온라인 광고에서의 보안: 새로운 세계에서의 도둑(침입자)과 수호자[1][2]

벤자민 에델만

컴퓨터 보안에 관한 최근의 황당한 기사를 읽으신다면 온라인 광고에서 얼마나 많은 문제들이 발생하고 있는지 아시게 될 것입니다. 온라인 광고는 최종 이용자가 무료로 웹사이트를 이용할 수 있는 기반이기에 온라인 광고는 어디에나 존재합니다. 하지만 광고 보안의 허점도 널리 퍼져있습니다. 예를 들어 사기성 안티 스파이웨어 소프트웨어를 광고해주는 배너광고(악하다는 의미의 "Mal"수식어와 광고 "Advertisement"가 합쳐 Malvertisement 라고 함)에서부터 부정클릭 및 스파이웨어와 에드웨어까지 온라인 광고의 보안 허점은 눈에 띄게 많습니다.

지난 5 년 동안 저는 이용자를 속이는 수백 개의 사기성 온라인 광고를 발견했습니다. (웹의 최고 광고주들은 말할 것도 없습니다) 제가 찾은 사기성

---

1 본 논문은 Andy Oram 및 John Viega(O'Reilly Media, Inc., 2009)에 의해 편집된 것으로Beautiful Security에 영어로 실린 내용입니다.

2 본 번역은 서울대학교 법과대학 기술과법센터에서 제공하였습니다.

온라인 광고, 이용자와 광고주가 그들을 어떻게 보호할 수 있는지에 대해 본 장에서 요약하겠습니다.

이용자에 대한 공격

이용자들이 보통 온라인 광고 공격의 전형적이고 직접적인 일차 피해자입니다. 사기성 팝업 광고에서부터 완벽한 브라우저 사기까지 이용자들은 피해 복구과정의 비용을 직접 부담하게 됩니다. 이러한 온라인 광고의 가해자에 대해 본 장에서 알아보고자 합니다.

Exploit 탑재 배너 광고

'스팸왕'에서 '스파이웨어 유포자'로 변한 샌포드 월리스는 2004 년 3 월에 이용자의 동의 없이 컴퓨터에 소프트웨어를 설치하는 방법을 찾았습니다. 월리스는 윈도우, 인터넷 익스플로러, 또는 컴퓨터 사용자 소프트웨어의 결점 등 보안 취약점을 이용해 이용자의 동의 없이 컴퓨터를 조정할 수 있었습니다. 이전의 침입자들은 실행 파일이나 바이러스 감염이 된 문서를 열도록 컴퓨터 이용자를 설득해야 했었습니다. 하지만 이용자가 더 이상 이런 수법에 넘어가지 않고 피하는 것을 배우게 되자, 월리스는 새로운 exploit(시스템 침투에 관한 파일과 소프트웨어로서, 시스템의 취약점을 이용하여 해킹함)을 이용하여 이용자가 사이트를 방문만 해도 컴퓨터를 조정할 수 있는 방법을 찾은 것입니다. 우리는 하루에도 수많은 사이트를 방문하고 있습니다.

월리스는 협력자에게 메일을 보내 이번 성과를 알렸습니다.[3]

보낸이: 샌포드 윌리스, *masterwebfanclub@aol.com*

받은이: 자레드 랜스키, *jared@optintrade.com*

제 목: 내가 해냈다

일 자: 2004 년 3 월 6 일

이용자의 간섭 없이 실행 프로그램을 설치하는 방법을 찾아냈다. 이번이야말로 큰 돈을 벌 수 있는 기회로 보인다.

윌리스가 이러한 exploit 를 사용하여 이용자의 컴퓨터를 조종하게 되면 그가 원하는 어떤 소프트웨어도 설치할 수 있습니다. 여러 회사가 자신들의 소프트웨어를 이용자의 컴퓨터에 설치 할 수 있도록 윌리스에게 돈을 지불했습니다. 그래서 윌리스는 이용자의 PC 에 그들의 습성을 추적할 수 있는 프로그램을 설치했으며, 팝업 광고가 뜨게 하고, 추가적인 툴바를 더해 브라우저를 복잡하게 만들었습니다.

