Security Trend

ASEC REPORT

VOL.79

July, 2016

AhnLab

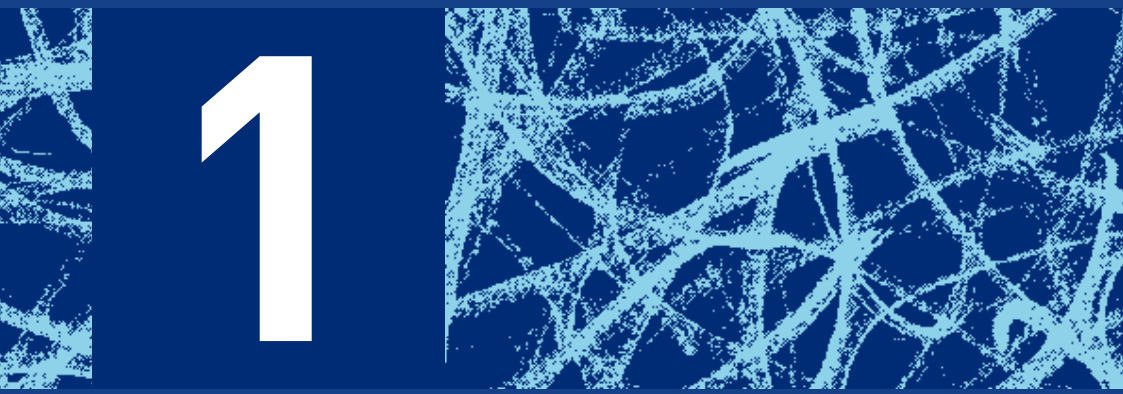
ASEC REPORT

VOL.79 July, 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 7월 보안 동향

Table of Contents

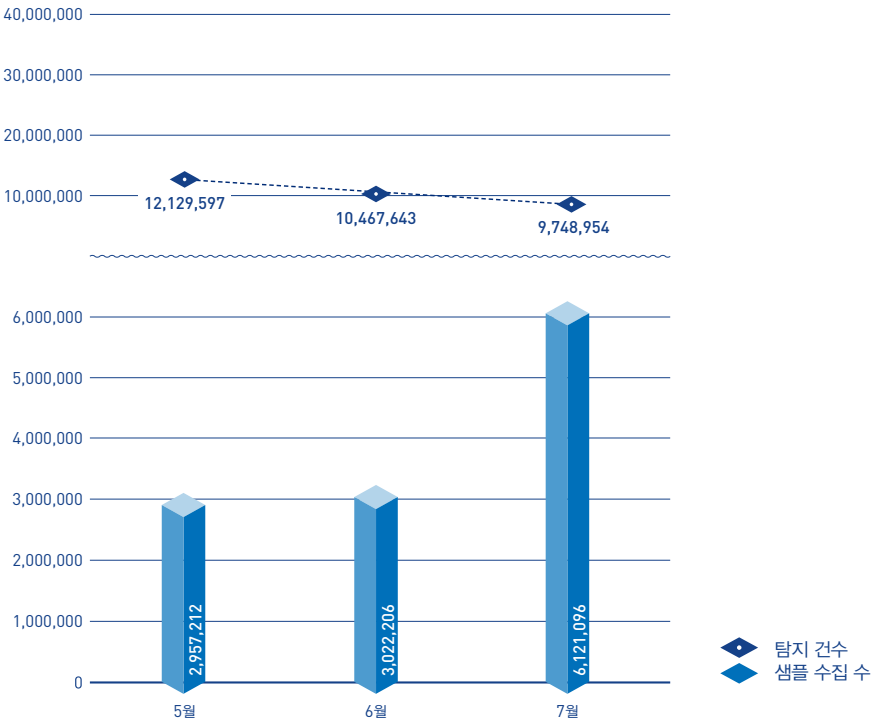


1

보안 통계
STATISTICS

01 악성코드 통계

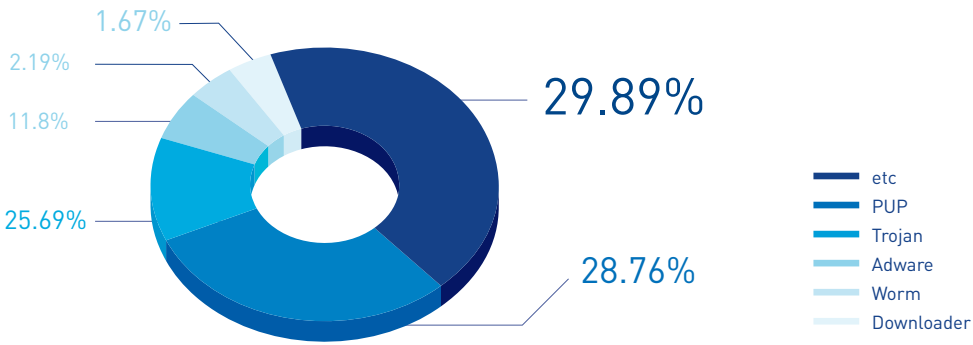
ASEC이 집계한 바에 따르면, 2016년 7월 한 달간 탐지된 악성코드 수는 974만 8,954건으로 나타났다. 이는 전월 1,046만 7,643건에 비해 71만 8,689건 감소한 수치다. 한편 7월에 수집된 악성코드 샘플 수는 612만 1,096건이다.



