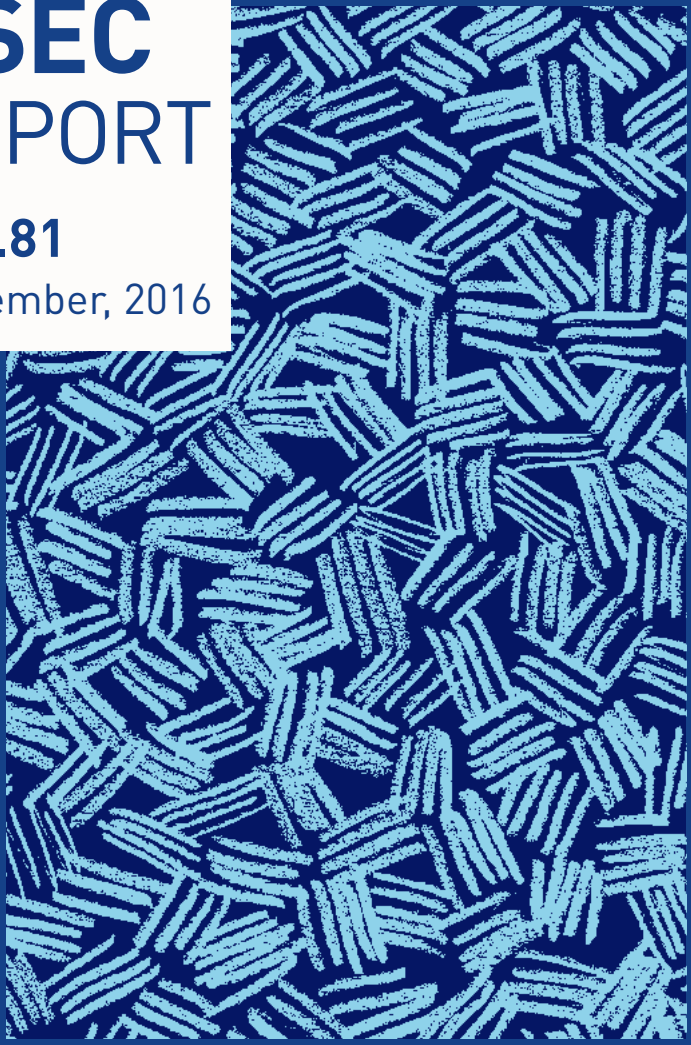
Security Trend

ASEC REPORT

VOL.81

September, 2016



AhnLab

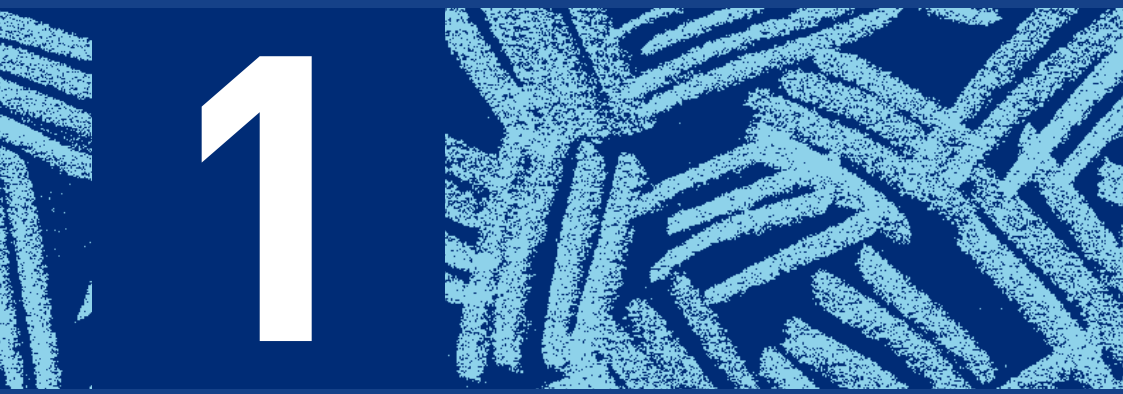
ASEC REPORT

VOL.81 September, 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 9월 보안 동향

Table of Contents

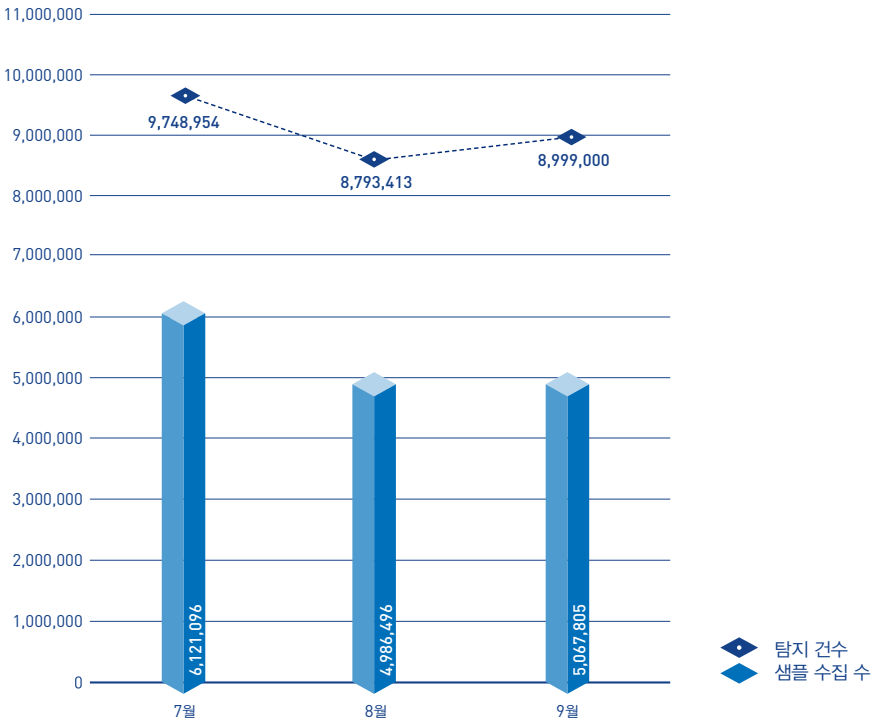


1

보안 통계
STATISTICS

01
악성코드 통계

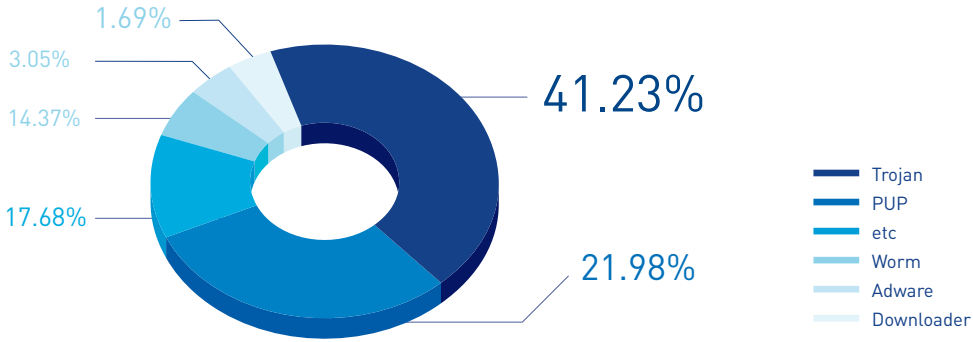
ASEC이 집계한 바에 따르면, 2016년 9월 한 달간 탐지된 악성코드 수는 899만 9,000건으로 나타났다. 이는 전월 879만 3,413건에 비해 20만 5,587건 증가한 수치다. 한편 9월에 수집된 악성코드 샘플 수는 506만 7,805건이다.



[그림 1-1] 악성코드 추이(2016년 7월 ~ 2016년 9월)

* '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 9월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 트로이목마(Trojan) 계열의 악성코드가 41.23%로 가장 높은 비중을 차지했고, 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 21.98%, 웜(Worm)이 14.37%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 9월 주요 악성코드 유형

