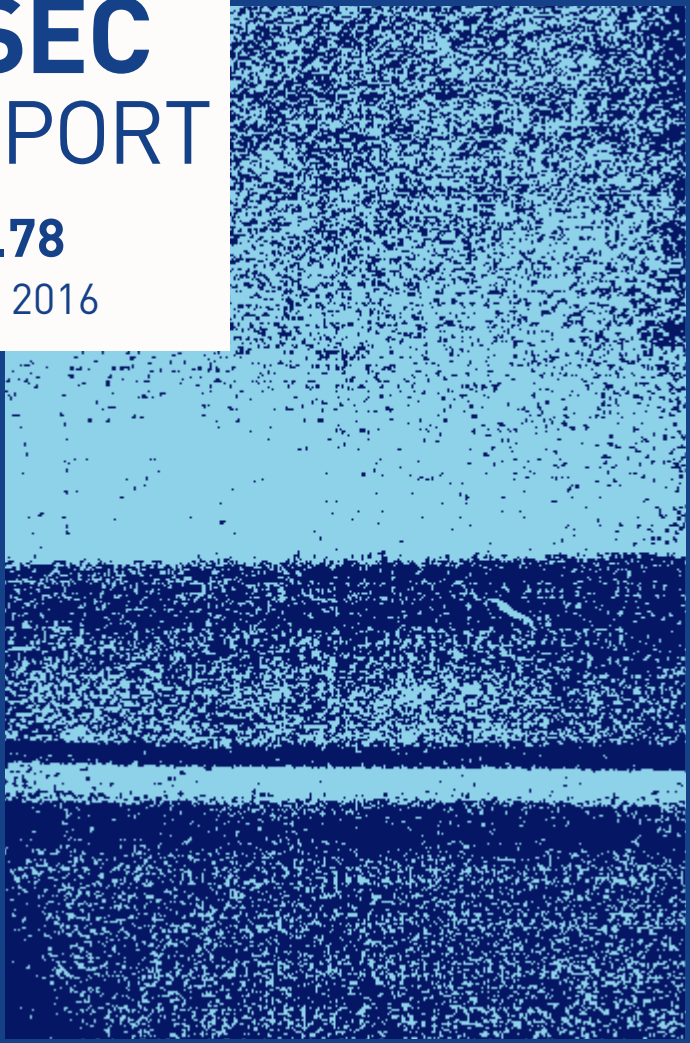
Security Trend

ASEC REPORT

VOL.78

June, 2016



AhnLab

ASEC REPORT

VOL.78 June, 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 6월 보안 동향

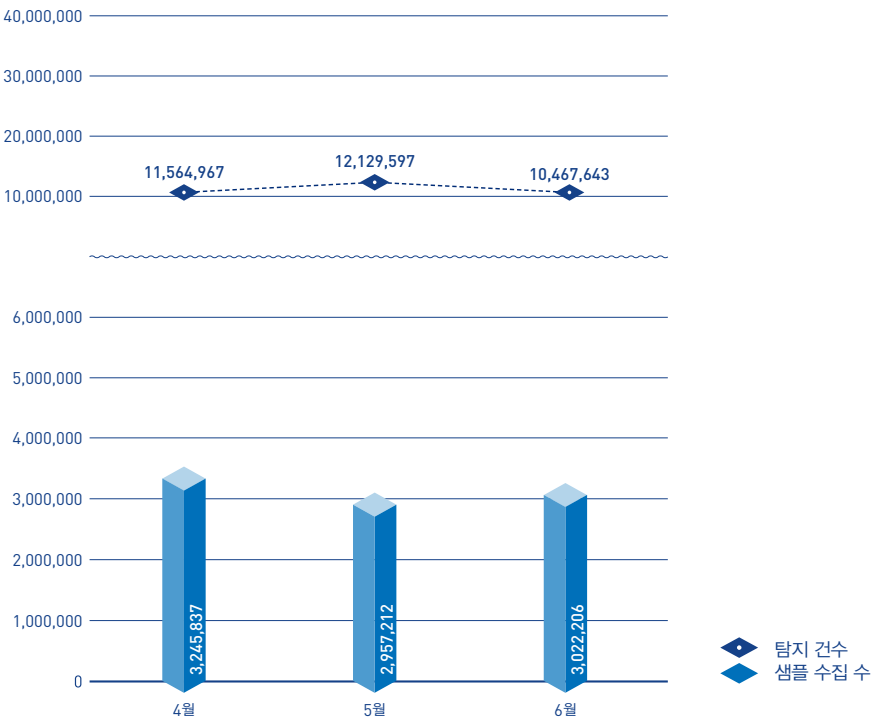
Table of Contents

1

보안 통계
STATISTICS

01 악성코드 통계

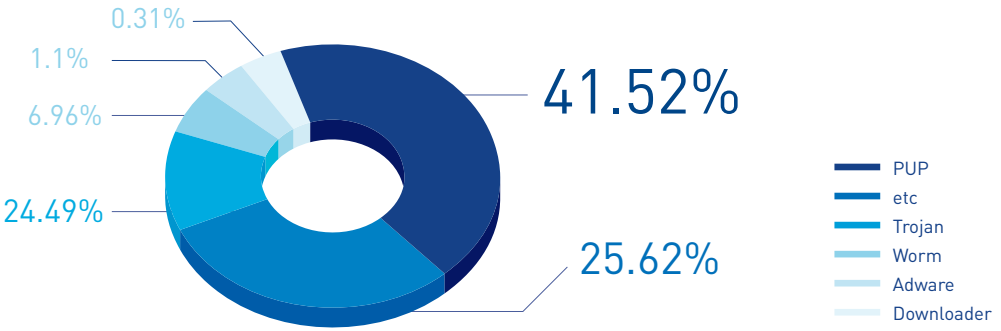
ASEC이 집계한 바에 따르면, 2016년 6월 한 달간 탐지된 악성코드 수는 1,046만 7,643건으로 나타났다. 이는 전월 1,212만 9,597건에 비해 166만 1,954건 감소한 수치다. 한편 6월에 수집된 악성코드 샘플 수는 302만 2,206건이다.