[그림 1-1] 악성코드 추이(2016년 5월 ~ 2016년 7월)

* '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 7월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 28.76%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 25.69%, 애드웨어(Adware)가 11.8%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 7월 주요 악성코드 유형

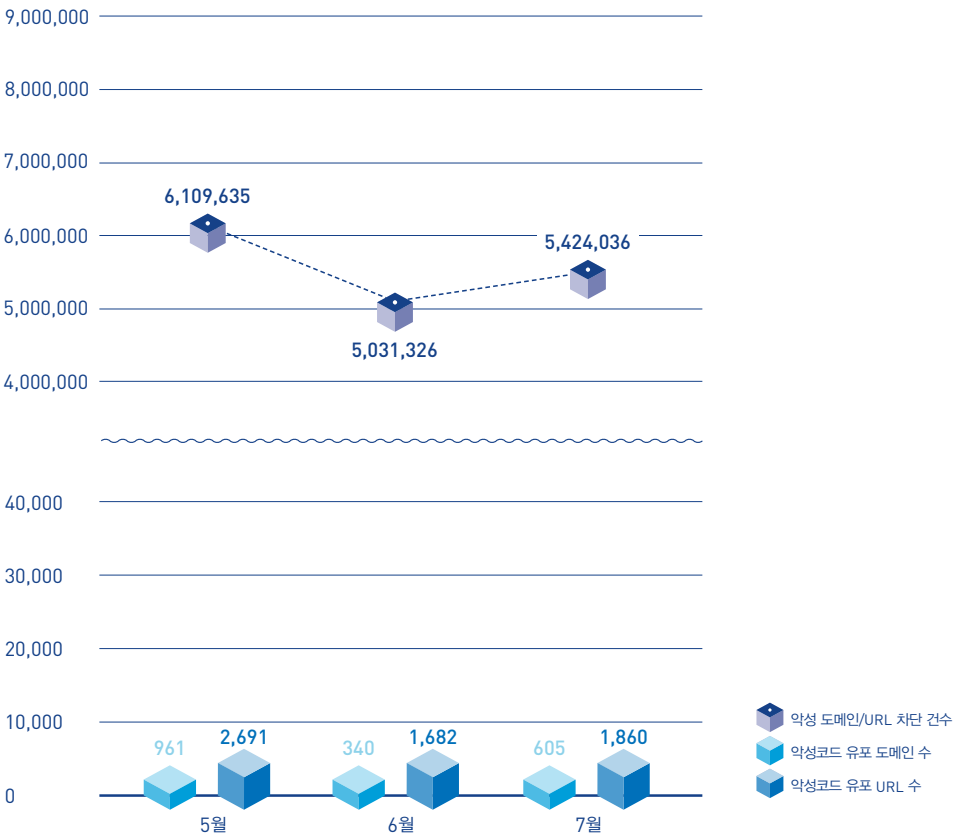
[표 1-1]은 7월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Malware/Win32.Generic이 총 36만 4,815로 가장 많이 탐지되었고, Trojan/Win32.Starter가 17만 9,373건으로 그 뒤를 이었다.