하지만 윌리스에게는 여전히 문제가 있었습니다. 보안 허점을 통해 이용자의 컴퓨터를 조종하기 위해서는 이용자가 우선 윌리스의 exploit 를 심는 사이트를 방문하게끔 해야 됐습니다. 어떻게 방법을 구했을까요? 자레드 랜스키에게 답이 있었습니다. 그는 배너 광고 네트워크를 통해 광고를 하는 방법을 활용하였습니다. 이제 일반 웹사이트 내에서 광고를 보기만 해도 이용자의 컴퓨터는 윌리스의 필요 없는 소프트웨어에 무더기로 감염될 수 있게 되었습니다.

---

[3] 본 이메일은 미국 연방거래위원회 소송 때 밝혀졌습니다. 출처: *FTC v. Seismic Entertainment, Inc., et al.*
No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. 2004).

그런데도 배너 광고 활용은 몇 가지 큰 걸림돌이 있었습니다. 일부 웹사이트는 광고를 광고주에게 직접 판매한다는 점입니다. 사실 대부분 사이트는 자기의 광고 공간을 광고 네트워크 (광고중개자로서 광고주를 카테고리로 묶어서 퍼블리셔에게 판매)를 통해 판매를 했습니다. 하지만 광고 네트워크가 실상을 알게 되면 분명히 격분할 것이었고 무엇보다도 월리스의 exploit 는 광고 네트워크 및 관련 있는 웹사이트 평판에 영향을 끼칠 것이 분명했기 때문입니다. 월리스와 랜스키는 추적을 피하기 위해 2 가지 계획을 세웠습니다. 첫째 그들은 광고 네트워크가 신경을 안 쓰는 주말에 exploit 를 운용했습니다.

보낸이: 샌포드 윌리스, *masterwebfanclub@aol.com*

받은이: 자레드 랜스키, *jared@optintrade.com*

제 목: 전략

내가 몰래 했어... 오늘부터 일요일 내내 - 다들 나가있을 때...

둘째, 만약 광고 네트워크에게 적발이 될 경우 랜스키는 일어난 일에 대한 관련성을 부인하는 것입니다. 예를 들어 싸이도어 광고 네트워크 부회장 밥 레귤러의 항의에 대해 랜스키는 이렇게 답변했습니다.

보낸이: 샌포드 윌리스, *masterwebfanclub@aol.com*

받은이: 밥 레귤러, *bob@cydoor.com*

제 목: 회신: OptinTrade Online Pharmacy 의 종료를 요청합니다 – 합의 위반

안녕하세요 – 해당 pharmacy campaign 은 새로운 코드 셋을 가진 신 광고입니다. 시험 단계에서 팝업 또는 내 홈페이지를 변경하지 않았기에 당신 회사의 광고에서 적용을 한 겁니다. 그런데 왜 이런 일이 일어났는지 모르겠군요. …

웰리스와 랜스키는 이런 방식으로 수천 개의 컴퓨터를 감염 시켰습니다(소송 자료에는 정확한 수치를 공개하지 않음). 하지만 그들의 수법은 결국 미국 연방거래위원회(Federal Trade Commission)에 의해 적발됐고 약 400 만 달러의 부당이득반환소송을 당하게 되었습니다.[4] 안타깝게도 웰리스와 랜스키의 전략은 단지 빙산의 일각이었습니다.

그 후 2004 년에 영국의 IT 뉴스 사이트 *The Register*[5]는 악성 소프트웨어를 이용자 컴퓨터에 설치하고 팝업을 보여주면서 이용자의 행동을 주의 깊게 추적하고 심지어 이용자의 컴퓨터를 스팸메일을 계속 생산하는 좀비 PC 로 전환시키는 exploit 에 의해 공격 당했습니다. 제가 그 exploit 를 시험해본 결과 수백 개의 파일과 수천 개의 레지스트리 키를 포함한 적어도 수십 개의 프로그램을 설치하는 것이라는 사실을 확인할 수 있었습니다.[6] 2005 년과 2006 년에 본 다른 exploit 도 이런 비슷한 수법을 이용했습니다.[7]

자주 이용하거나 신뢰하는 사이트를 방문해도 이용자는 사이트가 악성프로그램을 유포하고 있는 공장으로 변질했는지조차 모르는 사이에 이용자의 컴퓨터가 bot(인터넷상의 정보 검색을 위해 다른 사이트의 페이지도 자동적으로 연달아 검색 수집하는 프로그램)로 변하게 합니다. .

---

[4] FTC v. Seismic Entertainment, Inc., et al. No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788(D.N.H. 2004).

[5] "Bofra Exploit Hits Our Ad Serving Supplier." The Register. November 21, 2004. http://www.theregister.co.uk/2004/11/21/register_adserver_attack/.