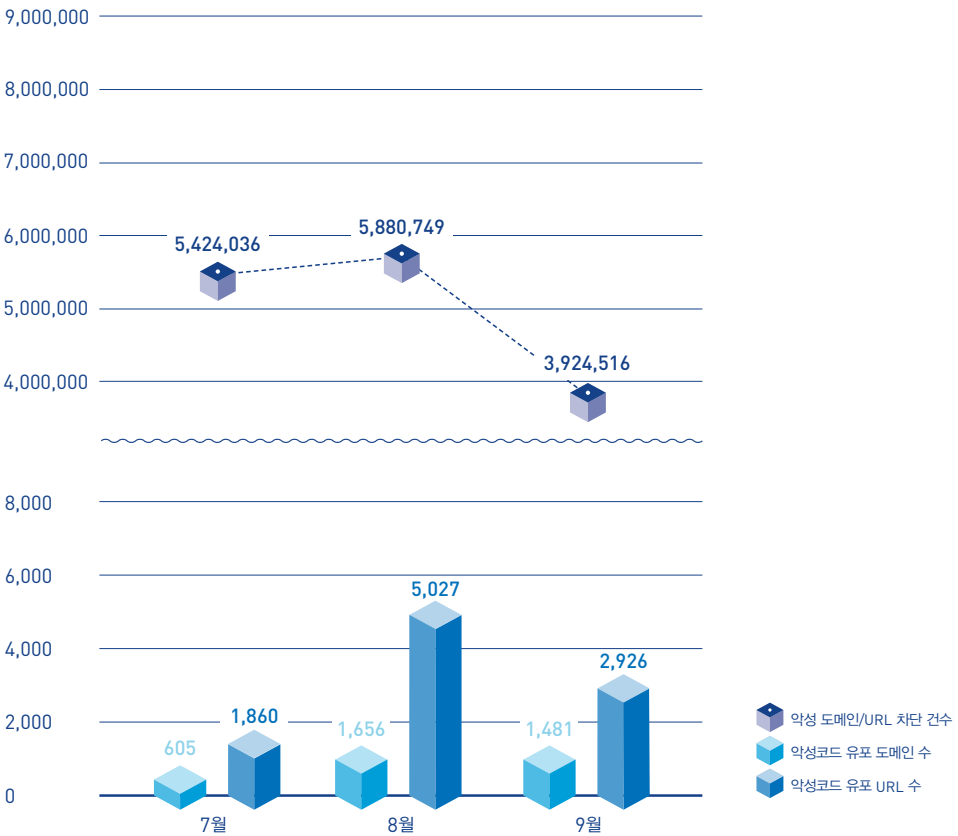
[표 1-1]은 9월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Malware/Win32.Generic이 총 36만 4,620건으로 가장 많이 탐지되었고, Trojan/Win32.Starter가 23만 7,449건으로 그 뒤를 이었다.

[표 1-1] 2016년 9월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Malware/Win32.Generic	364,620
2	Trojan/Win32.Starter	237,449
3	Unwanted/Win32.HackTool	136,623
4	Trojan/Win32.Agent	84,673
5	Trojan/Win32.Neshta	80,937
6	HackTool/Win32.Crack	72,632
7	Trojan/Win32.Banki	68,817
8	ASD.Prevention	60,727
9	Unwanted/Win32.Keygen	57,950
10	Trojan/Win32.OnlineGameHack	55,808

02
웹 통계

2016년 9월에 악성코드 유포지로 악용된 도메인은 1,481개, URL은 2,926개로 집계됐다([그림 1-3]). 또한 9월의 악성 도메인 및 URL 차단 건수는 총 392만 4,516건이다.