[표 1-1] 2016년 7월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Malware/Win32.Generic	364,815
2	Trojan/Win32.Starter	179,373
3	Unwanted/Win32.HackTool	110,173
4	Trojan/Win32.Agent	78,755
5	Trojan/Win32.Neshta	70,323
6	HackTool/Win32.Crack	68,710
7	Trojan/Win32.CryptXXX	65,758
8	Trojan/Win32.Cerber	57,281
9	ASD.Prevention	54,878
10	Unwanted/Win32.Keygen	53,390

02
웹 통계

2016년 7월에 악성코드 유포지로 악용된 도메인은 605개, URL은 1,860개로 집계됐다([그림 1-3]). 또한 7월의 악성 도메인 및 URL 차단 건수는 총 542만 4,036건이다.

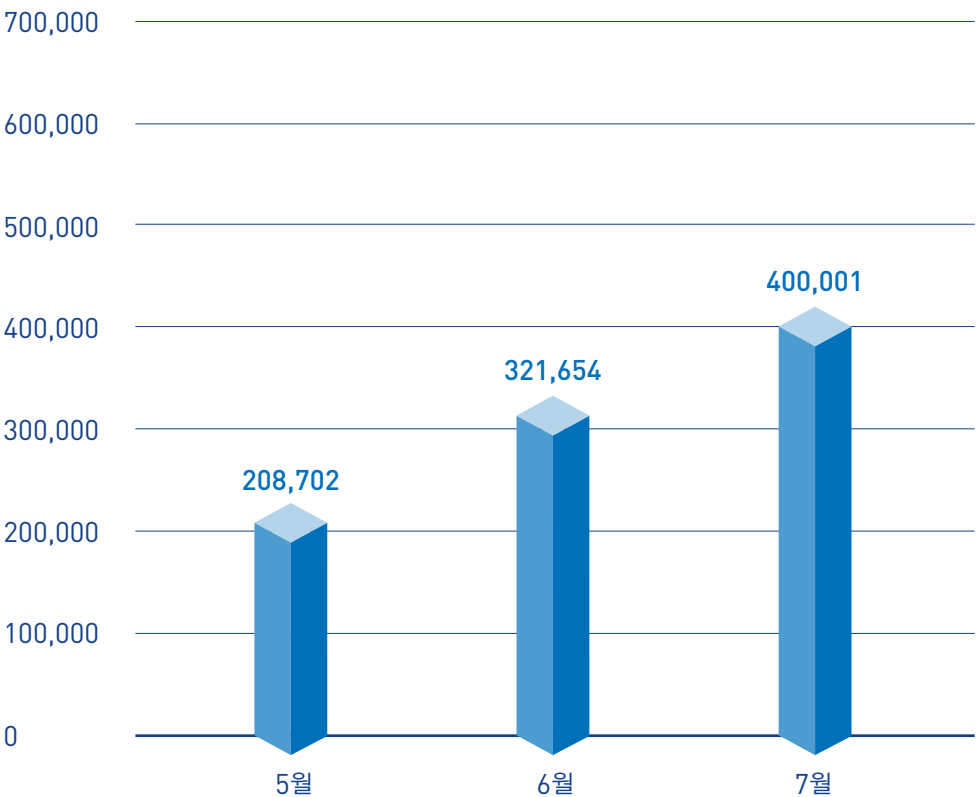


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 5월~2016년 7월)

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

03
모바일 통계

2016년 7월 한 달간 탐지된 모바일 악성코드는 40만 1건으로 나타났다([그림 1-4]).

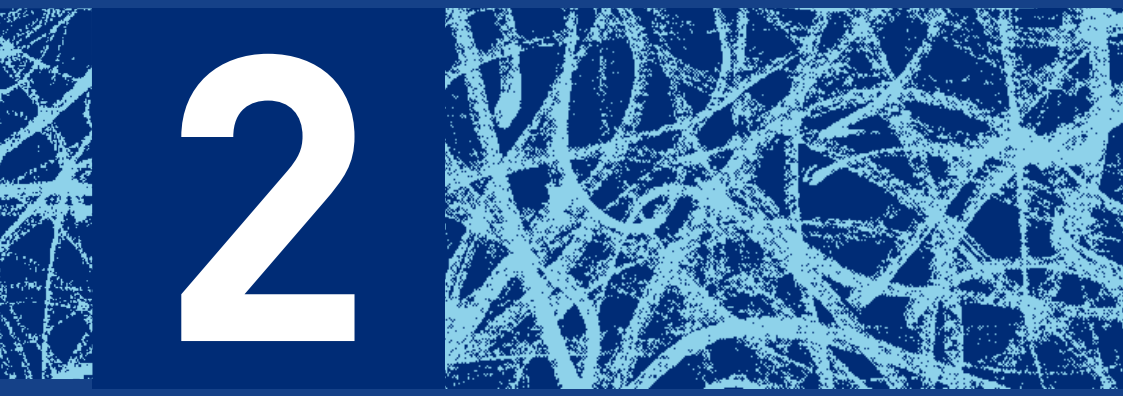


[그림 1-4] 모바일 악성코드 추이(2016년 5월 ~ 2016년 7월)