[그림 1-1] 악성코드 추이(2016년 4월 ~ 2016년 6월)

* '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 6월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 41.52%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 24.49%, 웜(Worm)이 6.96%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 6월 주요 악성코드 유형

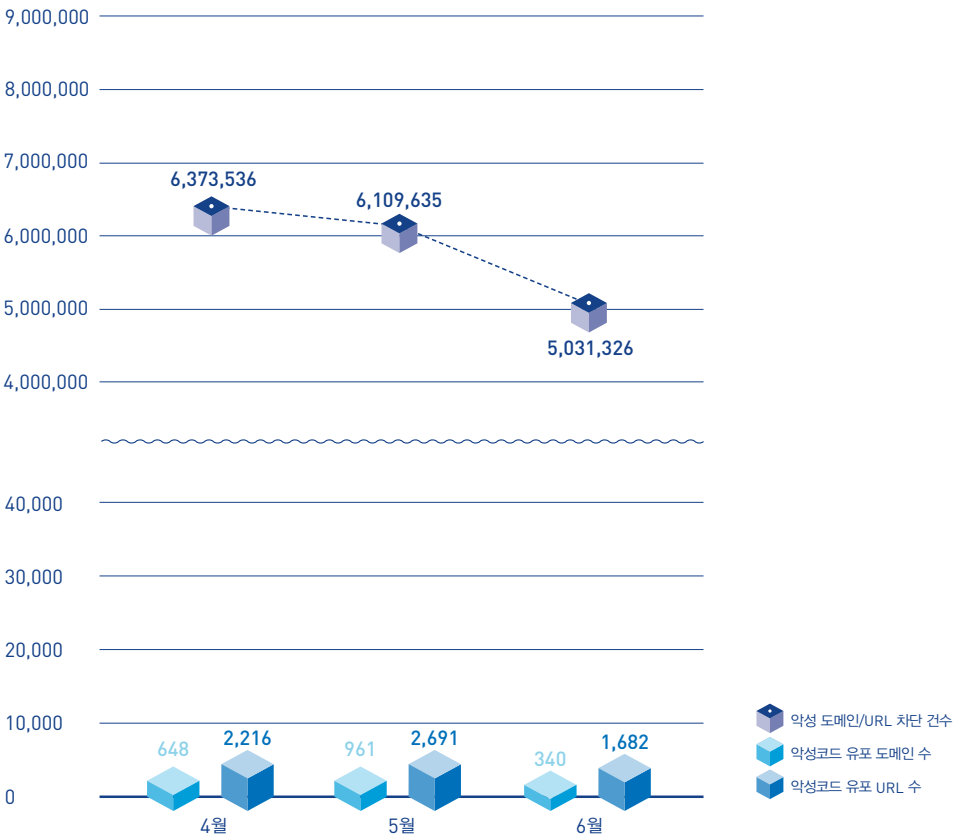
[표 1-1]은 6월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter가 총 21만 5,746건으로 가장 많이 탐지되었고, Malware/Win32.Generic 이 17만 2,381건으로 그 뒤를 이었다.

