Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.213

인터넷 광고 인젝션 유형에 대한 연구*

조 상 현,[1†] 최 현 상,[1] 김 영 갑[2‡]
[1]네이버, [2]세종대학교

A Study on Internet Advertisement Injection*

Sanghyun Cho,[1†] Hyunsang Choi,[1] Young-Gab Kim[2‡]
[1]Naver Corporation, [2]Sejong University

요 약

인터넷 광고는 오프라인 광고에 비해 여러 장점을 가지고 있지만, 광고 인젝션(advertisement injection)으로 인하여 다양한 피해가 발생할 수 있다. 일반사용자에게는 추가 적인 광고 노출로 인하여 불편함을 주고, 웹 콘텐츠 제공자에게는 서비스 품질 저하의 문제를 발생시킬 수 있다. 또한 광고주에게는 계획되지 않는 광고 노출로 인하여 기대한 광고 효과를 얻지 못하기도 한다. 하지만, 이와 같은 인터넷 광고 인젝션으로 인한 피해가 발생 가능함에도 불구하고 아직까지 광고 인젝션 유형에 관한 연구는 거의 진행되지 않았으며, 다만 구글(Google)의 최근 연구에서 인터넷 광고 인젝션 이슈를 다루고 있다. 따라서 본 논문에서는 국내 인터넷 포털 사이트 네이버를 대상으로 한 인터넷 광고 인젝션 유형을 분석하였다. 다운로더 27개와 이들이 설치하는 199개의 프로그램을 분석하여, 여섯 개의 인젝션 유형을 정의하고 각 유형별 동작 및 특징을 분석하였다.

ABSTRACT

Online advertisement has many benefits comparing to offline advertisement but it also has many challenging problems by online ad abuses. Advertisement injection (Ad injection) is one of the threats that surreptitiously inserts advertisements without a permission of site owners. Users are exposed to additional ads and redundant web traffic by injected ads can cause a service quality problem. Moreover, advertisers can have economic loss when injected ads are different from original ones. Although ad injection leads to these problems it has not been fully studied yet. A few ad injection researches are done by online advertising providers such as Google. In this paper, we analyze ad injection activities to Korean major portal, Naver. We classify 6 types of ad injections and describe their characteristics by analyzing 27 downloaders and 199 installed programs.

Keywords: Internet advertisement, ad injection, abusing

I. 서 론

인터넷 광고는 오프라인 광고에 비해 몇 가지 장점을 가진다. 소비자와의 직접적인 상호 작용이 가능하고 특정 수요층을 대상으로 광고 노출이 가능하다. 또한 기존 매체(TV, 신문, 라이오, 잡지 등)에 비해 상대적으로 광고비용이 저렴하고, 광고 노출과 동시에 소비자의 제품 구매를 유도하기도 한다[1]. 인터넷 광고의 일반적 형태는 검색엔진을 포함하여 네이버와 같은 웹 콘텐츠 제공자 사이트에서부터 광고주의 사이트로 하이퍼링크(hyperlink)나, 배너(banner) 광고 이미지를 클릭하여 이동 시킬 수 있도록 하고 그 대가를 지불한다. 하지만, 광고 인젝션(advertisement injection: ad injection)으로

Received(01. 10. 2017), Modified(03. 30. 2017), Accepted(04. 07. 2017)
* 본 연구는 NAVER 주식회사로부터 지원되었습니다.
† 주저자, super.bg@navercorp.com
‡ 교신저자, alwaysgabi@sejong.ac.kr (Corresponding author)

인하여 원래의 광고가 출력되지 않고, 엉뚱한 광고 링크나, 배너 광고가 노출되어, 실질적으로 해당 웹 콘텐츠 게시자의 광고 수익을 잃게 하거나, 노출되어야 할 광고주의 광고 링크가 노출되지 않는 문제가 생겨날 수 있다.

인터넷 광고 인젝션은 인젝션 프로그램 유포과정에서도 일반적인 프로그램 형태가 아니라, 다른 프로그램에 기생하거나, 이용자 모르게 설치되는 경향이 많다. 이렇게 설치된 프로그램은 특정 검색 엔진에서 입력한 키워드에 반응하여, 준비된 광고를 추가적으로 노출함으로써 이용자에게 불편함이 생기며, 웹 콘텐츠 제공자 입장에서는 품질 문제로 이어질 수 있다. 광고주 입장에서는 특정 웹 콘텐츠 제공자에게 광고비를 지불했으나, 자신의 사이트로 인입되는 트래픽이 없거나, 반대로 원하지 않는 사이트에 자신의 광고가 노출되어, 실제 기대한 대로 매출 향상으로 이어지지 않을 수 있다. 이렇게 인터넷 광고 인젝션으로 인한 피해가 발생함에도 불구하고, 현재까지도 광고 인젝션 유형에 대한 분류 및 특성에 관한 연구는 거의 없으며, 다만 구글(Google)의 최근 연구 [2]에서 인터넷 광고 인젝션 이슈를 다룬바 있다. 따라서 본 논문에서는 국내 인터넷 포털 사이트 네이버를 대상으로 한 인터넷 광고 인젝션 유형을 분석하고, 특히 다운로더(downloader)라고 불리는 프로그램들이 얼마나 많은 광고 인젝션 프로그램을 유포하고 있는지 확인하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 인터넷 광고 인젝션 관련 기존 연구들에 대해 기술한고 Ⅲ장에서는 광고 인젝션을 유형을 분석하기 위한 방법을 제시한다. Ⅳ장에서는 네이버(Naver)[1]를 대상으로 한 인터넷 광고 인젝션의 유형에 대해 분석하고, 각 유형에 대하여 다각적으로 분석하고 의미해석을 수행한다. Ⅴ장에서는 인터넷 광고 인젝션의 대응방안 및 시사점에 대해 논의하고, Ⅴ장에서는 결론 및 향후 연구해야 할 사항에 대해 기술한다.

