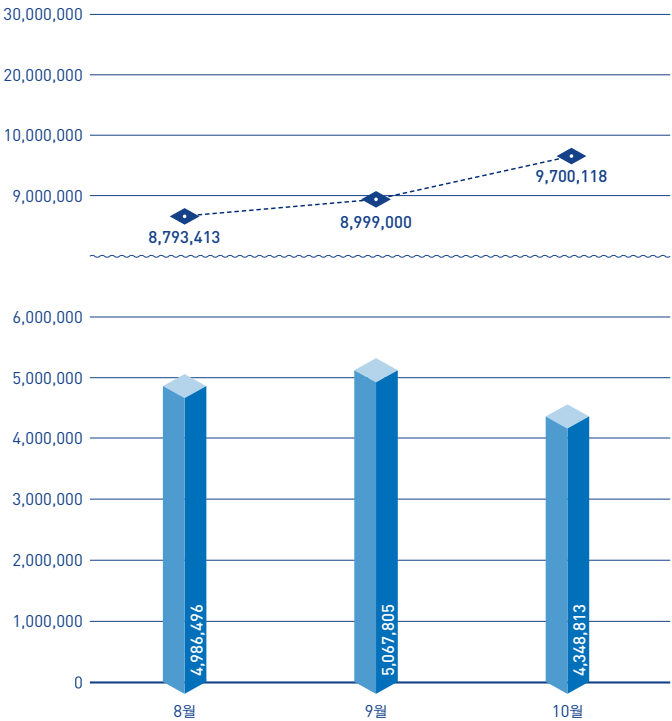


1

보안 통계
STATISTICS

01
악성코드 통계

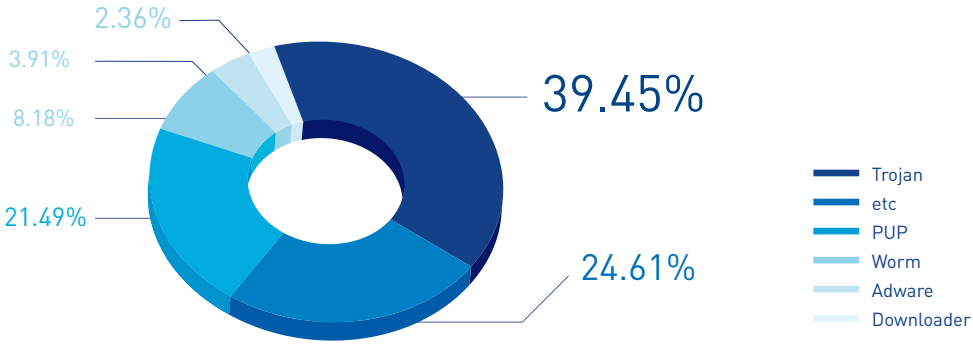
ASEC이 집계한 바에 따르면, 2016년 10월 한 달간 탐지된 악성코드 수는 970만 118건으로 나타났다. 이는 전월 899만 9,000건에 비해 70만 1,118건 증가한 수치다. 한편 10월에 수집된 악성코드 샘플 수는 434만 8,813건이다



[그림 1-1] 악성코드 추이(2016년 8월 ~ 2016년 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 2016년 10월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이 목마(Trojan) 계열의 악성코드가 39.45%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 21.49%, 웜(Worm)이 8.18%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 10월 주요 악성코드 유형