[표 1-2]는 7월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 7월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	81,588
2	Android-PUP/Shedun	58,123
3	Android-PUP/SmsReg	33,097
4	Android-PUP/Zdpay	26,288
5	Android-PUP/Noico	20,338
6	Android-PUP/Dowgin	17,879
7	Android-Trojan/Hidap	12,051
8	Android-Trojan/Agent	11,063
9	Android-Trojan/Moavt	10,598
10	Android-Trojan/AutoSMS	8,752



2

보안 이슈
SECURITY ISSUE

01 ‘포켓몬 고(Pokemon Go)’ 열풍 속 악성코드 확산 주의보

2016년 7월 초 미국과 오스트리아를 시작으로 현재까지 총 35개국에 정식 출시된 ‘포켓몬 고(Pokemon Go)’는 증강현실(Augmented Reality, AR)을 이용한 스마트폰 게임으로, 전세계적인 열풍을 일으키고 있다. 아직 국내에서는 공식 서비스가 제공되지 않음에도 불구하고 이미 사용자 수가 100만명을 넘어섰으며, 이들 중 상당수는 해외 스토어를 이용하거나 웹사이트 등을 통해 APK 파일을 직접 다운받아 설치한 것으로 추정된다.

그림 2-2 | 정상 APK 파일에 추가된 클래스

이처럼 공식 스토어가 아닌 다른 경로로 게임을 설치하는 사용자들이 증가하고 있는 가운데, 최근 포켓몬 고(Pokemon Go)의 설치 파일 내부에 악성코드가 삽입된 악성 APK 파일이 발견되어 사용자들의 각별한 주의가 필요하다.

그림 2-1 | ‘포켓몬 고(Pokemon Go)’ 공식 홈페이지
(출처: http://www.pokemongo.com)

최근 발견된 악성 APK 파일은 포켓몬 고 게임을 정상적으로 설치하지만, [그림 2-2]와 같이 스마트폰의 정보를 유출하는 악성 기능이 포함된 클래스가 존재한다. 내부 패키지명을 확인한 결과, 드로이드잭(DroidJack)이라고 불리는 안드로이드 RAT(Remote Access Trojans)임을 알 수 있었다. 드로이드잭은 감염된 안드로이드 스마트폰을 공격자가 원격으로 제어할 수 있는 해킹 툴이다.

그림 2-3 | 악성 APK 설치 시 특정 권한 요구

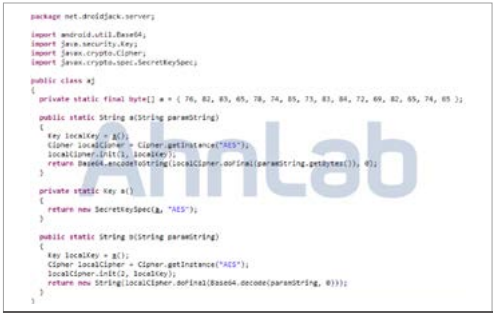


그림 2-4 | 데이터 암호화 부분

안드로이드 운영체제는 사용자가 앱을 설치할 때 해당 앱이 사용하는 특정 권한에 대한 동의 여부를 확인한다. 포켓몬 고의 악성 APK 파일은 [그림 2-3]과 같이 SMS, 전화, 녹음 등 게임과 관련 없는 권한을 요구하여 스마트폰 내 사용자 정보에 접근한다.

표 2-1 | 포켓몬 고 악성코드가 탈취하는 사용자 정보

- SMS
- 주소록
- 통화내역
- GPS 정보
- 단말기 내 파일
- 애플리케이션 실행 및 제어
- 마이크를 이용한 도청 및 녹음

공격자는 [표 2-1]과 같이 포켓몬 고 악성코드에 감염된 스마트폰에서 사용자 정보를 탈취하고, 스마트폰의 시스템을 원격으로 제어한다.