Ⅱ. 관련 연구

논문의 온라인 서비스에서의 어뷰징(abusing)은 오래전부터 많은 연구가 진행되어 왔다. 대표적으로 부정클릭 어뷰징(click fraud abusing)에 대하여 10여 년 전부터 많은 연구가 진행되어 왔다. [3]에서는 봇넷(botnet)의 일종인 클릭봇(clickbot)을 이용한 부정클릭 어뷰징 기술 중 최신 기술들에 대한 내용을 기술되어 있다. 2014년에는 전 세계 900만대 이상의 PC를 감염시킨 ZeroAccess 봇넷의 부정클릭 어뷰징에 대한 연구논문이 발표되었다[4]. 온라인 광고를 이용해 악성코드 감염에 이용이 되는 경우도 있는데 Alexa[2]에 랭크된 상위 9만개 웹사이트들 중에서 약 1%의 웹페이지들이 악성코드 감염과 관련된 온라인 광고를 포함하는 것으로 연구되었다[5].

2000년대 후반에는 ISP가 사용자의 데이터를 변조하거나 프록싱(proxing)한다는 사실이 알려지기 시작했다. ISP가 사용자의 웹 트래픽에 데이터를 변조하는 데에는 여러 가지 목적이 있는데 유해사이트의 접속을 막기 위해서나 혹은 정부차원에서 특정 웹사이트의 접속을 막는 경우도 있다. 최근에 ISP가 사용자의 웹 트래픽을 변조하는 주된 목적은 광고 데이터 삽입을 위해서다[6]. Gabi[6]의 연구에 따르면 ISP 트래픽 인젝션을 수행하는 대부분은 중국의 ISP들이었는데 이들 중 에서는 심지어 악성코드를 인젝션 하는 경우도 있었다. 네트워크 트래픽 데이터에 광고 데이터를 인젝션 할 때 ISP들은 주로 인젝션한 데이터를 원본데이터보다 먼저 사용자에게 도착하게 하는 방법을 이용하였는데, 이런 경우 사용자의 요청에 대해 웹페이지 응답이 중복되어 도착하게 된다. 논문에서는 여러 웹사이트를 돌아다니면서 중복된 응답받았는데 데이터가 다른 경우를 찾아내는 방식으로 온라인 광고 인젝션을 탐지하였다.

Muhammad[7]의 논문은 온라인 광고 어뷰징과 관련된 연구논문은 아니었으나 온라인 광고의 에코시스템(ecosystem)의 체인(chain)을 밝히는 연구이다. 온라인 광고 어뷰징은 사용자 레벨에서도 발생하는데, 본 논문에서 언급한 바와 같이 악성코드에 감염되어 웹 트래픽에 광고가 인젝션 되는 경우도 있고 또한 악성 브라우저 익스텐션(extension)에 의해서도 광고가 인젝션 되기도 한다. [8]에서는 악성 브라우저 익스텐션을 탐지하는 기술을 개발하였다. 악성 브라우저 익스텐션은 광고 인젝션 뿐만 아니라 검색 키워드 하이재킹(hijacking)이나 사용자 트래킹(tracking)과 같은 악성행위도 수행한다.

구글의 Kurt Thomas[9]의 연구에서는 웹페이지 컨텐츠가 수정되었는지를 서버 레벨에서 확인할

1) http://www.naver.com

2) http://www.alexa.com/topsites

수 있도록 자바스크립트를 이용하였으며 (웹페이의 컨텐츠가 수정되는 경우 서버에 알림) 인젝션된 데이터가 이진 데이터인 경우 'Google safe browsing'을 이용해 광고 인젝션을 수행하는 바이너리를 탐지하였다. 인젝션된 데이터가 브라우저 익스텐션인 경우 구글이 내부적으로 사용하고 있는 크롬 익스텐션 검수 시스템인 'WebEval'과 악성 브라우저 익스텐션 탐지 기능이 있는 'Hulk'를 이용하여 광고 인젝션을 수행하는 브라우저 익스텐션을 탐지하였다. 이 논문에서는 이와 같은 탐지 시스템들을 이용하여 실제로 광고 인젝션에 대한 데이터 분석을 수행하였는데 구글의 웹사이트에 접속하는 IP들 중에 약 5%의 IP에서 광고 인젝션이 발생하였다고 한다. 구글 연구[2]에 의하면, 5만개의 브라우저 익스텐션과 34,000개의 애플리케이션이 사용자의 브라우저를 제어할 수 있고 광고 인젝션이 가능한 사실을 발견했으며, 이 중 30% 이상은 명백히 악성적이고, 계정 정보 수집, 검색 쿼리(query) 하이재킹, 이용자 행위를 제3자에게 제공하고 있다. 특히 윈도우의 5.1%, Mac의 3.4%의 페이지 뷰(page view)는 광고 인젝션 프로그램이 설치되었음 보여줬다.