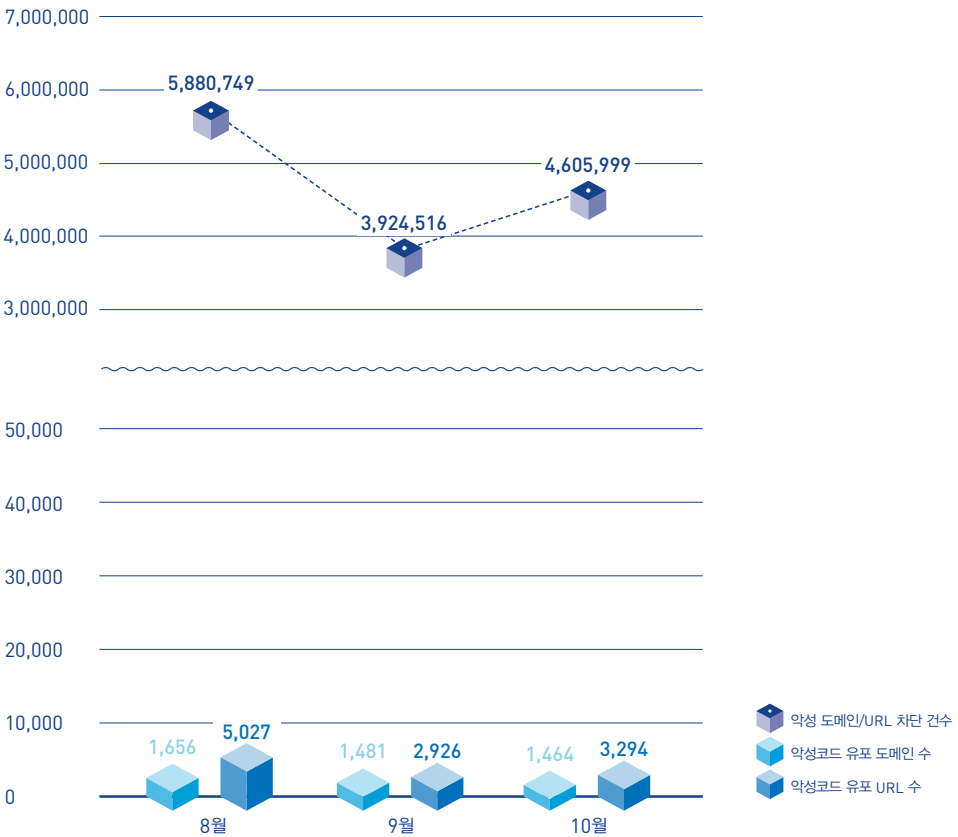
[표 1-1]은 10월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Malware/Win32.Generic이 총 26만 9,368로 가장 많이 탐지되었고, Trojan/Win32.Starter가 20만 7,927건으로 그 뒤를 이었다.

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

순위	악성코드 진단명	탐지 건수
1	Malware/Win32.Generic	269,368
2	Trojan/Win32.Starter	207,927
3	HackTool/Win32.KMSAuto	144,305
4	Trojan/Win32.Banki	141,351
5	Unwanted/Win32.HackTool	129,318
6	Unwanted/Win32.KMS	123,049
7	Worm/Win32.IRCBot	96,306
8	Trojan/Win32.Agent	90,254
9	Trojan/Win32.Neshta	86,531
10	HackTool/Win32.Crack	62,890

02
웹 통계

2016년 10월에 악성코드 유포지로 악용된 도메인은 1,464개, URL은 3,294개로 집계됐다([그림 1-3]). 또한 10월의 악성 도메인 및 URL 차단 건수는 총 460만 5,999건이다.