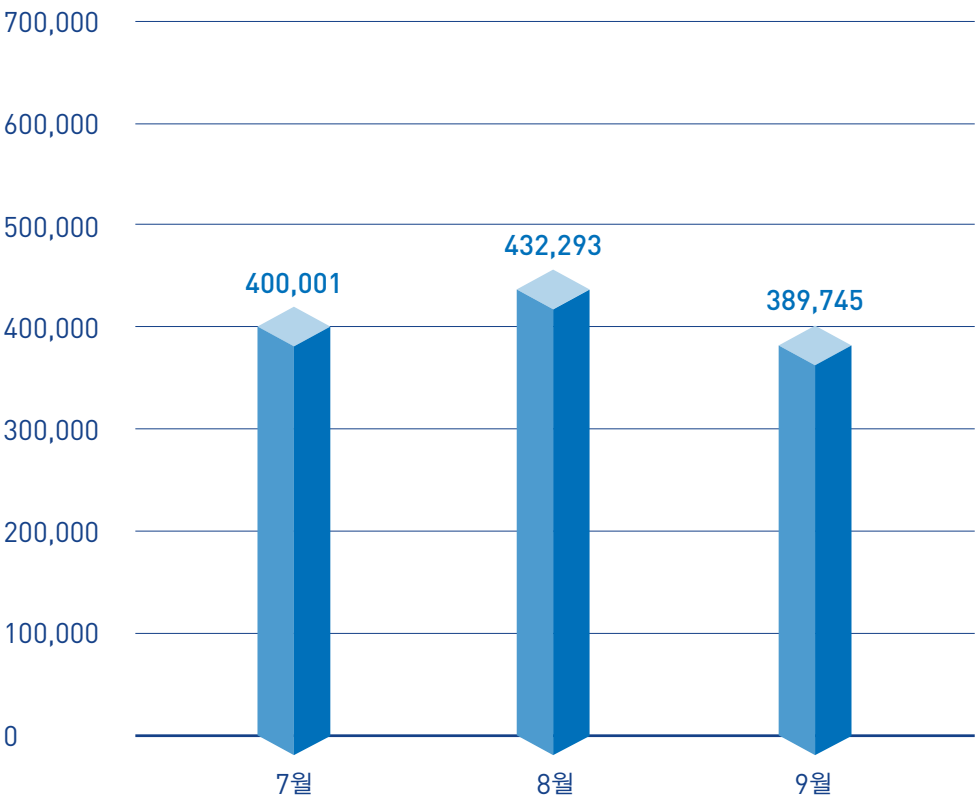


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 7월~2016년 9월)

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

03
모바일 통계

2016년 9월 한 달간 탐지된 모바일 악성코드는 38만 9,745건으로 나타났다([그림 1-4]).



[그림 1-4] 모바일 악성코드 추이(2016년 7월 ~ 2016년 9월)

[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 9월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	109,366
2	Android-PUP/Shedun	60,317
3	Android-PUP/SmsReg	29,238
4	Android-PUP/Noico	23,426
5	Android-PUP/Zdpay	19,957
6	Android-PUP/Agent	15,889
7	Android-Trojan/AutoSMS	11,700
8	Android-Trojan/Agent	9,802
9	Android-PUP/Dowgin	8,352
10	Android-Trojan/Shedun	7,939

2

보안 이슈
SECURITY ISSUE

01 HTA(HTML Application) 파일 형태의 랜섬웨어 다운로더 등장

랜섬웨어로 인한 위협이 점점 고도화되는 가운데, 최근 랜섬웨어를 다운로드하는 '*.hta' 형태의 랜섬웨어 다운로더가 발견됐다. HTML 애플리케이션(HTML Application, HTA) 파일을 뜻하는 HTA 파일은 본래 HTML 파일이 시스템 내 브라우저를 통해 실행되는 것과는 달리, 웹 브라우저와의 연결없이 응용 프로그램처럼 동작하는 것이 특징이다. 이번에 발견된 HTA 랜섬웨어 다운로더는 이와 같은 HTA 파일의 특징을 악용하여 랜섬웨어를 유포시켰다.

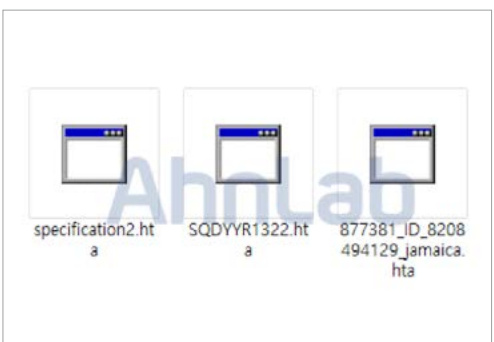


그림 2-1 | HTA 파일 형태의 랜섬웨어 다운로더

[그림 2-1]과 같은 HTA 파일 형태의 랜섬웨어 다운로더는 주로 스팸 메일 내 첨부 파일로 유포되었으며, 해당 파일은 분석이 어렵도록 모두 난독화된 스크립트로 작성되어 있다.