탈취된 스마트폰 내 주요 정보들은 [그림 2-4]와 같이 데이터 암호화를 거쳐 C&C 서버로 전송된다. 최종적으로 공격자는 감염된 시스템을 제어하는 드로이드잭 콘솔을 통해 해당 정보들을 손쉽게 획득할 수 있다.

```
package net.droidjack.server;

public class br
{
  protected static String a = "pokemon.no-ip.org";
  protected static int b = 1337;
  protected static byte c = -1;
}
```

그림 2-5 | 악성 포켓몬 고가 연결하는 C&C 서버 주소

아직 국내에는 정식 출시되지 않은 포켓몬 고 게임을 설치하고 싶어하는 사용자들이 늘어남에 따라 이러한 심리를 이용한 사이버 범죄 및 악성 APK 파일 관련 피해 사례가 증가하고 있다. 스마트폰 이용자는 앱을 다운받아 설치할 때 반드시 공식 스토어를 이용해야 하며, 출처가 불분명하고 안전성이 검증되지 않은 APK 파일의 무분별한 설치는 삼가해야 한다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Android-Trojan/Sandrorat (2015.01.17.01)

02 PC방 관리 프로그램 노린 악성코드 유포 주의

PC방을 노리는 악성코드가 꾸준히 발견되고 있다. 공격자들이 PC방을 노리는 이유는 온라인 게임, 티켓 예매, 수강 신청 등을 위해 많은 사용자들이 밀집되어 있어 악성코드 유포가 용이하기 때문이다. 이처럼 많은 사용자가 이용하는 만큼 PC방의 보안 관리는 더욱 철저히 이루어져야 하는데, 최근 PC방 관리 프로그램을 악용한 악성코드가 발견되어 각별한 주의가 필요하다.

그림 2-6 | PC방 관리 프로그램

[그림 2-6]의 프로그램은 PC방에서 사용하는 관리 프로그램으로, PC의 바탕화면을 관리하는 응용 프로그램이다. 악성코드 제작자는 해당 프로그램이 접근하는 업데이트 서버를 변조하여 PC방의 PC가 악성 파일을 다운로드하도록 유도했다. 변조된 서버를 통해 다운로드된 악성 파일은 [표 2-2]와 같은 경로에 설치된다.

표 2-2 | 악성 파일 설치 경로

%SystemRoot%\syswow64\ime\ping\compts.exe

설치 경로에 있는 compts.exe가 실행되면 [표 2-3]과 같은 악성 파일들이 생성된다. 이때 생성된 atiamellJhKh.dll은 악성 DLL 파일로, rundll.exe에 로드되어 악성 행위를 수행한다.

표 2-3 | 파일 생성 정보

C:\Windows\atiamellJhKh.dll
C:\Windows\Win.log (생성파일 경로 정보)
C:\Winlog.ini (레지스트리 설정 정보)

또한 [표 2-4] 경로에 생성된 Sgfwlxjjf.gif 파일은 atiamellJhKh.dll과 동일한 파일로, 악성 DLL 파일이 자기 자신을 복사한 파일을 이용하여 [그림 2-7]과 같이 *.gif 확장자 형태의 이미지 파일로 위장한 것이다.

표 2-4 | 파일 생성 정보

C:\Program Files\Llrr\Sgfwlxjjf.gif

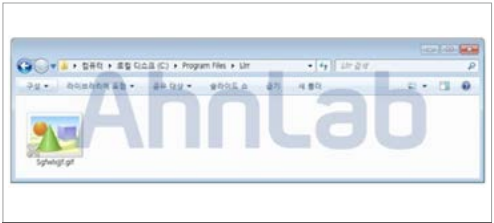


그림 2-7 | .gif 파일로 위장한 악성 DLL 파일

이후 악성 파일은 [표 2-5]와 같이 서비스 항목의 레지스트리를 변경하여, 해당 악성 파일이 자동 실행되도록 한다.

표 2-5 | 변경된 레지스트리

HKLM\SYSTEM\ControlSet001\Services\Team viewer\ImagePath
"%SystemRoot%\System32\svchost.exe -k imgsvc"
HKLM\SYSTEM\ControlSet001\Services\Team viewer\DisplayName
"Vdittd Smwactxm Wjwwamwk Bwjw"

분석 결과, Sgfwlxjjf.gif 파일은 악성 행위를 위해 정상 %system32%\svchost.exe 프로세스에 로드되어 지속적으로 네트워크 접속을 시도하는 것으로 확인됐다. 발견된 C&C 서버는 국내 CDN 서버이며, 분석 당시에는 통신이 이루어지지 않았다.