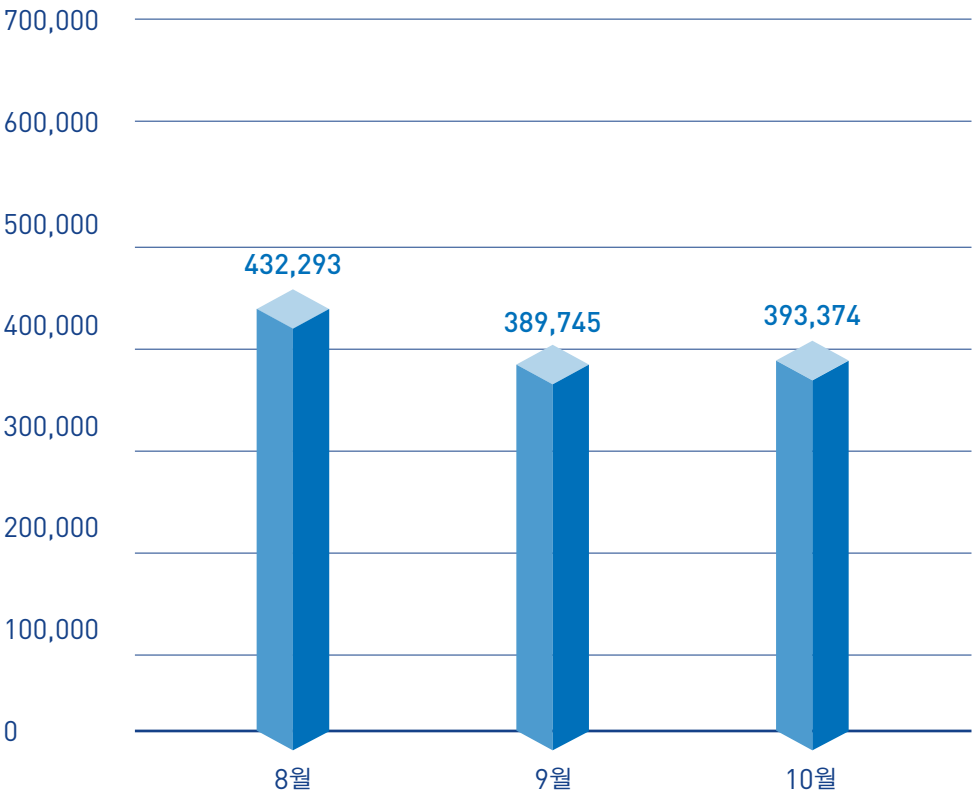


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 8월~2016년 10월)

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

03
모바일 통계

2016년 10월 한 달간 탐지된 모바일 악성코드는 39만 3,374건으로 나타났다.

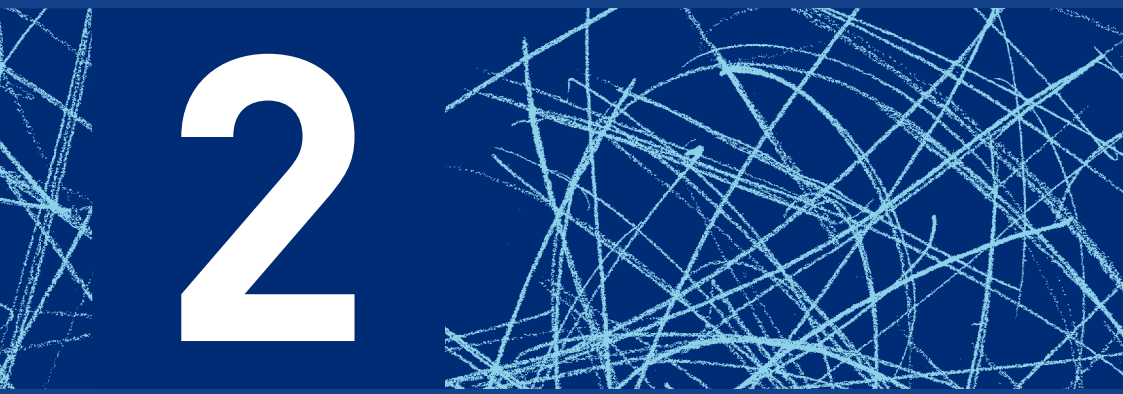


[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 9월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

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

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	55,675
2	Android-PUP/Shedun	37,948
3	Android-PUP/Baogifter	31,087
4	Android-PUP/SmsReg	28,336
5	Android-PUP/Agent	27,592
6	Android-Trojan/FakeInst	26,767
7	Android-Trojan/SmsSend	12,471
8	Android-Trojan/Shedun	10,045
9	Android-PUP/Noico	9,590
10	Android-Trojan/AutoSMS	9,012



2

보안 이슈
SECURITY ISSUE

01 파밍 공격으로 이어지는 ActiveX 주의보

지난 2015년 마이크로소프트(Microsoft)사가 웹 브라우저의 비표준기술인 액티브X(ActiveX)에 대한 공식적인 지원 중단을 발표했다. 하지만 국내의 경우 상당수의 웹사이트에서는 여전히 액티브X를 사용 중인 가운데, 최근 액티브X의 보안 취약점을 노린 파밍(Pharming) 악성코드가 발견됐다. 주로 드라이브 바이 다운로드(Drive-by-download) 방식으로 유포된 기존과 달리, 이번에 발견된 파밍 악성코드는 액티브X를 통해 설치된 불필요한 프로그램(이하 PUP, Potentially Unwanted Program)을 이용해 유포되어 국내 사용자들의 주의가 필요하다.