국내에서는 온라인 서비스 어뷰징과 관련해서 몇 가지의 연구가 진행되었는데 대부분은 부정클릭과 관련된 연구이고 광고 인젝션과 관련해서는 거의 연구가 진행되지 않았다. 이는 광고 인젝션에 대한 피해는 온라인 광고를 메인으로 하는 대형 온라인 포털 사이트를 제외하고는 관심의 대상이 아니었으며, 광고주는 직접적인 피해를 인지하지 못하는 경우가 일반적이었다. 또한 간접적인 피해를 입는 사용자의 경우도, 포털 사이트에서 제공하는 광고로 오인하여 불만을 갖지, 자신의 PC에 인젝션 프로그램이 어떻게 설치되어 무슨 일을 하는지 모르는 경우가 대부분이었다. 따라서 본 연구에서는 대형 온라인 포털 사이트인 네이버를 대상으로 한 온라인 광고 인젝션의 유형을 분석하고, 각 인젝션 유형의 특성을 분석함으로써 국내에서 크게 주목받지 못했으나, 서비스의 위협적이며 그 유포 방법이 좀비PC를 확보하려는 행위와 크게 다르지 않음에 주목하여, 대응에 기여하고자 한다.

III. 인터넷 광고 인젝션 분석 기법

본 장에서는 본 논문에서 제시하는 광고 인젝션 유형을 도출하기 위한 분석 기법에 대해 기술한다. 인터넷 광고 인젝션은 유형에 따라 대응 방법과 위험도가 상이한데, 광고 인젝션은 Fig.1.에서와 같이 BHO(Browser Helper Object)기준으로 Sidebar(1), Toolbar(2), DOM(Document Object Model)(3) 추가형태로 온라인 컨텐츠 제공자 사이트에서 인젝션이 발생하거나, 2차 사이트에서 Sidebar나 Toolbar가 나타나는 형태가 있다 (여기서, 2차 사이트는 네이버의 검색 광고를 클릭하여 이동하는 광고주 사이트를 의미한다).

광고 인젝션 프로그램의 주요 설치 경로는 다음과 같다.: 1) 인터넷 검색을 통해 특정 프로그램을 다운로드 받으려고 할 때, 함께 설치되거나, 2) 웹하드(P2P)의 다운로더 프로그램과 동반 설치되거나, 3) 웹하드(P2P)에 있는 무료 유틸리티나, 동영상등의 컨텐츠와 함께 다운로드 되거나, 4) 동영상 재생 시 필요한 플레이어인 것처럼 위장하여 설치되기도 한다. 5) 또한, 무료 게임 사이트에서 게임 재생을 위해 필요한 프로그램인 것처럼 설치되거나, 6) 브라우저 익스텐션(browser extension)을 통해 그 동작이 일어난다. 특히 초기 설치 시에는 포함되어 있지 않지만 업데이트 과정을 통해 인젝션 프로그램이 추가되는 경우가 많다.

본 연구에서는 광고 인젝션 프로그램 분석을 위해, 광고 인젝션 프로그램의 배포 경로와 행위 확인을 위한 수집, 분석을 진행하였다. 앞서 언급한 광고 인젝션 프로그램의 여러 설치 경로 중, 인터넷 검색을 통해 특정 프로그램을 다운로드 받으려고 할 때 '다운로더' 라는 프로그램과 함께 설치되는 형태에 대해 살펴본다. 이 경로의 선정 이유는, 짧은 시간에 가장 많은 광고 인젝션 프로그램을 설치할 수 있으며, 가장 흔히 이용되는 방식이기 때문이다. 다운로

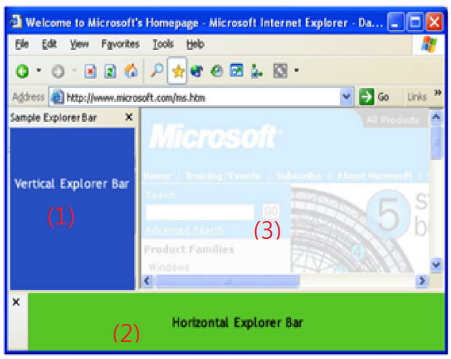

Fig. 1. Ad-injection area

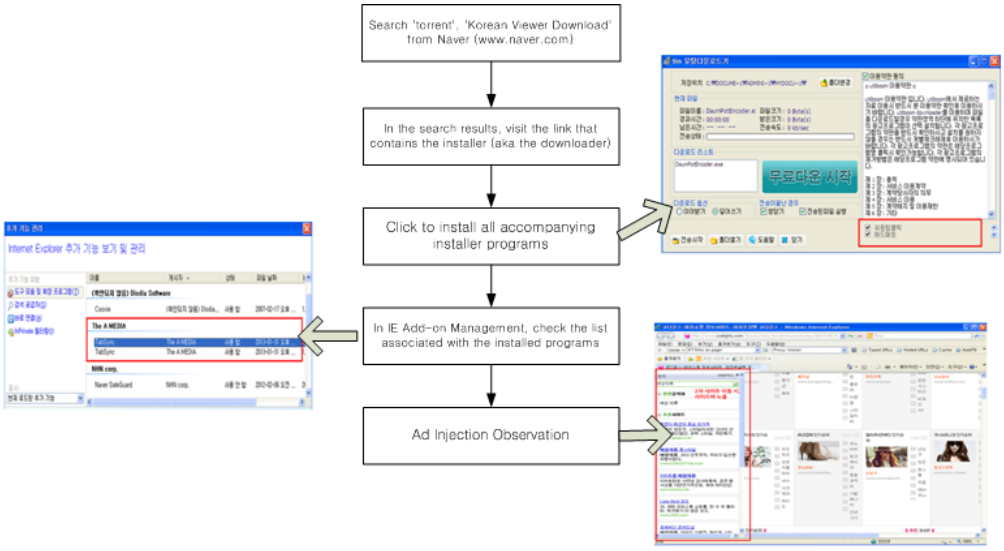

Fig. 2. Ad-injection analysis method

더는 이용자가 원하는 프로그램 외에 광고 인젝션 기능을 가진 다수의 프로그램(흔히 스폰서 프로그램이라고 불림)을 설치하게 한다. 본 연구에서는, 2012년 11월부터 12월까지 다운로더 27개와 이들이 설치하는 199개의 프로그램을 분석하였다.