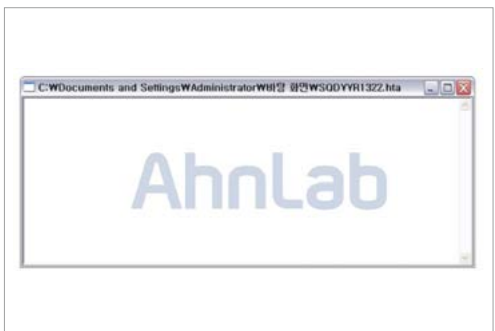


그림 2-2 | HTA 파일 실행 화면

사용자가 악성 HTA 파일을 실행하면 웹 브라우저가 아닌 [그림 2-2]와 같은 프로그램 창이 나타나며, 해당 악성 HTA 파일은 윈도우(Windows) 정상 파일인 mshta.exe를 이용하여 악성 스크립트를 동작시킨다.

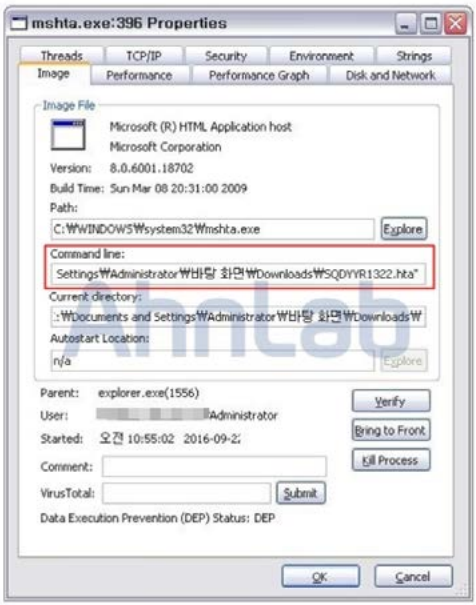


그림 2-3 | mshta.exe 속성

[그림 2-3]과 같이 실행 중인 mshta.exe 파일의 속성 값에서 커맨드 라인(Command line)을 확인하면, 다운로드 경로에 있는 HTA 파일이 실행되고 있음을 알 수 있다.

이 후 악성 스크립트는 [표 2-1]의 주소로 네트워크 연결을 시도한다. 하지만 분석 당시에는 네트워크 연결로 인한 추가 악성 행위는 이뤄지지 않았다. 최종적으로 네트워크가 연결된 후에는 케르베르(Cerber) 랜섬웨어가 사용자 PC에 다운로드된다.

표 2-1 | 네트워크 연결 정보

207.179.106.94:80
198.46.82.242:80
70.39.235.94:80

이번 사례에서 확인할 수 있는 바와 같이 사용자가 실행 파일인 PE 파일을 직접 실행하는 경우에만 랜섬웨어에 감염되는 것은 아니다. HTA 다운로더에 의해 다운로드된 파일이 실행될 때 랜섬웨어에 감염될 수도 있다. 최근 랜섬웨어 다운로더로 다양한 확장자의 파일들이 이용되고 있는데, 그 중 활발히 유포되고 있는 랜섬웨어 다운로더는 *.js, *.wsf, *.hta 파일이다.

따라서 해당 확장자를 가진 파일이 첨부된 스팸 메일을 수신한 경우에는, 해당 메일을 가급적 열어보지 말아야 한다. 또한 랜섬웨어를 다운로드하는 악성 스크립트 파일은 주로 윈도우 정상 프로그램인 wscript.exe와 mshta.exe를 통해 실행되기 때문에 사용자가 의도하지 않았음에도 불구하고 해당 프로그램이 시스템에서 실행 중인 경우, 악성 스크립트 파일이 존재할 가능성이 있으므로 시스템을 점검해 보아야 한다.

V3 제품에서는 해당 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

JS/Downloader (2016.09.21.00)

02 윈도우 업데이트로 위장한 랜섬웨어 주의

최근 윈도우(Windows) 운영체제의 업데이트로 위장한 랜섬웨어가 발견되어 사용자의 각별한 주의가 필요하다. 그동안 윈도우 등 주요 운영체제 및 응용 프로그램의 보안 업데이트를 적용하는 것이 랜섬웨어로 인한 피해를 예방할 수 있는 중요한 수칙 중 하나로 널리 알려져 온 만큼, 윈도우 업데이트 위장 랜섬웨어로 인한 사용자들의 잠재적 피해가 예상된다.