사용자가 악성 사이트에 접속하면 [그림 2-1]과 같이 PUP 사용을 위해 액티브X를 설치하도록 유도한다. 설치 과정에서 사용자의 동의를 받는 것처럼 보이지만 실제로는 해당 PUP의 이용 약관을 제공하지 않는다.

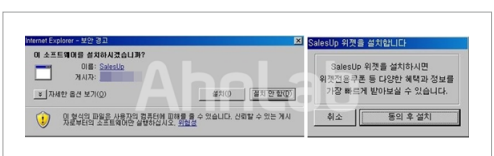


그림 2-1 | 액티브X 설치 화면

사용자가 액티브X의 설치를 실행하면 셋업(Setup) 파일을 통해 PUP가 다운로드되는데, 이때 함께 다운로드되는 version.txt 파일이 [표 2-1]과 같이 변조되어 파밍 악성코드 유포에 이용된다.

표 2-1 | version.txt 정상 (왼쪽) / 변조 (오른쪽)

[version.txt 정보]	
/salesup_up/SalesUpMon.exe	/salesup_up/SalesUpMon.exe
/salesup_up/SalesupUpdate.exe	/salesup_up/Salesup_Update.exe
/salesup_up/SalesupUninstall.exe	/salesup_up/SalesupUninstall.exe
/salesup_up/SalesUp.exe	/salesup_up/SalesUp.exe

파밍 악성코드는 [그림 2-2]와 같이 변조된 version.txt 파일을 기반으로 공격자가 PUP 서버에 생성해둔 악성 업데이트 파일을 사용자 PC에 다운로드한다.

그림 2-2 | 다운로드 된 악성 업데이트 파일 (왼쪽) / 정상 업데이트 파일 (오른쪽)

악성 업데이트 파일이 실행되면 파밍 악성코드는 기존 방식과 동일하게 [표 2-2]와 같이 레지스트리 등록을 통해 웹 브라우저의 메인 페이지를 국내 유명 포털 사이트로 변경시키고, 방화벽에 자기 자신을 예외로 등록한다. 또한 시작 프로그램에 추가하여 시스템이 다시 시작될 때마다 악성코드가 자동으로 실행될 수 있도록 설정한다.

표 2-2 | 레지스트리 등록

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "실행된 경로"

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\[실행된 경로] "Disabled"

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page "www.***.com"

최종적으로 PUP 설치가 완료되면 [그림 2-3]과 같이 사용자에게 설치 완료 페이지를 보여준다. 또한 사용자가 웹 브라우저를 통해 포털 사이트 메인 화면을 접속하면 해당 사이트와 관련된 광고를 노출한다.

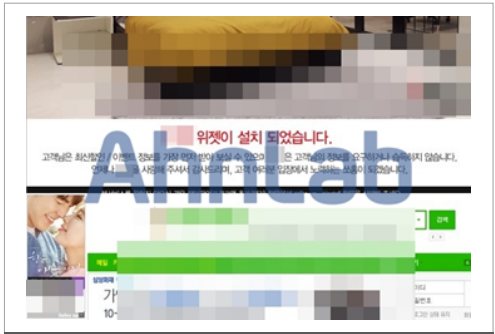


그림 2-3 | 설치 안내 및 광고 노출

이후 사용자가 웹 사이트에 접속하면 [그림 2-4]와 같이 파밍 페이지가 노출된다. 금융감독원 등을 사칭하는 허위 팝업 창을 노출해 사용자로 하여금 주민등록번호, 계좌번호, 비밀번호 등 중요한 개인정보를 입력하도록 유도한다.

그림 2-4 | 파밍 페이지

액티브X는 인터넷 익스플로러(Internet Explorer)에서 멀티미디어 구동, 결제 등 다양한 웹 서비스 이용을 위해 관련 프로그램을 사용자 PC에 직접 설치하는 방식이다. 그러나 호환성 문제, 무분별한 PUP 설치로 인한 PC 성능 저하, 그리고 악성코드 유포 수단으로 악용되면서 보안상의 이유로 지원이 중단됐다.

