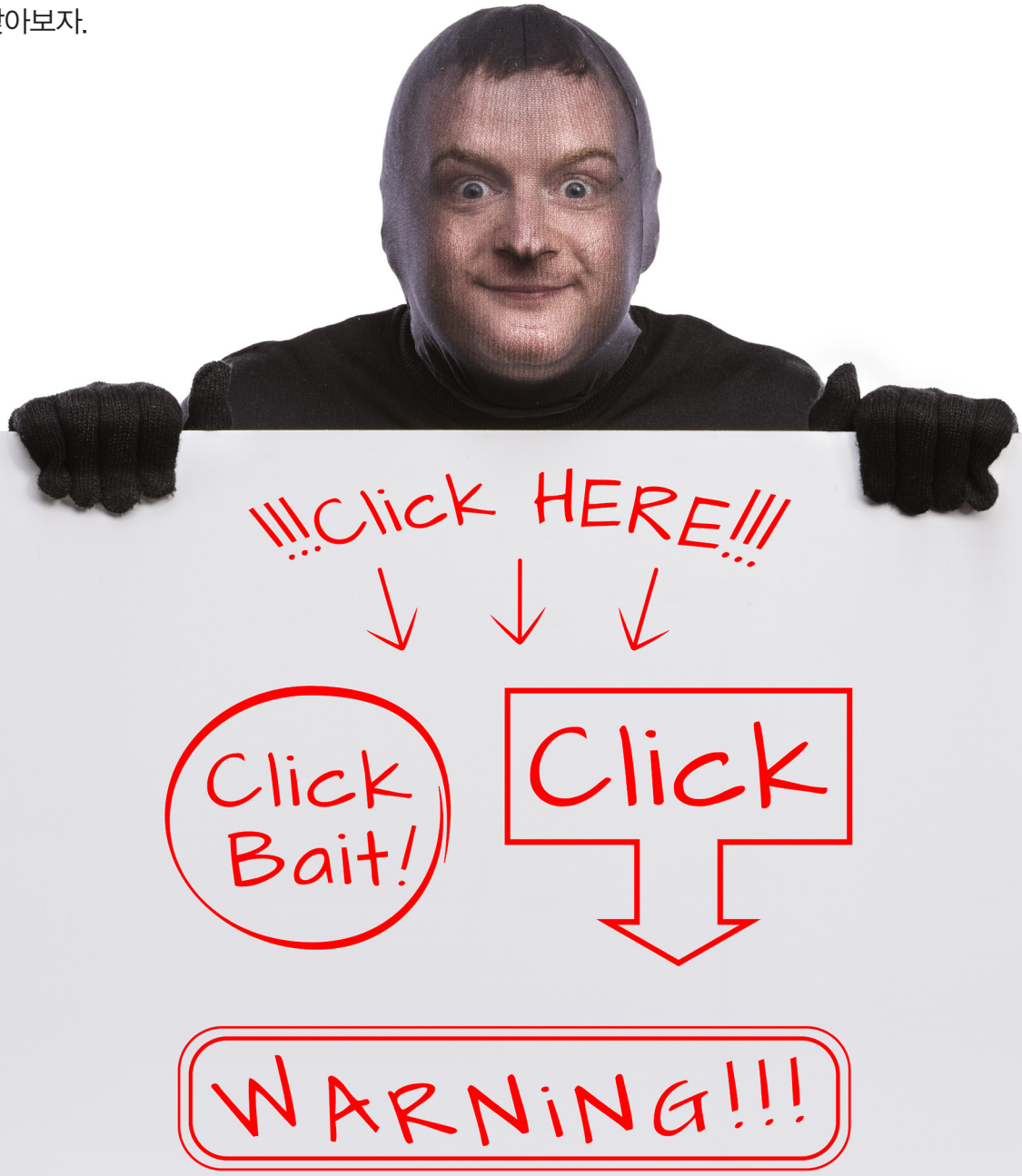
IDG

IT WORLD CIO

IDG Tech Report | Malvertising

"광고 속 악성코드" 멀버타이징의 이해와 대처법

멀버타이징(Malvertising). 악성코드를 합법적으로 보이는 광고에 감춰 유포하는 행위로, 최근 엄청난 속도로 증가하는 사이버 공격 방법 가운데 하나다. 탐지도, 체포도, 처벌도 힘든 멀버타이징에 대응하는 방법은 생각보다 까다롭다. 광고 속 악성코드, 멀버타이징의 동작 원리를 알아보고 방어법도 찾아보자.