[6] Edelman, Benjamin. "Who Profits from Security Holes?" November 18, 2004. http://www.benedelman.org/news/111804-1.html.

[7] Edelman, Benjamin. "Spyware Installation Methods." http://www.benedelman.org/spyware/installations/.

이런 exploit 가 탑재된 악성 소프트웨어의 설치를 막을 방법이 없습니다. 승인 없이 프로그램을 설치하는 행위를 금지하는 명령을 미국 연방거래위원회에서 여러 번 내렸으며[8], 소비자 집단소송에서도 승인 없이 프로그램을 설치하는 행위가 동산 침해행위(소비자가 사적 재산, 즉 컴퓨터를 이용하는 행위에 대한 방해)인 것으로 확인되었습니다.[9] 그럼 exploit 가 탑재된 악성 소프트웨어를 설치하는 사람들은 어떻게 매번 무사히 피할까요? 그들은 월리스의 교활한 방법으로 주말에만 활동을 하고 있습니다. 영업 외 시간에만 활동하는 자들을 본적이 있고 특정지역 이용자에게만(특히 광고 네트워크가 조사 및 조치를 취할 수 있는 곳에서 멀리 떨어진) 활동하는 것을 보기도 했습니다.

일반적으로는 악성 프로그램 설치자들은 중간 매개자를 이용하여 책임을 피합니다. 월리스와 랜스키의 협력관계와 같이 이런 중간 매개자는 여러 회사 · 파트너 · 협력자가 포함됩니다. 공모자 한명은 배너 광고를 하고 다른 한 명은 exploit 를 실행하며 또 다른 한 명은 소프트웨어를 개발하고 마지막으로 다른 한 명은 소프트웨어를 통해 돈을 버는 방법을 찾을 수 있습니다. 만약 이들에게 압력을 가하게 되면 서로가 서로에게 책임을 넘기게 됩니다. 예를 들어 배너 광고를 한 회사는 자신이 exploit 를 실행하지 않았다고 주장할 것이고, 소프트웨어를 제작한 회사는 배포자가 이용자 동의를 얻을 것을 약속한 계약을 제출할 것입니다. 서로 책임을 피하는 방식을 통해서 공모자들은 광고 네트워크,

---

[8] See FTC v. Seismic Entertainment, Inc., et al. See also In the Matter of Zango, Inc. f/k/a 180Solutions, Inc., et al. FTC File No. 052 3130. See also In the Matter of DirectRevenue LLC, et al. FTC File No. 0523131.

[9] Sotelo v. Direct Revenue. 384 F.Supp.2d 1219 (N.D. Ill. 2005).

규제자 또는 소비자 변호사측이 어느 특정인에게 책임을 지게끔 하는 행위를 예방합니다.

이런 공격은 계속 진행되고 있지만 눈에 띄게 줄었습니다. 무엇이 변한 것일까요? 윈도우즈 XP 서비스 팩 2 는 exploit 설치로부터 더 나은 보호 장치를 제공해줍니다. 인터넷 익스플로러의 포스트 SP2 패치와 결합하면 더욱 효과가 있습니다. 또한 규제자와 소비자가 많은 exploit 설치자들의 돈줄인 애드웨어 제작사를 상대로 소송을 걸었으며 대중적이지 않은 팝업을 통해 광고하는 것을 꺼려하는 광고주들 때문에 exploit 를 실행하는 경제적 이익이 점차 사라지고 있습니다.

전문지식이 있는 사람이라면 이런 악성프로그램을 직접 찾아낼 수도 있습니다. VMware Workstation 을 이용하여 새로운 가상의 기계를 마련하고 서비스 팩이 포함하지 않은 새로운 Windows XP 와 같이 공격받기 쉬운 컴퓨터 운영체제(Operating System, OS)를 설치해 보십시오. 웹을 띄워서 특이한 디스크나 네트워크 행동을 찾아보십시오. 더 좋은 방법은 패킷스니퍼(패킷으로 흘러드는 정보 속에서 패스워드 등의 정보를 판독하는 프로그램. 예: 무료 Wireshark)를 실행하거나 하나 혹은 더 많은 변화 추적기(저는 전반적인 스캔을 할 때에는 InCtrl 을, 빠른 스캔을 할 시에는 HijackThis 을 사용함)를 실행해 보십시오. 만약 컴퓨터가 exploit 를 발견하게 되면 패킷스니퍼의 로그를 확인하면서 무엇이 그리고 어떻게 반응하고 있는지 찾아내보십시오. 그런 후 이런 exploit 를 중지할 수 있게끔 사이트, 광고 네트워크 그리고 다른 중간 매개자에게 연락을 하십시오. 원칙적으로 말씀 드리자면 exploit 는 어디든 존재하지만 저는 보통 게임, 음악가사, 비트토렌트(BitTorrent: P2P 파일 전송