국내에서도 금융권을 중심으로 여러 규제를 완화시키며 액티브X 퇴출을 선언했지만, 여전히 일부 웹사이트는 액티브X를 이용하고 있다. 액티브X를 통한 악성코드 감염을 방지하기 위해서는 확인되지 않은 프로그램은 설치하지 않도록 해야하며, 웹에서 프로그램을 다운로드할 경우에도 반드시 정식 배포 사이트를 이용하는 것이 중요하다.

V3 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.banki (2016.10.12.03)

Trojan/Win32.Zegost (2016.10.13.00)

PUP/Win32.ShopAdvance (2016.10.13.05)

02
진화하는 '피싱' 메일, 금융정보 노린다

사용자의 금융정보를 노리는 파밍(Pharming) 공격 기법이 나날이 다변화하고 있다. 파밍은 PC에 악성코드를 감염시켜 사용자가 피싱 사이트에 접속하도록 유도한 뒤 입력한 금융정보를 탈취하는 공격 기법이다. 파밍 악성코드는 주로 웹사이트에 접속만 해도 감염되는 드라이브 바이 다운로드(Drive-by-download) 방식이나 정상 유틸리티 프로그램의 업데이트 모듈을 이용하는 방식 등으로 유포된다. 그런데 최근 기존 유포 방식과 달리 '피싱(Phishing) 메일'을 이용한 파밍 악성코드 유포 사례가 발견되어 사용자들의 피해가 우려된다.

이번에 발견된 파밍 악성코드는 [그림 2-5]와 같이 상품 배송 관련 메일로 위장한 피싱 메일을 통해 유포되었다.

그림 2-5 | 상품 배송 정보로 위장한 피싱 메일

공격자는 대량 메일 발송 서비스를 이용하여 불특정 다수의 사용자에게 해당 피싱 메일을 발송한 것으로 추정된다. 발송된 메일은 국내의 한 오픈마켓 웹 사이트로 사칭하고 있으며, 주문한 상품의 배송 조회를 미끼로 메일 수신자에게 상세 내용 조회를 위한 하이퍼링크를 클릭하도록 유도한다.

사용자가 메일 본문의 해당 하이퍼링크를 클릭하면, [표 2-3]과 같이 공격자가 사전에 제작한 악성코드 유포 사이트로 연결된다.

표 2-3 | 악성코드 유포 사이트 정보

174.***.1**.***/index.html

해당 악성코드 유포 사이트는 드라이브 바이 다운로드(Drive-by-download) 방식을 이용한다. 따라서 시스템에 보안 취약점이 존재하는 경우, 해당 웹사이트에 접속만 해도 사용자가 모르는 사이 PC에 악성코드가 다운로드된다.

다운로드된 악성코드가 실행되면 동적 링크 라이브러리(DLL) 파일을 생성한 뒤, 자가삭제된다. 이

때 윈도우(Windows) 운영체제의 정상 파일인 'Rundll32.exe'는 [표 2-4]와 같은 명령어를 통해 생성된 DLL 파일을 실행시킨다.

표 2-4 | DLL 파일 실행 명령어

C:\Windows\System32\Rundll32.exe "C:\...\...\[랜덤문자열]\[랜덤문자열].dll", gPack

실행된 악성코드는 [표 2-5]의 C&C 서버에 연결하여 파밍 공격을 위한 악성 행위를 수행한다.

표 2-5 | C&C 서버 정보

174.1**.1**.**

또한 해당 악성코드는 인터넷 익스플로러(Internet Explorer)의 시작 페이지를 국내 유명 포털 사이트로 변경한 뒤, 자동 구성 스크립트를 수정하여 사용자를 [그림 2-6]과 같은 피싱 페이지로 유도한다.