[표 1-1] 2016년 6월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	215,746
2	Malware/Win32.Generic	172,381
3	ASD.Prevention	128,266
4	Unwanted/Win32.HackTool	98,625
5	Trojan/Win32.Agent	73,884
6	Trojan/Win32.Neshta	68,886
7	Trojan/Win32.Banki	68,409
8	Trojan/Win32.CryptXXX	62,640
9	HackTool/Win32.Crack	61,036
10	Unwanted/Win32.Keygen	53,875

02
웹 통계

2016년 6월에 악성코드 유포지로 악용된 도메인은 340개, URL은 1,682개로 집계됐다([그림 1-3]). 또한 6월의 악성 도메인 및 URL 차단 건수는 총 503만 1,326건이다.

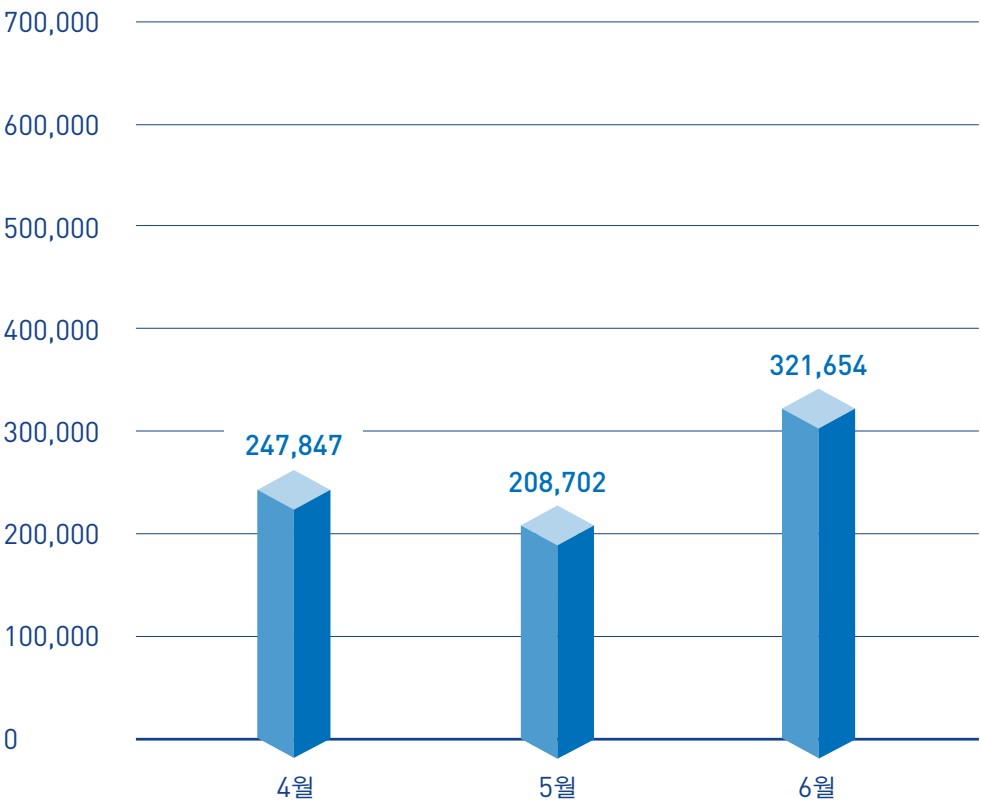


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 4월 ~ 2016년 6월)

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

03
모바일 통계

2016년 6월 한 달간 탐지된 모바일 악성코드는 32만 1,654건으로 나타났다([그림 1-4]).



[그림 1-4] 모바일 악성코드 추이(2016년 4월 ~ 2016년 6월)

[표 1-2]는 6월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 6월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	84,728
2	Android-PUP/Zdpay	20,401
3	Android-Trojan/Moavt	19,027
4	Android-PUP/Noico	18,709
5	Android-PUP/Skymobi	18,456
6	Android-PUP/SmsReg	17,203
7	Android-Trojan/Hidap	14,132