분석 방법은 프로그램들을 설치한 후, 인터넷 익스플로러(IE) BHO인지 확인하고, 인터넷 포털 사이트 네이버에서 주요 키워드 입력 후 검색 광고주 사이트로 이동할 때 광고 인젝션이 발생하는지 살펴보았다. 이와 관련된 분석 방법을 순서도로 나타내면 Fig.2.와 같다.

IV. 인터넷 광고 인젝션의 유형 및 분석

4.1 인터넷 광고 인젝션 유형

앞서 기술한 인터넷 광고 인젝션 분석 기법을 통하여 여섯 개의 광고 인젝션 유형을 발견하였으며, 각 유형의 종류 및 특성은 다음과 같다.

(Ad-injection Type-Ⅰ) 네이버 통합 검색 시, 입력한 키워드와 관련 있는 광고 팝업창을 출력:

Fig. 3.에서와 같이, '청바지'라는 키워드를 입력하였더니 "HalfTong"이라는 사이트가 팝업으로 출력되면서 기존 검색 결과를 가리고 있다.

Table 1의 URI (Uniform Resource Identifier) 정보를 이용하여 보다 자세히 살펴보면, 실제 설치된 프로그램은 청바지(%EC%B2%AD...)라는 키워드와 네이버 검색(search.naver.com)에서 얻은 데이터를 "clickpang.co.kr" 광고대행사 사이트로 전달한다(Table 1-No-1). "clickpang.co.kr"에서 사용자의 웹 브라우저로 하여금 "click.interich.com"로 "halftong"이라는 데이터를 전달하게 하며(Table 1-No-2), "click.interich.com"은 최종적으로 "halftong.com"으로 이동하게 한다(Table 1-No-3). 이 과정에서 웹 서버의 응답은 '302 Object moved(HTTP redirect)'였다.

(Ad-injection Type-Ⅱ) 네이버 통합 검색 시, 현재 브라우저 화면 상단에 광고 툴바 생성:

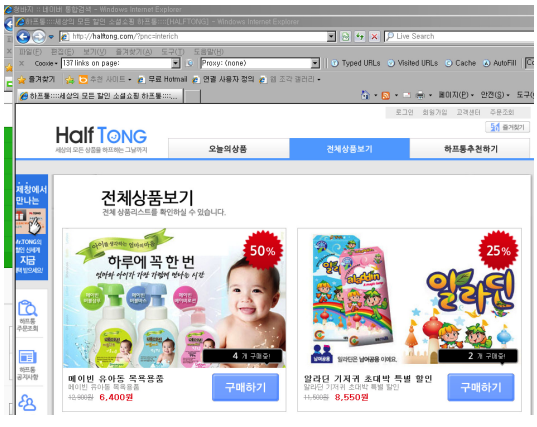

Fig. 3. Search term related advertisement pop-up

Table 1. Ad-Injection Type-Ⅰ URIs

No	URI
1	http://clickpang.co.kr/c/link.php?q=%EC%B2%AD%EB%B0%94%EC%A7%80&d=search.naver.com&ad_id=210&ad_type=1&url=aHR0cDovL2NsaWNrLmludGVyaWNoLmNvbT9hX2lkPXRlZXBpdSZhX251bT0xJm1faWQ9aGFsZnRvbmcmbV9udW09MTk2NDk5
2	http://click.interich.com?a_id=teepiu&a_num=1&m_id=halftong&m_num=196499
3	http://halftong.com/interich/Interclickfront.php?redirect_site=http%3A%2F%2Fhalftong%2Ecom%2F%3Fpnc%3Dinterich&m_id=halftong&m_num=196499&cookie_date=7&a_id=teepiu&a_num=1&r_1=&r_2=

Fig. 4.에서와 같이 '아이라이너'라는 키워드를 검색했을 때, 브라우저 상단에 광고 툴바가 생성된다.

Table 2의 URI 정보를 분석하면, 광고 인젝션 프로그램 UtilZone.dll은 키워드(%EC%95...), 이용자 PC의 MAC Address(000C...), 검색엔진(search.naver.com), IE 버전 정보를 "utilz.net"에 전달하고 있다. 결과적으로 Fig. 4.의 빨간색 부분과 같이 상단에 툴바가 출력된다.

Fig. 4. Advertisement tool bar on browser

Table 2. Ad-Injection Type-Ⅱ URIs

No	URI
1	http://www.utilz.net/fd/?k=%EC%95%84%EC%9D%B4%EB%9D%BC%EC%9D%B4%EB%84%88&id=UZ114&mac=000C296EA022&dmn=search.naver.com&iev=8

(Ad-injection Type-Ⅲ) 통합 검색 시, 검색 결과 외에 추가 광고 탭 노출:

IE 브라우저에서 IWebBrowser2의 Navigate 메소드를 호출하여 새 탭을 생성하는 방법이 있는데 이를 이용하여 Fig. 5.에서 보이는 바와 같이 "http://c.winggo.co.kr/index8.php?b...I9MQ==" 탭을 만들고 iframe 태그 삽입을 통해 '시크폭스'라는 페이지가 로드되었다("<script type='text/Javascript'>location.href='http://www.chicfox.co.kr/?cm_id=pop11';</script>").