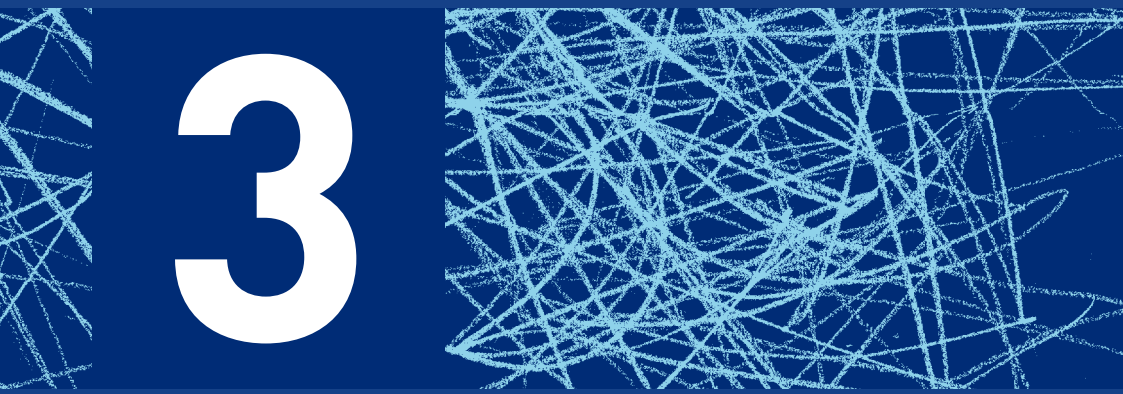
그림 2-6 | 피싱 페이지

전자 금융 거래가 확대됨에 따라, 지난 수년간 파밍 공격은 지속적으로 증가하고 있는 보안 위협 중 하나다. 뿐만 아니라 피싱 메일과 결합한 이번 사례와 같이 파밍 공격은 점점 더 교묘하게 진화하고 있다. 진화한 파밍 공격의 피해를 예방하기 위해서는 기본적으로 출처가 불분명한 메일 열람에 주의해야 하며, 드라이브 바이 다운로드(Drive-by-download) 방식을 이용하는 교묘한 파밍 사이트를 통해 악성코드에 감염되지 않도록 평소 주요 프로그램의 보안 업데이트를 설치해야 한다. 또한 V3 등 백신 제품의 엔진을 항상 최신 버전으로 유지하는 등의 올바른 습관이 필요하다.

V3 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Banki (2016.09.15.06)



3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

01 PC 부팅 방해하는 페트야(PETYA) 랜섬웨어 주의!

01
PC 부팅 방해하는 페트야(PETYA) 랜섬웨어 주의!

최근 사용자 PC의 정상적인 부팅을 불가능하게 만드는 페트야(PETYA) 랜섬웨어가 '스피어 피싱(Spear Phishing)' 메일을 통해 유포됐다. 페트야 랜섬웨어는 파일을 암호화 대상으로 삼는 기존의 랜섬웨어와 달리 사용자 PC의 MBR(Master Boot Record) 영역 코드 자체를 변조하여 감염된 이후에는 정상적인 PC 부팅을 불가능하게 하는 것으로 알려져 있다.

한편 '스피어 피싱(Spear Phishing)'은 '창'이라는 뜻의 영어 단어 스피어(Spear)와 '사용자를 속이는 행위'를 의미하는 용어인 피싱(Phishing)의 합성어다. 악성 첨부 파일을 이용해 수신자의 PC를 감염시킨다는 점은 동일하지만 불특정다수가 아닌 특정인 또는 특정 조직을 노린다는 점에서 더욱 주의해야 한다.

그림 3-1 | 스피어 피싱 메일 정보

[그림 3-1]과 같이 페트야 랜섬웨어를 유포한 스피어 피싱 메일은 홍보 영상에 대한 의견을 구하는 내용으로 위장했다. 그럴 듯한 내용의 메일로 자연스럽게 위장하여 수신자의 관심을 끌고 첨부한 파일을 열어보도록 유도하고 있다.

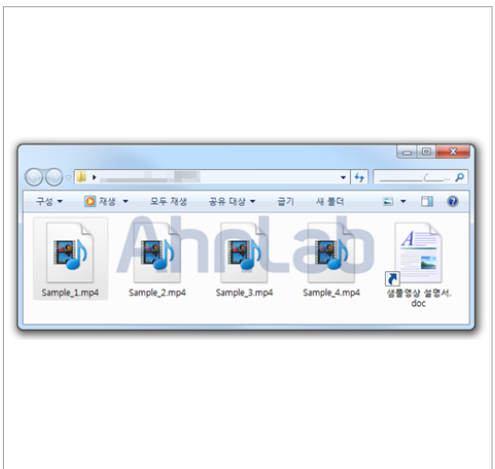


그림 3-2 | 메일 내 첨부 파일

사용자가 메일에 첨부된 파일을 압축 해제하면 [그림 3-2]와 같이 '*.mp4' 형태의 동영상 파일 4개와 '*.doc' 형태의 문서 파일 1개가 나타난다.