“광고 속 악성코드” 멀버타이징의 이해와 대처법

Andrada Fiscutean | CSO

악성코드(Malware)와 광고(Advertising)의 합성어인 멀버타이징은 범죄자가 은밀하게 사람들을 공격대상으로 삼기 위해 광고를 사용하는 공격기법이다. 일반적으로, 범죄자는 믿을 수 있는 웹사이트의 광고 공간을 구매하고, 보기에는 합법적인 광고를 게재하면서 광고 내부에 악성코드를 숨겨 놓는다. 악성 광고(Bad ads)는 사용자를 악성 웹사이트로 우회시키거나 컴퓨터 또는 모바일 기기에 악성코드를 설치한다.

멀버타이징과 애드웨어의 차이점

뉴욕타임스, 스포티파이, 그리고 런던 증권 거래소를 포함해 전세계에서 인기있는 웹사이트들이 부주의로 악성 광고를 게시해 사용자들을 위험에 빠뜨린 적이 있었다. 걱정스러운 점은 사용자가 광고 이미지를 클릭하지 않더라도 감염된다는 것이다. 해당 광고를 로드하는 것만으로도 충분하다. 피해자가 한 일이라고는 어떤 웹 페이지를 거쳐간 것뿐이기 때문에 이런 방법을 “드라이브 바이 다운로드(Drive-by Download)”라고 부른다.

사이버 범죄자들은 랜섬웨어(Ransomware), 크립토마이닝 스크립트(Cryptomining Script), 뱅킹 트로이목마(Banking Trojans) 등 다양한 형태의 돈벌이용 악성코드를 유포하기 위해 멀버타이징을 사용한다. 이를 통해 공격자는 상당한 이득을 챙길 수 있다. 악성 광

고 대응 솔루션 개발 업체인 콘피언트(Confiant)의 공동 창업자이자 CTO인 제롬 단구는 "현재 멀버타이징은 매우 조직화된 비즈니스다"라고 말했다.

멀버타이징은 간혹 애드웨어(Adware)와 혼동되곤 한다. 멀버타이징은 광고물에 포함된 숨어있는 악성코드를 가리키고, 이는 감염된 웹사이트에 들어온 사용자에게 영향을 미친다. 반면 애드웨어는 사용자의 컴퓨터 상에서 구동되는 프로그램이다. 애드웨어도 합법적인 소프트웨어 패키지 안에 숨겨진 채로 설치되거나, 사용자 모르게 컴퓨터에 설치될 수 있다.

빠른 속도로 증가하는 멀버타이징 공격

멀버타이징 공격은 빠른 속도로 증가하고 있는데, 콘피언트는 온라인 광고 200개 중 1개가 악성이라고 추산한다. 안티멀버타이징 솔루션 판매업체 지오엣지(GeoEdge)는 최대 100개 중 1개의 광고가 안전하지 않다고 추정한다. 2017년, 구글은 사용자들에게 악성 웹사이트를 보내려고 시도한 7,900만 개의 광고를 차단했으며, 원치 않는 소프트웨어 설치를 추천한 4,800만 개의 광고를 삭제했다.