그림 2-4 | 윈도우 업데이트로 위조된 화면

먼저 영어권 사용자를 노린 것으로 추정되는 윈도우 10 업데이트로 위장한 팬텀(Fantom) 랜섬웨어 사례를 살펴보자. 해당 악성코드는 사용자 PC에 'WindowsUpdate.exe' 라는 이름으로 파일을 생성한 뒤 실행한다. 이때 [그림 2-4]와 같이 윈도우 중요 업데이트로 위장한 화면을 사용자에게 보여주는 데, 이와 같은 가짜 업데이트가 진행되는 동안 랜섬웨어는 사용자 몰래 시스템 내 파일을 암호화한다. 기존 랜섬웨어와 동일하게 시스템 내 거의 모든 포맷의 파일을 암호화시키며, 암호화가 완료되면 파일 확장자 끝에 'fantom' 이라는 문자열을 추가한다.

끝으로, 팬텀 랜섬웨어는 시스템의 바탕화면을 변경하고 'DECRYPT_YOUR_FILES.HTML' 파일을 생성하여 암호화된 파일 복구와 관련된 내용을 사용자에게 안내한다. 또한 [그림 2-5]와 같이 VSC(Volume Shadow Copy) 파일을 삭제하는 %APPDATA%\delback.bat'를 생성하여 시스템 복원을 방해한다.

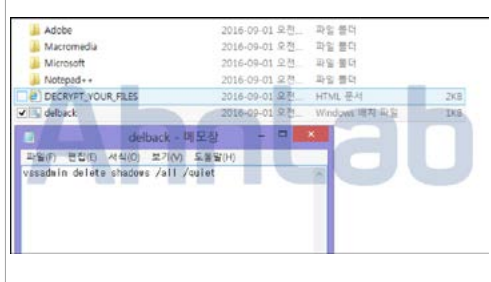


그림 2-5 | VSC 파일을 삭제하는 delback.bat

팬텀 랜섬웨어에 이어 최근에는 러시아 사용자를 노리는 것으로 추정되는 RAA 랜섬웨어가 발견됐다. RAA 랜섬웨어는 앞서 살펴본 사례와 마찬가지로 윈도우 업데이트를 위장한 내용으로 사용자들을 유도하고 있다.

RAA 랜섬웨어는 DOC 문서 파일 형태로 유포되며, 해당 악성 파일을 실행하면 [그림 2-6]과 같이 러시아어로 '이 파일은 MS 오피스 워드의 최신 버전에서 만들어진 것으로, 문서를 보기 위해서는 공식 업데이트 패키지를 설치하라'는 내용이 나타난다.

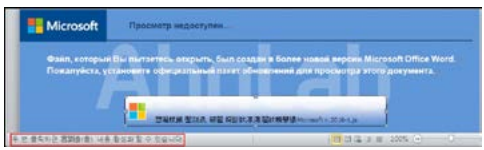


그림 2-6 | RAA 랜섬웨어가 포함된 DOC 문서

또한 해당 내용의 하단에는 마이크로소프트(Microsoft)사의 로고가 포함된 설치 패키지가 있어, 사용자가 의심하지 않고 실행하도록 유도한다. 설치 패키지를 실행하면 내부에 삽입된 스크립트가 실행되는데, 해당 스크립트에는 [표 2-2]와 같은 내용의 악성 행위를 수행하는 코드가 존재한다.

표 2-2 | 악성 행위를 수행하는 코드 정보

1. 내 문서 폴더에 스크립트 복제 - dfsdb.js
2. 특정 문자열이 포함된 확장자 파일 암호화
3. base64로 인코딩된 데이터(랜섬 노트, 실행 파일) 복호화 및 생성
4. 특정 URL 접근

악성 스크립트의 내용을 분석한 결과, [그림 2-7]과 같이 파일 암호화를 수행하는 코드가 있는 것이 확인됐다. 또한 [그림 2-8]과 같이 스크립트의 일부 내용은 난독화되어 사용자가 확인할 수 없도록 했으며, href 태그(google.com)가 설정된 사항 이외에 접근하는 URL에 대한 다른 내용은 확인되지 않았다.