8	Android-PUP/Shedun	14,043
9	Android-Trojan/AutoSMS	11,429
10	Android-Trojan/Agent	10,030

2

보안 이슈
SECURITY ISSUE

01 크로스플랫폼(Cross-Platform) 애드웨어 등장

최근 ARM 아키텍처 기반 프로세서를 비롯해 iOS, 안드로이드(Android) 등 다양한 운영체제를 사용하는 추세에 따라 운영체제, 즉 플랫폼에 관계없이 동작하는 크로스플랫폼(Cross-Platform) 소프트웨어가 다수 개발되고 있다. 심지어 애드웨어(Adware)도 크로스플랫폼 형태로 등장했다.

최근 해외 보안업체 사이버리즌(Cybereason)이 발견한 피릿(Pirrit) 애드웨어는 크로스플랫폼 프레임워크를 이용해 개발됐다. 기존의 피릿 애드웨어는 윈도우(Windows) 운영체제에서 동작하며, 2014년 처음 발견된 후 지속적으로 나타나고 있다. 다양한 프로그램에 포함되어 함께 설치되며, 웹 브라우저의 프록시 설정을 변경하고 사용자가 웹 서핑을 할 때 [그림 2-1]과 같이 광고 팝업창을 보여준다.

그림 2-1 | 윈도우 기반의 피릿(Pirrit) 애드웨어(*출처: Microsoft.com)

이번에 발견된 맥(Mac) 운영체제용 OS X 피릿 애드웨어도 다양한 유틸리티 프로그램에 포함되어 유포된 것으로 추정되며, [그림 2-2] 와 같이 크로스플랫폼 개발 프레임워크인 Qt를 이용하여 제작되었다.

그림 2-2 | Qt 4 크로스플랫폼 개발 프레임워크 사용

애드웨어에 포함된 문자열을 확인한 결과, OS X에서 실행되는 애드웨어임에도 불구하고 [그림 2-3]과 같이 윈도우 레지스트리 키(Windows Registry Key) 값을 포함하고 있다.

그림 2-3 | 피릿 애드웨어 문자열에 포함된 윈도우 레지스트리 키 값

해당 악성코드가 프록시 설정 변경을 시도한다는 점은 기존의 윈도우용 피릿 애드웨어와 동일하지만, 시스템 내의 http 트래픽을 라우팅하기 위해 http 프

록시 서버(Proxy server)를 9882 포트로 실행하는 등 방식에는 차이가 있다.