Table 3의 디코딩한 인자 부분에 MAC Address를 암호화한 것으로 추정되는 부분이 있다. 광고 인젝션 프로그램들은 공통적으로 정산을 위해 설치 PC의 MAC Address를 수집한다.

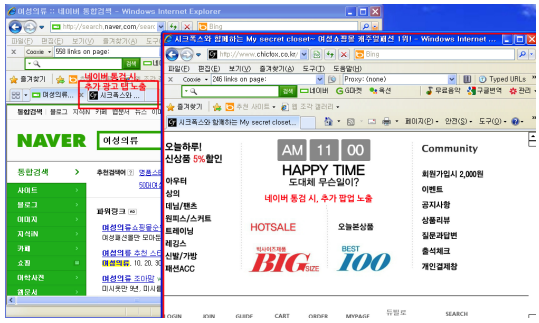

Fig. 5. Additional advertisement tab for ad-injection

Table 3. Ad-Injection Type-III

Parameter encoded with BASE64	Decoded Parameter
bUNvZGU9MTIzJmlDb2RlPSZhQ29kZT0xMjAyJmNDb2RlPTQzNzEmdUNvZGU9JmtDb2RlPTcyMzA5JnByaWNlPTIwJmFkVHlwZT0xJmFjVHlwZT0mYWNpZHg9Jm1hYz1NREF0TUVNdE1qa3RORGN0TUVZdE5ETSZ0YWI9MQ==	mCode=123&iCode=&aCode=1202&cCode=4371&uCode=&kCode=72309&price=20&adType=1&acType=&acidx=&mac=MDAtMEMtMjktNDctMEYtNDM&tab=1

(Ad-injection Type-Ⅳ) CPS[3] 검색 광고 클릭 시, 2차 사이트에서 사이드 바에 다른 검색 광고 노출:

3) Click Per Sales : 링크 클릭이 발생할 때마다 광고료가 차감되는 방식

네이버에서 '여성의류'를 클릭 결과 광고 클릭 중에 '코디걸스'를 클릭하여 사이트를 이동할 경우, Fig. 6.와 같이 사이트 좌측에 사이드바 영역에 다른 검색 광고가 출력된다.

Table 4의 URI 내용을 분석하면, 광고 인젝션 프로그램인 WinPro.dll은 이용자가 입력한 키워드인 여성의류(%EC%97..)와 Mac Address(000C...)를 "www.winpro.co.kr"으로 전달한다. 그 결과 좌측에 키워드 광고가 추가된다.

(Ad-injection Type-V) 사이트 이동 시, 해당 사이트에서 추가 광고 팝업창 출력

Fig. 7.에서는 네이버에서 '여성의류'를 검색하고 나온 결과 중에 3번째 링크를 클릭 했을 때의 결과이다. "joamom"이라는 사이트 출력되어야 하는데, 광고 인젝션 프로그램에 의해 "아뜨랑스", "SHOWROOM" 사이트가 추가적으로 출력되었다.

Table 5의 URI 정보를 살펴보면, 광고 인젝션 프로그램인 FreeListenManager.exe는 "ad.openmatch.co.kr"에 MAC Address와 검색엔진 정보를 전달하면(Table 5-No-1), 이동할 URI 정보를 수신 받게 된다(Table 5-No-2).

BASE64로 인코딩되어 있는 이 정보를 디코딩하면 "http%3A//attrangs.co.kr/%3Fcafe_mkt

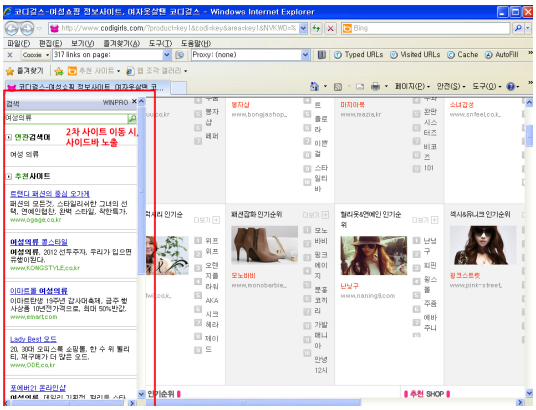

Fig. 6. Sidebar ad-injection of CPS advertisement click

Table 4. Ad-Injection Type-Ⅳ URIs

No	URI
1	http://www.winpro.co.kr/fd/?k=%EC%97%AC%EC%84%B1%EC%9D%98%EB%A5%98&id=WP37&m=000C29470F43 HTTP/1.1