그림 2-7 | 파일 수정 및 암호화를 수행하는 스크립트 일부

그림 2-8 | 난독화된 스크립트 내부 및 복호화 후 실행 파일을 생성하는 스크립트

파일 암호화 진행 시, 랜섬웨어는 자바스크립트(JavaScript)의 indexOff를 통해 암호화 대상 파일의 확장자를 검색한다. [표 2-3]과 같은 문자열을 포함하는 확장자를 검색하므로 docm, docx, xlsx 등의 문서 파일도 모두 암호화 대상이다.

표 2-3 | 암호화 대상 문자열

.doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar, csv

악성 스크립트를 통해 생성된 실행 파일(ii.exe)은 특정 네트워크로 연결을 시도하지만, 분석 당시에는 해당 C&C 서버와 연결이 되지 않아 추가 기능은 확인할 수 없었다. RAA 랜섬웨어의 감염 안내 메시지는 [그림 2-9]와 같다.

그림 2-9 | RAA 랜섬웨어 감염 안내 메시지

이번에 발견된 두 건의 윈도우 업데이트로 위장한 랜섬웨어는 각각 영어와 러시아어로 제작된 것으로 보아 국내 사용자를 공격 대상으로 한 랜섬웨어는 아닌 것으로 추정된다. 다만 이러한 유형의 악성코드는 변형되어 언제든 국내로 유포될 가능성이 있으므로 이에 대한 사용자의 각별한 주의가 필요하다. 특히, 사용 중인 프로그램 및 운영체제의 최신 버전 업데이트는 반드시 정품 소프트웨어 제조사에서 제공하는 업데이트 사이트를 통해 진행하는 것이 바람직하다.

V3 제품에서는 해당 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

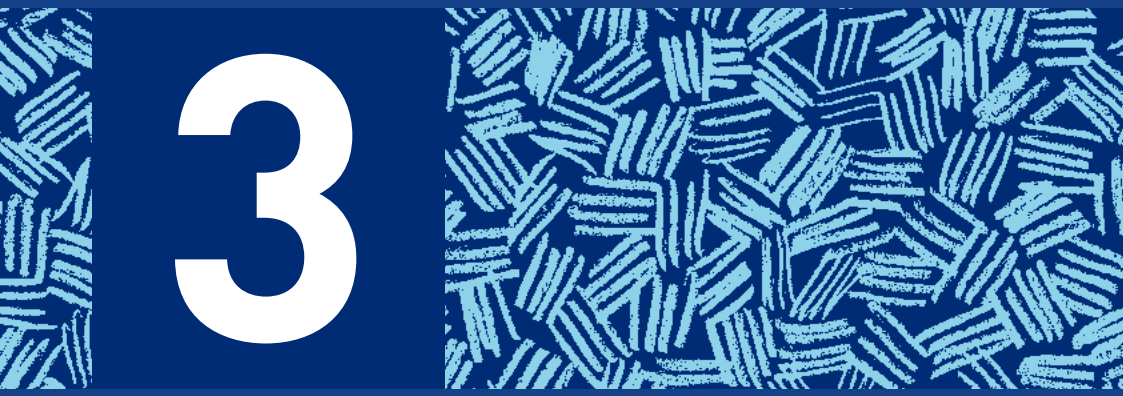
<V3 제품군의 진단명>

Trojan/Win32.Tear (2016.08.26.03)

DOC/Downloader (2016.09.01.00)

JS/Downloader (2016.09.01.00)

Trojan/Win32.Upbot (2016.08.30.03)



3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

01 해킹된 업데이트 서버 통한 파밍 주의보

01 해킹된 업데이트 서버 통한 파밍 주의보

최근 국내 가상 드라이브 프로그램의 업데이트 서버가 해킹되어 파밍(Pharming) 악성코드가 유포된 사례가 발견됐다. 공격자는 웹 사이트나 스팸 메일 내 첨부 파일을 통해 악성코드를 유포한 것이 아닌, 정상 업데이트 서버를 이용하여 다수의 사용자 PC를 감염시켰다. 정상적인 업데이트 파일로 위장해 사용자 PC에 설치된 파밍 악성코드는 공인인증서를 탈취하고, 인터넷 접속 시 금융감독원을 사칭하는 팝업창을 통해 사용자의 개인정보를 입력하도록 유도하고 있어 사용자의 각별한 주의가 필요하다.