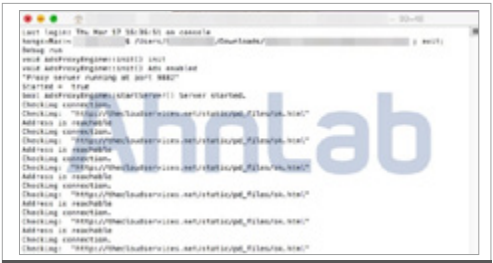


그림 2-4 | 프록시 서버(Proxy server) 동작

다양한 디바이스와 운영체제를 이용하는 사용자들이 늘어나면서 보안의 범위 또한 넓어지고 있다. 여전히 맥(Mac) 운영체제가 윈도우(Windows) 운영체제에 비해 안전하다는 인식이 남아있지만, 최근 발견되는 맥 악성코드를 살펴보면 윈도우 악성코드에 비해 유포 수만 적을 뿐, 기능과 방식 모두 유사하다. 또한 오픈 소스와 크로스플랫폼 개발 프레임워크가 발전함에 따라 윈도우 외의 다른 플랫폼을 노리는 악성코드 수가 점점 증가하고 있는 추세다. 따라서 윈도우 운영체제 외에 맥 등 다른 운영체제를 사용하는 경우에도 프로그램 설치 시, 또는 스팸 메일에 포함된 첨부 파일 실행 시 악성코드 감염에 대한 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

OSX64-Adware/DLNow.141732
(2016.06.03.00)
OSX64-Adware/Pirrit.414196
(2016.06.03.00)

02 최신 영화 파일로 위장한 RAT 악성코드 발견

토렌트를 통해 꾸준히 악성코드를 유포하는 공격자들은 시종일관 동일한 수법을 이용한다. 아이콘과 확장자를 동영상 파일처럼 보이도록 변경하고, 최신 영화나 드라마로 위장하여 사용자를 유인하는 것이다. 최근 발견된 RAT 악성코드도 최신 개봉 영화의 동영상 파일로 위장하여 유포되고 있어 사용자들의 각별한 주의를 요한다.

그림 2-5 | 동영상 파일로 위장한 악성코드

해당 RAT 악성코드는 [그림 2-5]와 같이 겉으로 보기엔 동영상 파일처럼 보인다. 그러나 폴더 옵션 내 보기 탭에서 [알려진 파일 형식의 파일 확장명 숨기기]를 비활성화하면, 해당 파일의 확장자가 화면보호기의 확장자인 .scr로 확인된다. 즉, 이 파일은 동영상이 아닌 악성 PE 파일임을 알 수 있다.

그림 2-6 | XtremeRAT 뮤텍스 생성

또한 중복 실행 방지를 위한 뮤텍스(Mutex) 생성 시 'XtremeRAT'라는 문자열이 존재하는 것으로 보아 해당 악성코드는 과거부터 지속적으로 유포되는 Xtreme RAT인 것을 알 수 있다. RAT(Remote Administration Tool) 악성코드는 감염 시스템을 원격으로 조종하며 주로 클립보드, 시스템 내 데이터 등을 유출하는 키로깅 기능을 갖고 있다.

해당 악성코드는 윈도우(Windows)의 정상 프로세스인 svchost.exe와 iexplore.exe(또는 chrome.exe)를 생성한 뒤 CreateRemoteThread()를 통해 인젝션된다.

표 2-1 | 레지스트리 등록 값

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HKLM	"C:\WINDOWS\InstallDir\win31.exe"
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\HKCU	"C:\WINDOWS\InstallDir\win31.exe"

이후 이 악성코드는 'C:\WINDOWS\InstallDir\win31.exe' 경로에 자가복제하여 [표 2-1]과 같은 레지스트리 등록을 통해 시스템 시작 시 자동 실행되도록 한다.