악성 광고로 인해 사용자는 다양한 위험에 직면해 있다. 지오엣지의 마케팅 담당 부사장인 토비아스 실버는 "가장 일반적인 멀버타이징 공격은 자동 리다이렉트(Auto-redirect)를 통해 사용자를 웹

페이지에서 전혀 다른 위치로 이동시켜 여러 가지 위협에 노출시키는 것이다. 익스플로잇 킷(Exploit Kit), 파일 자동 다운로드로 이어지는 피싱 사기, 랜섬웨어 공격, 그리고 악성 광고 등이 사용자들을 노리고 있다"고 말했다.

지오엣지에 따르면, 2018년 4분기 전체 멀버타이징 공격의 47.6%를 자동 리다이렉트가 차지했다. 한편, 악성 광고 프리 클릭(Pre-click, 웹 페이지의 최상위 스크립트에 내장된 드라이브 바이 다운로드나 악성코드) 건수는 총 사건의 25%에 달했다. 또한 악성 광고 포스트 클릭(Post-click, 사용자가 광고를 클릭하면 곧바로 감염되거나 악성 웹사이트로 리다이렉트 된다) 건수는 7%를 차지했다.

화이트 옵스(White Ops)의 공동 창업자이며 사장인 마이클 티파니는 "멀버타이징 공격 그룹은 계속 성공할 것으로 보이는데, 그 이유는 이들을 법정에 세우기가 어려운 경우가 많기 때문"이라고 말했다. 2018년 말, 화이트 옵스는 "3ve(이브, Eve로 발음)"라 부르는 가장 정교한 광고 사기 조직을 와해시키기 위해 구글을 비롯한 10여 개의 단체, 사법 기관들과 공조해야 했다. 3ve는 돈벌이를 위해 웹사이트 허위 버전과 허위 방문자들을 만들어냈다.

이 사건에서는 범인들을 체포했지만, 일반적인 광고 사기에 대한 사건은 그렇지 못하다. 티파니는 "범죄자들에게 죄값을 치르게 하는 것이 여전히 드문 경우다. 이브는 광고 사기를 하는 정교한 사이버 범죄자를 처벌하는 성과를 거둔 최초의 사례였다"고 말했다.

멀버타이징의 발전과 동작 원리

멀버타이징은 2007년 말 혹은 2008년 초에 처음으로 등장한 이후 계속해서 새로운 요령을 배웠다. 당시에는 어도비 플래시에 있던 취약점을 통해 마이스페이스(MySpace)를 포함한 몇 곳의 웹사이트에 악성 광고를 배포했다. 2011년에는 드라이브 바이 다운로드

의 최초 사례가 발견되었다. 이 공격에서 스포티파이는 한 달에 수백 달러로 빌릴 수 있었던 악명높은 블랙홀 익스플로잇 킷을 사용한 멀버타이징 공격의 중심에 있었다.

이후 수년 동안, 멀버타이징의 범행 수법은 동일하다. 일반적으로, 공격자들은 광고 대행사에서 광고 공간을 구매한 다음 들키지 않기를 바라면서 감염된 이미지를 제출한다. 처음에는 합법적인 광고를 보내다가, 나중에 악성코드를 삽입하기 시작한다. 사람들을 충분히 감염시킨 뒤에는, 스스로 흔적을 지우고 악성코드를 제거할 수 있다.

이런 사이버 범죄자들은 흔히 광고 업계에서 채택하고 있는 복잡한 메커니즘을 악용한다. 많은 경우, 광고주와 광고 대행사 사이에는 광고 네트워크(Ad Network) 그리고 한 곳 이상의 재판매 업체가 포함된 아주 긴 공급망이 있다. 체크포인트는 최근의 멀버타이징 공격이 보여주듯이, 전체 공급망을 조작할 수 있어 합법적인 온라인 광고 회사가 멀버타이징 조직의 중심에 있을 수도 있다고 지적했다.