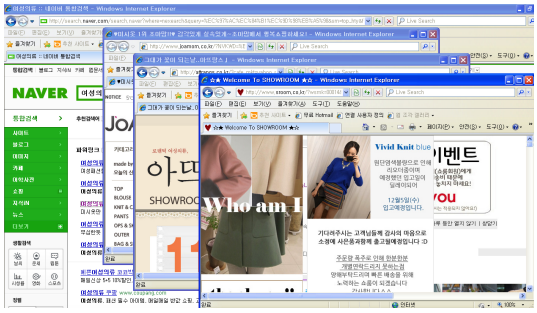

Fig. 7. Additional advertisement popup of page navigation

Table 5. Ad-Injection Type-Ⅴ URIs

No	URI
1	http://ad.openmatch.co.kr/AppCom/OpenmatchOpenLog.asp?ak=JXVDNUVDJXVDMTMxJXVDNzU4JXVCOTU4&ac=000C29DAB7EC&cddtc=120&nw=1&nt=10&sh=SEARCH.NAVER.COM
2	http://ad.openmatch.co.kr/?ref=aHR0cCUzQS8vYXR0cmFuZ3MuY28ua3IvJTNGY2FmZV9ta3QlM0R5YWhvb19wbA==
3	http://adm.adgod.co.kr/app/domain_under.php?domain=joamom.co.kr&uid=1101&app=120 HTTP/1.1
4	http://www.sroom.co.kr/?wsmk=00014&ref=appli_cation&product=adgod&codi=popunder&area=key

%3Dyahoo_pl"이며, 결과적으로 '아뜨랑'이라는 사이트를 출력하게 된다.

계속해서 "adm.adgod.co.kr"에 이동한 광고주 사이트인 "joamom.co.kr"정보가 전달되며(Table 5-No-3), 그 결과 "sroom.co.kr"라는 사이트로 이동하게 한다. 따라서 2개의 사이트가 추가로 이용자에게 출력 된다(Table 5-No-4).

(Ad-injection Type-Ⅵ) 사이트 이동 시, 해당 사이트에서 상단에 광고바 출력:

Fig. 8에서와 같이 네이버 검색 광고주 사이트 이동시, 웹 브라우저에 광고 툴바가 생성되는 경우이다.

Table 6의 URI 정보 1에서, 광고 인젝션 프로그램 (winexpand.exe)에 의해 "tops.jssearch.net"에 현재 방문한 사이트 주소(localurl)와 인젝션 프로그램 이름(site), 사용자 PC의 MAC Address(000c..)가 전달되며, 이어서

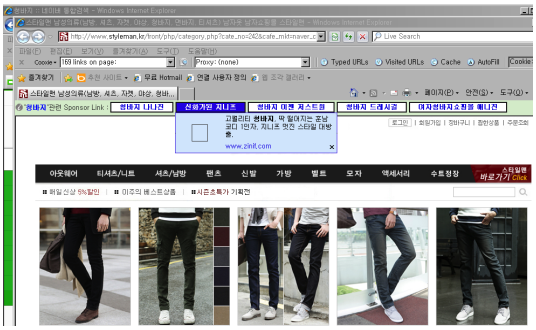

Fig. 8. Ad-injection on the upper bar of a navigated page

Table 6. Ad-Injection Type-Ⅴ URIs

No	URI
1	http://tops.jssearch.net/v2_index.php?type=&count=&pid=A_P_TOP_utiltop_5&keyword=û[redacted]&localurl=www.styleman.kr&pver=101&site=winexpand&umac=000c29a3155d%5F
2	http://tops.jssearch.net/v2_index_ad1.php?type=&count=&pver=101&pid=A_P_TOP_utiltop_5&keyword=%C3%BB%B9%D9%C1%F6&site=winexpand&umac=000c29a3155d_

Table 6의 2번 URI로 이동하도록 서버로부터 응답을 받게 된다.

Table 6의 정보 2에서, “tops.jssearch.net”에 keyword(EUC_KR 문자셋에서 %C3%BB는 ‘청’이라는 글자로, 청바지라는 키워드임)와 인젝션 프로그램 이름(site), 그리고 이용자 PC의 MAC Address(000c...)가 전달되고, 관련되는 광고 이미지를 서버로부터 수신하여, 브라우저 상단에 툴바 형태로 출력된다.

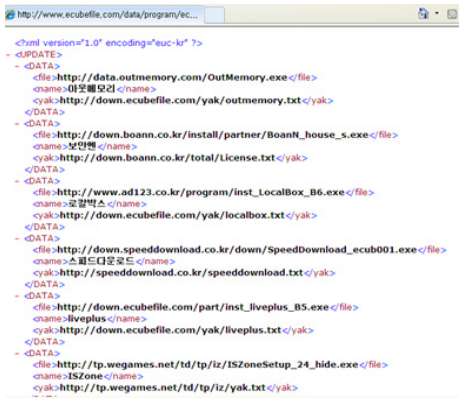

Fig. 10. Ad-injection on the upper bar of a navigated page

4.2 분석 결과

본 연구에서 분석한 27개 다운로더 중에 1개 이상의 네이버 광고 인젝션 프로그램을 설치한 다운로더는 93%(25개)였으며, 전체 프로그램 중 56%(111개)가 광고 인젝션 프로그램이었다. nc21 다운로더, 탑유틸다운로더, 조이유틸다운로더, 유틸봄다운로더는 각각 9개의 광고 인젝션 프로그램을 설치하였다. 특히 이들은 서로 같은 광고 인젝션 프로그램을 설치하기도 하였다.