'C:\DOCUME~1\[사용자계정]\Application Data\Microsoft\Windows' 경로에 추가 생성되는 '--((Mutex))--.dat' 파일은 Single Byte XOR(Key : 0x33)로 암호화되어 있으며, 키로깅(key-logging)한 클립보드 데이터가 저장된다.

그림 2-7 | HTML 형식으로 저장되는 데이터

사용자 시스템에서 탈취된 정보는 [그림 2-7]과 같이 HTML 형식으로 저장되어 공격자 서버로 전송되는 것으로 추정된다. 악성코드는 시스템 데이터 탈취 이외에도 프로세스 제어, 화면 캡처 등의 악성 행위를 수행한다.

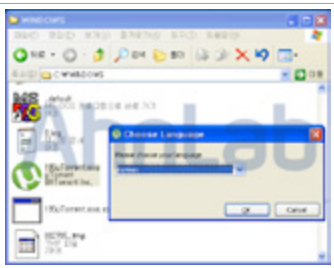


그림 2-8 | 정상 토렌트 설치 파일 실행

시스템을 장악한 악성코드는 사용자가 감염 사실을 인지하지 못하도록 [그림 2-8]과 같이 'C:\WINDOWS' 경로에 정상 토렌트 설치 파일을 생성한 뒤 이를 실행한다.

토렌트를 통해 공유되는 영화나 드라마 파일을 이용해 악성코드를 유포하는 사례는 꾸준히 발견되고 있다. 구체적인 방법으로는 다운로드 파일 중 일부에 악성코드를 첨부하고 정상 파일로 위장하는 등 여러 가지가 있다. 사용자는 토렌트를 통해 파일을 다운로드 할 때 폴더에 있는 파일 전체를 의심 없이 내려 받는 경우가 많은데, 여기에 포함된 악성코드가 사용자의 컴퓨터에서 악성 행위를 하게 되는 것이다. 이 밖에도 저작권 침해 우려가 있는 만큼, 토렌트 이용에 대한 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Injector (2016.06.19.03)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

웹 사이트 광고에 숨은 랜섬웨어 주의

웹 사이트 광고에 숨은 랜섬웨어 주의

2016년이 반환점을 지났지만, 사용자의 파일을 인질로 삼아 비용을 요구하는 랜섬웨어 공격은 여전히 계속되고 있다. 랜섬웨어 공격은 보통 스팸 메일과 멀버타이징 기법을 통해 이루어진다. 스팸 메일을 통한 유포 방법은 공격자가 불특정 다수의 사용자에게 스크립트로 된 첨부 파일을 포함한 메일을 전송한 뒤, 사용자가 이 첨부 파일을 실행하면 랜섬웨어에 감염되는 방식이다. 멀버타이징(Malvertising) 기법은 웹 사이트에 삽입되는 광고를 이용하여 랜섬웨어를 유포하는 방식이다.

악성코드(Malware)와 광고(Advertising)의 합성어인 멀버타이징(Malvertising) 기법은 스팸 메일을 이용한 랜섬웨어 유포 방법보다 파급 효과가 훨씬 크다. 웹 사이트 광고 특성상 하나의 광고 서버에서 여러 웹 사이트로 광고를 전송하고, 짧은 시간 동안 다수의 사용자에게 노출되기 때문이다. 이러한 이유로 사용자는 의심 파일을 다운로드하거나 실행한 적이 없음에도 불구하고 랜섬웨어에 감염될 수 있다. 이와 같은 피해 사례가 지속적으로 증가하고 있는 만큼, 멀버타이징 기법에 대해 좀 더 자세히 알아보도록 하자.