많은 사용자들이 PC방을 이용하는 만큼 더욱 철저한 보안 관리가 필요하다. 하지만 대부분의 PC방은 여전히 보안에 취약한 운영체제와 구 버전 웹 브라우저를 사용하고 있어 공격자들의 표적이 되고 있다. 따라서 정기적인 보안 점검을 시행하는 등 PC방에 설치된 악성코드로 인한 사용자의 피해가 발생하지 않도록 각별한 노력이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Redosdru (2016.07.22.00)
Trojan/Win32.PcClient (2016.07.22.00)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

01 바로가기 파일(.LNK) 형태로 위장한 랜섬웨어 등장

01 바로가기 파일(.LNK) 형태로 위장한 랜섬웨어 등장

랜섬웨어 위협이 연일 계속되고 있는 가운데, 최근 바로가기 파일(.LNK)의 확장자로 위장하여 유포되는 신종 랜섬웨어가 발견됐다. 윈도우의 바로가기 파일은 특정 파일의 대상 위치를 가지고 있는 파일로, 실행을 위해 매개 변수의 사용이 가능한 형태로 되어있다. 매개 변수에 특정 문자열을 추가해 의도한 동작을 수행하도록 할 수 있는데, 최근 이를 악용한 악성코드가 늘어나고 있다. 이번에 발견된 랜섬웨어 또한 이와 같은 바로가기 파일(.LNK)의 특성을 악용하고 있다.

그림 3-1 | 바로가기 파일의 매개 변수에 포함된 문자열

최근 발견된 랜섬웨어는 [그림 3-1]과 같이 바로가기 파일 형태로 유포되었으며, 명령 프롬프트(cmd.exe)에 자바스크립트(JavaScript) 소스를 입력하여 악성 스크립트를 실행한다. 해당 악성 스크립트가 실행되면 특정 URL로 연결하여 문자열 정보를 수신한다.

그림 3-2 | 수신된 문자열 정보

수신된 문자열 정보는 [그림 3-2]와 같으며, 자바스크립트 형태로 작성된 랜섬웨어 악성코드임을 알 수 있다. 해당 악성 스크립트 파일은 윈도우 응용 프로그램인 wscript.exe를 통해 실행된다.

최종적으로 악성 스크립트가 실행되면, 랜섬웨어는 사용자 파일을 암호화한 뒤 [그림 3-3]과 같은 감염 안내 메시지를 통해 돈을 지불해야 암호화된 파일을 복구시켜 준다는 내용을 사용자에게 보여준다.

그림 3-3 | 랜섬웨어 감염 안내 메시지

그림 3-4 | 난독화된 악성 스크립트

또한 다운로드된 악성 스크립트는 [그림 3-4]와 같이 분석을 어렵게 하도록 난독화되어 있으며, 암호화 라이브러리인 CryptoJS의 AES 알고리즘을 이용하여 파일을 암호화한다. 암호화 대상 파일의 확장자는 [표 3-1]과 같다.

표 3-1 | 암호화 대상 파일 확장자

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

지금까지 발견된 랜섬웨어는 *.js, *.vbs, *.wsf 형태의 악성 스크립트 파일이나 악성 매크로가 삽입된 문서 파일을 사용했지만, 이번에 발견된 랜섬웨어는 바로가기 파일(.LNK)의 취약점을 이용하여 악성 스크립트를 다운로드한 뒤 실행하는 것이 특징이다. 이는 곧 서버에 업로드된 해당 악성코드를 랜섬웨어가 아닌 다른 종류의 악성코드로 변경할 경우 시스템 유출 등의 추가적인 피해가 발생할 수 있다는 것을 의미하므로 주의해야 한다.

공격자들은 점점 다양한 방법을 통해 고도화된 랜섬웨어를 지속적하고 유포하고 있다. 랜섬웨어에 의한 피해를 방지하기 위해서는 보안 업데이트를 설치하여 드라이브-바이-다운로드(Drive-by-download) 공격을 방지하는 한편, 백신 프로그램의 엔진을 최신으로 유지하는 것이 필요하다. 또한 평소 중요한 파일은 별도로 백업해두는 것이 바람직하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

VBS/Raalocker (2016.07.07.04)

LNK/Downloader (2016.07.07.09)

AhnLab

ASEC REPORT

VOL.79
July, 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