이들 광고 인젝션 프로그램 중 63%에서는 PC의 MAC Address를 수집하여 특정 서버로 전송하는데 이는 설치한 PC 수에 따른 수익 배분을 염두에 둔 것으로 보인다. 특히 광고 대행사(ad network)인 “interich.com” 서버와 통신하는 searchup.exe, WindowLivePot.exe, HubGate.exe(dll), adsup.exe, primead.exe, realplus.exe의 프로그램들은 각각 “clickpang.co.kr”, “adsup.co.kr”,

(a) ADSUP website (b) PRIME-AD website (c) CLICKPANG website

Fig. 9. Similar ad-network pages

Table 7. Statistics of detected abusing behaviors by Naver SafeGuard

Detection Statistics	The first week of Jan. 2013	The first week of Dec. 2016	Remarks
# of SafeGuard Active User	4.15 million	3.7 million	-10.8%
# of abusing program installer	1.54 million	0.18 million	-88.3%
Ratio of abusing program installer	37%	5.1%	-31.9%
# of blocking count for abusing act	390 million	50 million	-87.1%
# of unknown abusing detection	25 million	4.6 million	-81.6%
# of blacklist	255	683	167%
# of pop-ups	297,385	3,381	-98.8%

"prime-ad.co.kr"와 관련 있었고 Fig. 9에서 보듯이 3개 회사의 소개 페이지는 매우 유사하였기 때문에 동일 사업자의 행위로 판단할 수 있다.다운로더가 설치하는 프로그램 목록을 지속적으로 모니터링 한 결과, 1일 평균 4.6개의 프로그램이 신규로 발견되었다. 이는 다운로더들이 설치하는 프로그램들이 계속 업데이트되고 있음을 알 수 있었다. 또한 설치되는 프로그램 정보를 분석해 보면, Fig. 10과 같이 〈DATA〉라는 태그 아래에 업데이트 할 파일 경로 〈FILE〉, 프로그램 이름 〈NAME〉, 프로그램 약관 경로인 〈yak〉으로 이루어져 있다.

V. 대응방안 및 시사점

앞서 언급하였듯이, 본 논문에서는 2012년 11월부터 12월까지 다운로더 27개와 이들이 설치하는 199개의 프로그램을 대상으로 분석하였다. 이렇게 과거의 데이터를 사용하여 논문을 작성한 이유는, 당시에 해당 프로그램들의 분석 결과의 공개로 인해 더 많은 모방 프로그램과 그로 인한 광고 어뷰징 피해 확산을 염려했기 때문이다. 하지만 현재 웹 브라우저에서는 이들 광고 인젝션 프로그램의 동작이 일부분 제한 받기도 하며, 정책 및 기술적인 대응 사례가 있다. 우선 기술적인 대응으로 본 논문에서는 상세히 다루지 않지만, 세이프가드(SafeGuard)[4] 모듈을 이용해서 광고 인젝션 행위를 탐지 및 차단한다. 세이프가드는 실제 BHO Connection, HTML Document 획득, 외부 프로세스 연결을 차단, HTML의 각 요소를 변조할 수 있는 메소드(method)를 제어, WinInet API 호출을 방지하여 대응하고 있다.

Table 7은 네이버 세이프가드의 주간 탐지 현황을 보여주고 있다. 2013년 대비하여 약 4년 사이에, 어뷰징 프로그램 설치자 수는 88% 감소하였고, 어뷰징 행위도 80%대로 줄어들었다. 이는 광고 인젝션 시장과, PC시장에서의 브라우저 점유율[5]의 변화에 영향을 받은 것으로 보여진다. 하지만 현재도 18만 명에 가까운 이용자의 PC에서는 광고 인젝션이 발생하고 있다.

광고 인젝션에 대한 기술적인 대응책 뿐만 아니라 정책적인 대응으로 사법적인 대응[6]과 과거 정보통신부에서 발간한 바 있는 스파이웨어(spyware)기준에 새로운 유형을 반영하기 위해 노력하고 있다. 2007년 개정된 스파이웨어에 대한 구체적인 행위가 다음과 같이 정의되었다.:

- 이용자 동의 없이 웹브라우저의 홈페이지 설정이나 검색설정을 변경하거나 또는 시스템 설정을 변경하는 행위
- 이용자 동의 없이 정상 프로그램의 운영을 방해 중지 삭제하는 행위
- 이용자의 동의없이 정상프로그램의 설치를 방

4) 네이버 백신, 툴바, 클리너에 포함되어 있는 보안 모듈

5) 스탯카운터[10]에 의하면 한국에서 2013년 1월 IE 점유율이 72.2%였는데, 2016년 11월에는 35.2%로 37% 감소하였고, 같은 기간 크롬은 19.9%에서 53.9%로 34% 증가하였다.

6) 광고인젝션 프로그램 개발 및 유포자와 광고 수익 수혜자에 대한 형사소송 결과, 불법으로 몇 차례 판결이 나온 바 있다.

해하는 행위
- 이용자의 동의 없이 다른 프로그램을 다운로드 해 설치하게 하는 행위.

광고 인젝션 행위와 관련하여, 특히 2차 사이트에 발생하거나, 출처 표시가 되어 있는 인젝션 된 광고의 경우 국내법으로 처벌하기 어렵다. 최근의 판례로 보면 출처 표시가 없거나, 원래 인터넷 사이트의 광고인 것처럼 오인하게 만들지 않는 한, 부정경쟁방지법으로 처벌받기 어렵다. 본 연구를 통하여 인터넷 광고 인젝션의 심각성과 더불어 이용자들을 보호하기 위한 기술적인, 정책적인 대응 방안 수립에 기반 데이터가 되었으면 한다.