그림 3-1 | 멀버타이징(Malvertising) 개념도

광고 서버는 웹 사이트의 광고 영역에 사전에 제작된 광고를 전송하는 역할을 한다. [그림 3-1]과 같이 멀버타이징 기법을 이용하는 공격자는 공격하고자 하는 광고 서버에 악성코드 유포 도구(Exploit Kit)와 정상적인 광고를 전송한다. 사용자가 광고가 포함된 웹 페이지 방문 시, 광고 서버는 정상적인 광고에 악성코드 유포 도구(Exploit Kit)를 포함하여 웹 페이지에 전송한다. 이렇게 전달된 웹 페이지가 사용자의 웹 브라우저에서 실행되면, 보안 취약점을 이용한 드라이브-바이-다운로드(Drive-by-download) 방식을 이용하여 사용자의 시스템을 감염시킨다.

그림 3-2 | 웹 사이트에 포함된 인터넷 광고

[그림 3-3]은 멀버타이징 공격 시 수집된 네트워크 정보다. 여기서 사이트 'www.livead*********.com'은 웹 페이지에 광고를 제공하는 광고 서버다.

그림 3-3 | 멀버타이징(Malvertising) 네트워크 정보

광고 서버는 사용자의 웹 브라우저에서 요청 받은 광고 페이지를 전송한다. 이때 전송된 페이지에는 사이트 'tom****.com'과 더불어 악성코드 유포지인 '108.**.***.63'이 포함되어 있다.

표 3-1 | 전송 받은 광고 페이지 정보

[www.livead*********.com/a/display.php]

```
<html>
<head>
<title></title>
   <link rel="dns-prefetch"
href="http:\/\/tom****.com\/************************
**************trackurl.php
... 생략 ...
```

[표 3-1]에서 확인할 수 있는 바와 같이 전송된 광고 페이지 내부는 'tom****.com' 사이트로 연결되도록 작성되어 있다.

표 3-2 | tom****.com 페이지 정보

[tom****.com.../trackurl.php]

```
<html>
<head>
<script type="text/javascript"
src="http://108.**.***.63/"></script>
<meta http-equiv="refresh" content="8;http://www.
tom***.com/********************">
</head>
</html>
```

또한 [표 3-2]와 같이 연결된 'tom****.com' 사이트는 악성코드 유포지인 '108.**.***.63'으로 연결되도록 작성되어 있다.

표 3-3 | vnunfse.**********.top 페이지 정보

[vnunfse.**********.top]

```
<html>
<body>
... 생략 ...
   <param name="bgcolor" value="#ffffff"/>
   <param value="always" name="allowScriptAccess"/>
   <embed src="/*****************/likewise-
**************-granny-pale-cottage.swf"
...생략... width="533" allowScriptAccess="sameDomain"
quality="high" height="120" loop="false"/>
</object>
</body>
</html>
```

마지막으로, [표 3-3]과 같이 최종 연결되는 페이지에서 플래시 파일이 실행되어 드라이브-바이-다운로드(Drive-by-download) 방식으로 랜섬웨어가 실행된다. 랜섬웨어가 사용자 PC 내에 주요 파일을 암호화한 후에는 [그림 3-4]와 같이 랜섬웨어 감염 안내 메시지가 출력된다.

그림 3-4 | 랜섬웨어 감염 안내 메시지

최근 랜섬웨어 공격의 범위가 점점 확대되고 있다. 랜

섬웨어 감염으로 인한 피해를 예방하기 위해서는 백신 프로그램을 설치하고, 엔진을 최신 버전으로 유지해야 한다. 또 운영체제, 웹 브라우저 및 주요 애플리케이션에 최신 보안 업데이트를 적용해야 한다. 발신자가 명확하지 않은 이메일에 첨부된 의심스러운 파일의 실행을 자제하고, 보안이 취약한 웹사이트는 방문하지 않는 것이 좋다. 업무 및 기밀 문서, 각종 이미지 등 주요 파일은 주기적으로 백업하되 특히 중요 파일들은 PC 외의 외부 저장 장치를 이용해 2차 백업을 해두는 것이 바람직하다.

V3 제품에서는 해당 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Win-Trojan/CryptXXX.Gen

AhnLab

ASEC REPORT VOL.78 June, 2016

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