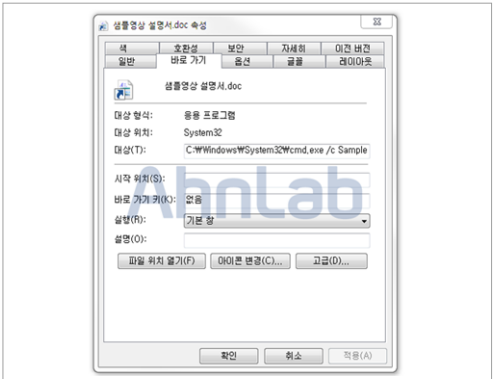


그림 3-3 | 문서 파일로 위장한 '샘플영상 설명서.doc' 파일 속성

[그림 3-3]와 같이 첨부 파일의 속성을 확인하면, '샘플영상 설명서.doc' 파일이 실제로는 문서 파일로 위장한 '*.LNK' 형태의 바로가기 파일임을 알 수 있다. 명령프롬프트를 이용하여 파일 'Sample_4.mp4' 파일을 실행하도록 설정되어 있다. 마찬가지로 'Sample_4.mp4' 파일 또한 영상 파일로 위장한 '*.exe' 형태의 실행 파일이다.

최종적으로 실행된 악성 파일은 메모리 내에 DLL 파일을 생성한다. 이때 시스템 경로인 Program Files (x86) 및 Program Files 폴더의 내부를 탐색하여 사용자 PC 내 백신 프로그램의 설치 여부도 함께 확인한다.

그림 3-4 | 부팅 불가 메시지 화면

페트야 랜섬웨어에 감염되면 [그림 3-4]와 같은 부팅 불가 메시지 화면이 나타나며, MBR(Master Boot Record)과 MFT(Master File Table) 영역을 암호화하여 PC의 정상적인 부팅을 불가능하게 한다. 또한 사용자에게 익명 통신 시스템인 토르 브라우저(Tor Browser)를 이용한 링크 접속을 통해, 시스템 복구를 위한 금전을 지불할 것을 요구한다.

랜섬웨어를 이용한 보안 위협은 점점 고도화되고 있다. 랜섬웨어에 감염되면 치료 및 복구가 어렵기 때문에 예방이 무엇보다 중요하며, 랜섬웨어로 인한 피해를 최소화하기 위한 랜섬웨어 감염 예방법은 [표 3-1]과 같다.

표 3-1 | 랜섬웨어 감염 예방법

- 의심스러운 메일의 첨부파일 열람 금지

- 문서(*.doc, *.ppt, *.pdf, *.hwp), 사진 파일 등 중요 파일의 백업

- 소프트웨어 및 보안업데이트 수시 적용: 랜섬웨어는 소프트웨어 취약점을 이용한 드라이브 바이 다운로드(Drive-by-download) 방식으로 유포되는 경우가 많음

이번 사례를 통해 알 수 있는 것처럼 최근 공격자들은 불특정 다수가 아닌 특정 대상을 목적으로 하는 스피어 피싱 기법을 이용하여 좀 더 신뢰할 만한 내용으로 사용자의 의심을 피한다. 따라서 사용자의 개인 정보에 관련된 내용이나 호기심을 자극하는 제목을 이용한 피싱 메일의 피해를 예방하기 위해서는 조금이라도 수상하거나 출처가 불분명한 메일을 수신했을 경

우, 첨부된 파일을 실행하지 않아야 한다. 또한 주요 프로그램의 보안 업데이트 및 백신 제품의 엔진을 최신 버전으로 유지하는 등 기본적인 보안 수칙을 준수하는 습관이 필요하다.

V3 제품에서는 페트야 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.DiskWriter (2016.10.04.08)

Trojan/Win32.Mischa (2016.10.06.07)

AhnLab

ASEC REPORT

VOL.82
October, 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