2018년 7월, 체크포인트 연구원들은 감염된 워드프레스 웹사이트를 방문했던 수천 명의 사용자들에게 대규모 멀버타이징을 한 활동을 적발했다. 악성 광고에는 어도비 플래시 플레이어를 포함해 브라우저와 브라우저 플러그인에 있는 패치되지 않은 취약점을 악용한 자바스크립트 코드가 포함되어 있었다. 공격자들은 공격을 혼란스럽게 만드는 활동적인 리그(RIG)를 포함해 여러 가지 익스플로잇 킷을 사용했는데, 리그는 여러 가지 웹 기술을 결합하고 있다(DoSWF, 자바스크립트, 플래시, 그리고 VB스크립트).

특히 체크포인트는 "유명 광고 네트워크 회사인 애즈테라(Ads-Terra)는 평범한 광고 대행사를 가장한 사이버 범죄자로부터 트래픽을 구매해 왔는데, 이 회사는 악의적인 활동을 통해 입수한 트래픽을 재판매했다"고 밝혔다.

콘피언트의 단구는 멀버타이저(멀버타이징 조직)들이 가장 유명한 광고 플랫폼들과 관계를 구축하고 있다고 말했다. 단구는 "광고 기술 업계에는 업계가 근본적으로 멀버타이저들에 의해 감염되었다는 인식이 커지고 있다"며, "악성 광고가 사용자에게 노출될 때마다, 광고 기술 생태계를 통해 여러 층의 탐지를 피해왔다"고 설명했다.

더 나아가 사이버 범죄자들은 대형 웹사이트를 직접 해킹할 수 있는 경우, 이 전 과정을 거칠 필요 없이, 사람들이 악성 광고에 노출되도록 속일 수 있다. 실제로, 보안 블로거인 랜디 아브람스는 에퀴팩스(Equifax)에서 악명높은 침해 사건 직후에 이런 일이 벌어졌음을 밝힌 바 있다.

일반 사용자의 관점에서 볼 때, 악성 광고는 종종 격한 반응을 이끌어내고 즉각적인 행동을 조장하기 때문에 주목하지 않을 수 없다. 예를 들어, "1달러로 아이폰을 구매한다" 등 헐값 제품을 약속해, 사용자들이 신용카드 데이터를 제공하도록 속인다. 콘피언트는 주말이 되면 멀버타이징 활동이 36%나 많아지는데, 멀버타이저들이 좋아하는 요일은 일요일이라는 것을 밝혀냈다. 휴일, 그리고 사람들이 적극적으로 할인을 찾는 블랙 프라이데이 같은 쇼핑 시즌에도 멀버타이징 활동이 급등한다.

점점 더 정교해지는 멀버타이징 공격 현황

멀버타이징 업계는 악성코드 전달 방법이 더욱더 정교해지고 있다고 밝혔다. 사이버보안 업체인 리스크IQ(RiskIQ)의 연구원 필 카우저는 2019년 초에는 사용자의 클릭조차 필요없는 드라이브 바이 악성 광고(drive-by malicious ads)가 증가했다고 밝혔다.

콘피언트의 단구는 "현재 가장 흔한 공격은 기프트 카드 사기"라고 말했다. 콘피언트는 2018년 말, 미국 시민의 iOS 기기를 목표로 하는 대규모 멀버타이징 캠페인을 밝혀냈다. 스캠클럽(ScamClub)

이라 알려진 사이버범죄 조직은 겨우 이틀만에 2억 개의 브라우저 세션을 가로챘다. 단구는 무료 아마존 기프트 카드 사기를 언급하면서 "공격자는 보상을 받을 거라고 기대한 피해자가 자발적으로 공유한 엄청난 양의 개인 데이터를 수집했다"며, "수집된 데이터에는 구매 의도, 건강 관련 데이터가 포함되어 있었으며, 공격자에 의해 데이터 공급업체에 재판매됐다"고 말했다.

e고블러(eGobbler)라는 또 다른 범죄조직도 미국 거주 사용자들을 목표로 삼았다. 이 대규모 작전은 미국 대통령의 날(2월 셋째 주) 주말과 연계되어 있었다. 피해자들이 광고를 클릭하면, 해당 광고는 피해자들을 악성 웹사이트로 리다이렉트했고, 이런 웹사이트 가운데 다수는 피해자들이 개인 데이터와 금융 데이터를 입력하도록 유도했다.