VI. 결 론

본 연구에서는 국내에서는 거의 연구되지 않은 인터넷 광고 인젝션 연구를 수행하였다. 국내 대형 포털 사이트 네이버를 대상으로 한 인터넷 광고 인젝션의 유형을 탐색 및 분류하고, 광고 인젝션의 특성을 분석하였다. 검색을 통해 특정 유틸리티 프로그램을 설치할 수 있는 다운로더를 일괄 분석한 결과, 대다수의 다운로더가 광고 인젝션 프로그램을 설치하고 있는 것을 확인하였다. 특히 광고 인젝션 프로그램 상당수가 수익 집계를 위해 설치 후 MAC Address를 수집한다는 사실과, 다운로더 중 상당수는 지속적으로 설치하는 광고 인젝션 프로그램을 달리하며, 그 목록은 서로 중복될 수 있다는 것을 확인하였다. 본 연구에서 발견된 광고 인젝션 프로그램 목록을 기술적으로 대응하여 한시적인 성과를 보기도 했으나, 업데이트는 되는 광고 인젝션 프로그램 특성상 보다 고도화된 차단 방법이 요구된다. 또한 광고 인젝션 프로그램의 배포형태가 악성코드 배포의 행위와도 유사하기 때문에 광고 인젝션에 기반한 악성행위 분석에 대한 향후 연구가 필요하다. 이와 더불어 광고 인젝션 행위가 모바일 환경으로도 진화되고 있기 때문에 이에 대한 향후 연구도 필요하다.

References

[1] Hong il Lee, Cheol Park, Youn Jin Lee, "A Typology and Effects of Internet Advertising according to the customer relationship stages", *Proceedings of the Korea Society of Information Technology Applications Conference*, pp. 3-6, Nov. 2003

[2] Google Security Blog, "New Research: The Ad Injection Economy", https://security.googleblog.com/2015/05/new-research-ad-injection-economy.html

[3] Brad Miller, Paul Pearce, Chris Grier, Christian Kreibich, and Vern Paxson, "What's clicking what? techniques and innovations of today's clickbots", I*n Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, pp. 164-183, Jul. 2011.

[4] Paul Pearce, Vacha Dave, Chris Grier, Kirill Levchenko, Saikat Guha, Damon McCoy, Vern Paxson, Stefan Savage, and Geoffrey M Voelker. "Characterizing Large-Scale Click Fraud in ZeroAccess", *ACM Conference on Computer and Communications Security (CCS)*, pp. 141-152, Nov. 2014.

[5] Zhou Li, Kehuan Zhang, Yinglian Xie, Fang Yu, and XiaoFeng Wang, "Knowing your enemy: understanding and detecting malicious web advertising", *ACM conference on Computer and Communications Security (CCS)*, pp. 674 - 686, Oct. 2012

[6] Gabi Nakibly, Jaime Schcolnik and Yossi Rubin. "Website-Targeted False Content Injection by Network Operators", *25th USENIX Security Symposium (USENIX Security 16)*, pp. 227-244, Aug. 2016

[7] Muhammad Ahmad Bashir, Sajjad Arshad, William Robertson, Christo Wilson, "Tracing Information Flows Between Ad Exchanges Using Retargeted Ads", *25th USENIX Security Symposium (USENIX Security 16)*, pp. 481-496, Aug. 2016

[8] Alexandros Kapravelos, Chris Grier, Neha Chachra, Christopher Kruegel, Giovanni Vigna, and Vern Paxson, "Hulk: Eliciting Malicious Behavior in

Browser Extensions", *23th USENIX Security Symposium (USENIX Security 16)*, pp. 641-654, Aug. 2014
〔9〕 Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon McCoy, Antonio Nappa, Vern Paxson, Paul Pearce, Niels Provos, and Moheeb Abu Rajab. "Ad Injection at Scale: Assessing Deceptive Advertisement Modifications", *Proceedings of the IEEE Symposium on Security and Privacy*, May. 2015
〔10〕 Statcount, http://gs.statcounter.com

〈저자소개〉

조 상 현 (Sanghyun Cho) 정회원
1997년 2월: 고려대학교 컴퓨터학과 졸업
1999년 2월: KAIST 전산학과 석사
2005년 2월: KAIST 전산학과 박사
2005년 3월~2006년 9월: 고려대학교 정보보호대학원 연구교수
2006년 9월~2007년 9월: KAIST 전산학과 시스템보안센터 연구원
2007년 9월~현재: Naver Security Leader
〈관심분야〉 정보보호, 서비스 보안, 이상탐지

최 현 상 (Hyunsang Choi) 정회원
2004년 8월: 고려대학교 컴퓨터학과 졸업
2006년 8월: 고려대학교 컴퓨터학과 석사
2012년 2월: 고려대학교 컴퓨터학과 박사
2012년 3월~2013년 2월: 고려대학교 연구교수
2013년 2월~2014년 2월: UC Berkeley Postdoc
2014년 3월~2016년 5월: Secui 책임
2016년 5월~현재: Naver 연구원
〈관심분야〉 정보보호, 전자공학, 통신공학

김 영 갑 (Young-Gab Kim) 정회원
2001년 8월: 고려대학교 컴퓨터학과부전공
2003년 8월: 고려대학교 컴퓨터학과 석사
2006년 8월: 고려대학교 컴퓨터학과 박사
2006년 9월~2008년 3월: 고려대학교 정보보호대학원 연구교수
2008년 3월~2010년 1월: 국가평생교육진흥원 선임전문원
2010년 2월~2013년 2월: 고려대학교 연구교수
2013년 3월~2015년 2월: 대구가톨릭대학교 IT공학부 조교수
2015년 3월~현재: 세종대학교 정보보호학과 조교수
〈관심분야〉 사물인터넷 보안, 보안공학, 위험분석