그림 3-1 | 업데이트를 통한 악성코드 다운로드

이번에 발견된 악성코드는 [그림 3-1]과 같이 'CDSpaceUpdate.exe'라는 프로그램의 업데이트를 위해 서버로부터 정상 파일을 다운받는 것처럼 위장한 뒤, 실제로는 악성코드인 'CDSpace8.exe' 파일을 다운로드한다.

그림 3-2 | 악성 파일인 CDSpace8.exe의 정보

사용자가 다운로드된 'CDSpace8.exe' 악성 파일을 실행하면, [표 3-1]과 같이 레지스트리 값이 추가되어 해당 악성코드가 시스템 시작 시 자동 실행될 수 있도록 한다. 또한 웹 브라우저의 시작 페이지를 특정 포털 사이트로 등록시킨다.

표 3-1 | 악성코드가 등록시키는 레지스트리 값

레지스트리 키	값
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\(시스템 MAC주소)	C:\ProgramFiles\CDSpace\CDSpace8\CDSpace8.exe
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page	www.naver.com

또한 해당 악성코드는 특정 URL에 접속하여 [그림 3-3]과 같이 IP 주소를 받아오게 되는데, 획득한 IP 주소를 통해 난독화된 스크립트를 실행하여 사용자 PC에서 파밍 행위를 수행한다.

그림 3-3 | 특정 URL 접속 후 IP 주소 획득

이때 악성코드는 사용자 PC 내 호스트(hosts) 파일의 직접적인 변조가 아닌 [그림 3-4]와 같은 프록시 자동 설정(Proxy Auto-Configuration, PAC) 스크립트를 이용하여 사용자가 포털 사이트 접속 시, 변조된 위조 웹 사이트로 접속하도록 유도한다.

그림 3-4 | 난독화된 PAC 스크립트

PAC 스크립트는 [그림 3-5]와 같이 공격 대상 사이트를 분별하여 공격자가 지정해 놓은 특정 사이트 접속 시에만 사용자를 위조된 웹 사이트로 연결시키며, 그 외 사이트 접속 시에는 정상 웹 페이지를 출력시킨다.

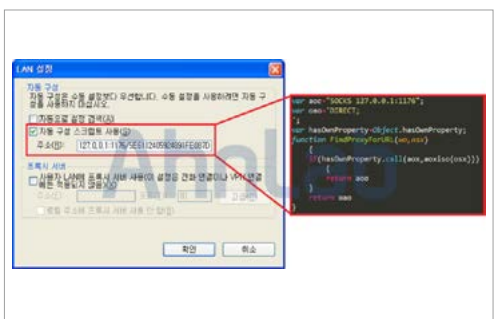


그림 3-5 | 공격 대상 사이트 분별

최종적으로 악성코드에 감염된 시스템에서 사용자가 해당 사이트를 접속하면, [그림 3-6]과 같이 파밍

공격 사례에서 흔히 볼 수 있는 금융감독원을 사칭한 파밍 감염 화면이 출력된다.

그림 3-6 | 파밍 감염 화면

시스템에 저장된 금융 정보 탈취 및 위조된 웹 사이트 접속 등의 기능을 가진 해당 파밍 악성코드는 기존의 파밍 악성코드와 유사하지만, 업데이트 서버를 이용했다는 점에서 사용자들의 피해가 우려된다. 최근에는 취약한 웹사이트를 공격하여 시스템 내 응용 프로그램 취약점을 통해 유포되는 드라이브 바이 다운로드(Drive-by-download) 공격 기법 이외에도 이번 사례와 같이 정상 프로그램의 업데이트 서버를 해킹하여 악성코드를 유포하는 방식 또한 증가하는 추세다. 점점 더 교묘하게 진화하고 있는 파밍 공격을 예방하기 위해서는 보안 업데이트를 설치하여 드라이브 바이 다운로드(Drive-by-download) 공격을 막고, 프로그램 설치 시 함께 설치되는 제휴 프로그램을 주의해야 한다. 또한 백신 제품의 엔진을 최신 버전으로 항상 유지하는 올바른 습관도 필요하다.

V3 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Banki (2016.09.11.06)

AhnLab

ASEC REPORT

VOL.81
September, 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