단구는 광고 업계의 복잡한 메커니즘도 일부 책임이 있다고 지적했다. 단구는 "가장 최근의 e고블러 공격 가운데 하나는 7개의 광고 플랫폼과의 직접적인 관계를 통해 감행되었다"고 말했다. 이는 믿기 어려운 수치이며 멀버타이징 조직들이 광고 기술 환경에 얼마나 깊숙이 뿌리내리고 있는 지를 보여준다.

e고블러는 악성코드를 감추기 위해 '크리에이트JS(CreateJS)'와 GSAP(GreenSock Animation Platform)과 같은 HTML5 라이브러리를 목표로 하고 있어, 보안 분석가나 자동 스캐너가 탐지해내기가 매우 어렵다. 단구에 따르면, 이 집단은 스캐너를 속이기 위해 정교한 안티봇(Anti-bot) 기법을 악용하고 있다.

멀버타이징의 기본 도구, 스테가노그래피와 폴리글롯 이미지

멀버타이징 집단이 즐겨 사용하는 도구 가운데 하나가 스테가노그래피(Steganography)다. 다른 텍스트나 이미지 안에 메시지를 감춘다는 스테가노그래피의 개념은 최소 2,500년 이상 되었으며, 헤로도토스가 '역사(Histories)'에서 두어 가지 사례를 언급하기도

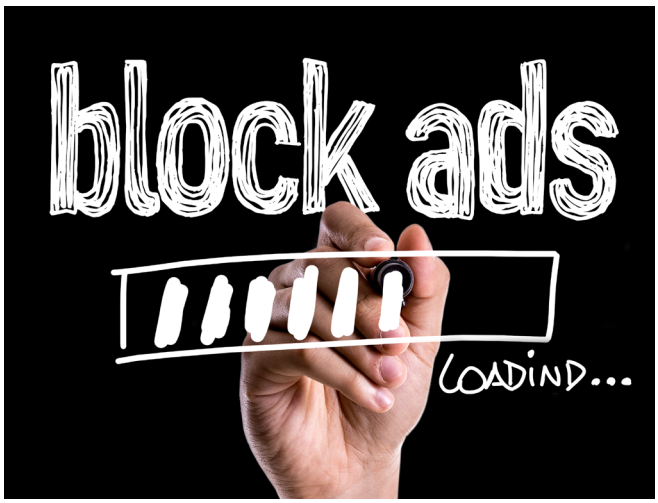
했다.

멀버타이징 조직은 흔히 악성코드를 광고 이미지에 숨겨진 이미지에 끼워넣는 동일한 접근방식을 사용하고 있다. 지오엣지에 따르면, 2018년 4분기를 거쳐 2019년에 접어들면서 이런 형태의 범죄가 기하급수적으로 증가하고 있다.

이 공격의 피해자 중에는 수십억 달러 가치의 정보 서비스 업체인 익스피리언(Experian)이 있다. 지오엣지의 실버는 "익스피리언의 광고 중 하나가 숨겨진 이미지로 공공연히 표적이 되었는데, 이 숨겨진 이미지는 사용자들에게는 보이지 않았지만 광고 요청 안에 숨겨져 있었고, 내장된 악성코드를 호출했다"고 말했다. 실버는 "사용자의 데스크톱이나 스마트폰에 이 광고가 나타나기만 하면, 악성코드가 활성화된다. 이 경우, 해당 악성코드는 미국 사용자들을 목표로 하는 피싱 사이트로의 자동 리다이렉트였다"고 덧붙였다.

콘피언트의 보고서에 따르면, 스테가노그래피는 베리멀(Very-Mal)이라는 멀버타이징 조직도 선택했는데, 베리멀은 맥 사용자를 표적으로 하고 있다. 이 경우 자바스크립트 악성코드가 이미지 파일 안에 숨겨져 있었다.

범죄 조직은 늘 개선점을 찾고 있어서, 스테가노그래피는 최근에 훨씬 더 영악한 동반자를 얻기에 이르렀다. 폴리글롯(Polyglot) 이미지가 바로 그것이다. 데브콘(devcon) 연구원들은 이 정교한 기법을 사용한 사이버범죄 조직을 밝혀냈다.



데브콘은 "스태가노그래피를 이용한 취약점 공격은 몇 개의 픽셀(Pixel)을 변조해 이미지에 숨겨진 데이터를 사용한다. 이미지를 보는 일반 사용자는 전혀 의심하지 않겠지만, 스테가노그래피는

변조된 픽셀을 찾아 실행가능한 자바스크립트로 재조립하기 위한 패턴과 옵셋을 알아내기 위해 (이미지에는 들어 있지 않은) 약간의 추가 자바스크립트를 필요로 한다"고 설명했다.

폴리글롯 취약점 공격은 한 걸음 더 나아간다. 이미지인 동시에 유효한 자바스크립트처럼 보일 수 있어서 이런 이름이 붙은 것이다. 폴리글롯의 또 다른 특징은 페이로드(Payload)를 추출해내기 위한 외부 스크립트가 필요없다는 것이다.

이 경우, BMP 이미지에 삽입된 악성코드는 파일의 16진수 바이트로 동작했다. 16진수 바이트를 조작해 컴퓨터가 이미지 크기 대신 /**에 해당하는 문자 코드를 읽을 수 있다. /**는 자바스크립트에서 주석을 가리키는 문자 조합으로, 자바스크립트 인터프리터는 그 사이에 있는 모든 것을 무시한다.

공격자는 시퀀스 ='를 추가한 다음 페이로드 문자열을 추가했다. 이를 통해, 이 파일은 브라우저에서 2가지 방식으로 구동할 수 있다 (자바스크립트를 무시하는 이미지 또는 이미지 데이터를 무시하는 스크립트).

초기 단계에 있는 모바일 멀버타이징

스마트폰과 태블릿 사용자는 기기의 보안을 그다지 걱정하지 않는 경향이 있기 때문에 멀버타이징 집단이 공격하기 좋은 대상이 되고 있다. 스마트폰을 사용하면서 실수로 광고를 탭하는 경우도 많다.

최근의 모바일 멀버타이징 공격은 안드로이드와 아이폰 사용자 모두를 목표로 하고 있다. 예를 들어, 2018년 말 적발된 페이리크(PayLeak)는 풀리처상 수상작의 관심 독자에게 악성 광고를 배포했다. 사용자가 광고를 클릭하면, 이 광고는 중국에 등록된 악성 도메인을 호출했다. 이 악성코드는 가령 피해자가 어떤 종류의 기기를

사용하고 있는지, 안티바이러스로 보호되고 있는지, 그리고 피해자가 이동 중인지, 아니면 쉬고 있는지 등을 알아내는 데 관심을 갖고 있었다. 안드로이드 사용자의 경우, 피싱 사이트로 리다이렉트하는 아마존 기프트 카드가 미끼로 쓰였다. 반면에, 아이폰 사용자들에게는 잇따른 팝업창이 표시되었는데, 애플 페이 계정을 갱신하라는 허위 안내문이 포함되어 있었다.

모바일 보안업체 완데라(Wandera) 부사장 마이클 코빙톤은 "모바일 멀버타이징은 초기 단계"라며, "공격자는 아직 기기의 이런 보호되지 않는 채널로 무엇을 할 수 있는 지를 파악하고 있는 중이다"고 말했다.

모바일 멀버타이징은 의도에 따라 크게 3가지 범주로 나눌 수 있다. 코빙톤은 "가장 널리 퍼져있는 멀버타이징의 용도는 아주 영악한 인앱(In-app) 피싱 공격을 감행하는 것이다. 두 번째는 광고 채널을 통한 크립토재킹(Cryptojacking)이다. 크립토 재킹은 암호화폐를 채굴하기 위해 다른 사람의 컴퓨터를 이용하는 것이다. 완데라는 크립토재킹의 영향을 받은 기기 수가 2018년 말에 월마다 거의 300%나 증가했다고 밝혔다. 세 번째 유형의 멀버타이징 공격은 기기에 악성코드 페이로드를 전달할 목적으로 설계된 것이다. 코빙톤은 "이 방법은 광고를 통한 공격 가운데 성공률이 가장 낮긴 하지만 공격자는 낌새를 차리지 못한 사용자에게 악성 앱을 전달하는 새로운 방법을 끊임없이 모색하고 있다"고 말했다.

멀버타이징으로부터 보호하는 방법

보안 연구원은 멀버타이징으로부터 자신을 보호하기 위해서는 안티바이러스를 설치하고 운영체제, 브라우저, 어도비 플래시 그리고 자바를 포함해 모든 소프트웨어를 최신으로 유지하라고 권고한다. 플래시와 자바 사용을 아예 중지한다면 더욱 강력하게 보호할 수 있다.

그런데, 보안 전문가는 광고 차단기(Ad Blocker)가 광고 업계와 저널리즘 모두를 죽일 수 있기 때문에 해결 방법으로 추천하지 않는다. 데브콘 CEO 매기 루이는 "LA 타임즈나 뉴욕타임스 등은 광고 수익을 통해 기자, 사진기자, 편집자의 임금을 지불하는 구조다." 며, "광고 차단기를 제공한다는 것은 매체의 모든 수입을 근본적으로 차단하는 것이다"고 말했다. 루이는 합법적인 광고는 통과시키고 악성 광고는 필터링할 수 있는 고스터리(Ghostery) 같은 도구를 권장한다.

대부분 보안업체는 개별 사용자가 멀버타이징 문제를 해결할 수 없다고 확신한다. 보안 업체들은 미디어, 브라우저 업계 그리고 광고 업계 모두가 현재 멀버타이징 사태에 더 큰 책임을 떠맡아야 한다고 주장한다. 그리고 미디어에게는 믿을 수 있는 광고 기업과만 함께 작업해야 할 것이라고 제안한다. 그러나 광고 업계의 이름높은 기업들도 멀버타이징에 영향을 받고 있다. 리스크IQ 연구원 필 카우저는 "미디어 발행인과 광고 거래소(Ad Exchange)가 광고의 전체 공급망에 대한 가시성을 제공하는 보안 제품을 사용해야 한다"고 권고했다.

단구는 멀버타이징 대처에 있어 작은 개선사항을 제안했다. 단구는 "점점 더 많은 미디어가 안전한 광고는 계속 가동하는 동시에 최종 사용자의 브라우저에서 곧바로 악의적 행태를 차단할 수 있는 실시간 클라이언트 측 탐지에 의지하고 있다"고 말했다.

공격자는 강제 리다이렉트(forced redirect)라 부르는 기법을 이용한 세션 하이재킹(Session Hijacking)에 크게 의존하고 있기 때문에 브라우저 공급업체들도 이를 이용해 멀버타이징에 대처하고 있다. 단구는 "HTML5 아이프레임 샌드박스(iframe Sandbox)는 하이재킹에 의한 광고로부터 보호하기 위해 서서히 도입이 늘어나고 있는 브라우저 기능이다"며, "구글은 자체적으로 교차 도메인 아이프레임(Cross-origin iframe)에 대한 더욱 광범위한 리다이렉트

차단기를 개발했다"고 말했다.

인터넷 보안업체인 맬웨어바이츠(MalwareBytes) 위협 정보 최고 책임자 제롬 세구라는 "멀버타이징 집단이 더욱 대담해지고 기만적인 공격을 하고 있기 때문에 최상의 보호 방법은 보안 소프트웨어를 실행하는 최신 시스템과 사기를 알아채기 위해 필요한 사용자 의식의 조합"이라고 말했다. 세구라는 "공격자는 인프라를 빠르게 바꿔가기 때문에 이들과 실랑이를 벌이기보다는, 능동적으로 대처해야만 공격자의 공격 방식을 규명해낼 수 있다"고 설명했다.

코빙톤은 "모바일 멀버타이징의 경우, 안전을 유지하기 위해 모바일 사용자들이 할 수 있는 최선의 방법은 개발자를 심사하지 않는 서드파티 앱 스토어를 피하는 것이다"면서, "우리는 멀버타이징을 통해 전달될 수 있는 폭넓은 위협을 탐지하기 위한 모바일 위협 방어 솔루션 사용을 권고하고 있다 "고 말했다.

수년 간 번창할 멀버타이징의 미래

보안 연구원들은 멀버타이징이 앞으로 수년간 번창할 것이며, 범죄 집단들은 더 똑똑해지고, 부유해지며, 색출하기가 더욱 어려워질 것이라고 본다. 데브콘의 루이는 폴리글롯의 사용이 증가할 것이라고 예상하고 있다. 루이는 "조만간 광고를 통해 유입되는 훨씬 더 발전된 위협들과 워터링 홀 공격(Watering Hole Attack)의 르네상스를 목격하게 될 것이다"고 말했다.

단구는 공격자가 공격방법을 계속해서 개선하고 있음을 우려하고 있다. 단구는 "1, 2년 전만 하더라도, 멀버타이징 페이로드는 코드가 달랐기 때문에 명확하게 인지할 수 있었다. 하지만 요즘 공격자는 광고 서버 고유 기능을 더 잘 활용해 서드파티 코드가 아닌 광고 기술 스택의 일부인 것처럼 숨기는 데 더 능숙해지고 있다"고 말했다.

대부분의 보안업체는 일부 사용자가 자신의 기기에 보안 제품을 설치하지 않아도 된다고 생각하기 때문에 멀버타이징 집단이 점점 더 모바일 사용자를 목표로 삼을 것이라고 예상하고 있다. 지오엣지는 2018년 멀버타이징 공격이 50%나 증가했으며, 2019년에 접어들면서 인앱 환경을 노린 악성 광고가 67%나 증가했음을 파악했다. 세구라도 유사한 트렌드를 발견했다. 세구라는 "여러 계층의 보호가 이미 존재하고 있는 데스크톱과는 달리, 모바일 기기는 보호 장치의 부재로 다양한 공격에 훨씬 더 취약할 뿐 아니라 사용자 인식 역시 부족하다"고 말했다.

몇 가지 밝은 희망도 있다. 리스크IQ의 카우저는 코인하이브(Coinhive)의 폐쇄로 자바스크립트 기반 암호화폐 채굴의 확산이 줄어들 것이라고 예상했다. 다른 연구원은 광고 업계가 이 문제를 더욱 심각하게 인식해 광고 품질 보장 도구와 광고 보안에 대한 더욱 강력한 요구를 반영하기를 바라고 있다. 지오엣지의 실버는 "매체의 발행인은 자사의 브랜드를 보호하고 긍정적인 사용자 경험을 보장하고 싶어하기 때문에, 사용자 불만은 점점 더 많은 발행인이 도움을 요청하게 만들 것이다"고 말했다.

콘피언트의 단구는 광고 업계가 할 수 있는 것에 대해 훨씬 더 낙관적이다. 몇 가지 계획은 보안 업계가 기여한 샌드박스된 광고 배치를 목표로 하고 있다. 단구는 "일단 이런 계획을 중심으로 한 도입이 일정 수준에 도달하면, 이들 공격 대부분은 제약을 받게 되기 때문에 공격자는 아직은 알 수 없는, 차세대 멀버타이징 페이로드로 선회할 수밖에 없을 것이다"고 말했다. ITWORLD