프로토콜의 이름이자 그것을 이용하는 응용 소프트웨어) 다운로드 링크에서 자주 찾게 됩니다. 무엇보다도 가상 기계가 감염되더라도 VMware 의 복구기능으로의 감염 전 단계로 복구 할 수 있습니다.

악성 광고(Malvertisements)

운이 좋지 않은 이용자들은 종종 웹 페이지에서 튀어나오는 배너 광고를 보게 됩니다. 이용자가 열고 있는 브라우저 이외에 다른 웹 브라우저가 뜬다는 면에서 팝업과 비슷합니다. 하지만 이런 '악성 광고'는 웹 사이트의 허락 없이 팝업으로 나오는 것입니다. 오히려 해당 웹 사이트는 팝업이 아닌 일반 배너 광고를 판매하고 싶어합니다. 더군다나 표준 팝업은 작은 공간을 차지하는데 비해 악성 광고가 웹 페이지에서 뜨게 되면 이용자의 스크린 전체를 차지하게 됩니다. 아주 드물지만 최악의 상황은 악성광고가 이용자의 전체 웹 브라우저를 다른 곳으로 교체해 버리면서 이용자가 원하는 사이트 대신 요청하지 않은 광고 사이트만 남게 됩니다.

사진 6-1 에서 보여주는 것처럼 악성 광고는 보통 자세한 증거 없이 이용자의 컴퓨터가 스파이웨어에 감염됐다고 통보하면서 사기성 안티스파이웨어 소프트웨어를 선전합니다.

예를 들어 화면에는 컴퓨터에 "scanningfilevw80.ocx"라는 파일이 존재한다고(테스트 PC 에는 해당 파일이 없더라도) 나옵니다. 사실 팝업한 웹 페이지는 문제점이 있는지 스캔을 할 수 없는 그야말로 일반 웹 페이지입니다. "지금 스캔 중"이라는 상단의 상자는 단지 광고의 일부분이며 진짜처럼 생긴 버튼이나 아이콘은 속임수입니다. 하지만 팝업과 실제의 user interface(일반

이용자들이 컴퓨터 시스템 또는 프로그램에서 데이터 입력이나 동작을 제어하기 위하여 사용하는 명령어 또는 기법), 과장된 감염 "경고"가 결합되어 이용자의 시선을 사로잡으면서 그들에게 구매하라고 설득하는 데에 상당한 효과를 가지게 됩니다.

사진: 6-1. 사기 스캔 광고

악성 광고는 웹 사이트와 광고 네트워크의 적발을 피하기 위해서 노력을 합니다. 무해한 상태에서 보게 되면 악성광고는 전형적인 플래시 광고(배너 혹은

애니메이션)처럼 보입니다. 하지만 적절한 시간이 되면 해당 악성 광고는 플래시 ActionScript 을 이용해 광고 프레임으로부터 나오게 합니다. 어떻게 하는 것일까요? ActionScript 는 stub(store unsigned byte) procedure 를 사용하여 블록을 해독한 후 일반적인 검사를 통해 난해한 코드를 나타냅니다. 다른 ActionScript 프로그램들은 이용자의 IP 주소를 참고하는 웹 서버를 확인하면서 광고가 어떤 행동을 취해야 하는지 결정을 내립니다. 이런 시스템은 타지에 있는 대리인을 고용해 먼 곳의 주소를 이용하면서 광고의 습성을 시험하여 감시자를 피할 수 있었습니다. 만약 이용자 PC 의 시간과 이용자 위치에 있는 IP 주소의 시간이 다르게 나오면 광고 서버는 해당 이용자가 대리인을 통한 감시자인 것으로 간주하여 기존에 해를 끼치지 않은 배너 모드로 전환합니다.

이런 공격을 막는 제일 좋은 방법은 고객의 장치를 완벽하게 보호하는 것입니다. 전형적인 배너 광고에서 플래시는 단지 사진, 애니메이션 그리고 가끔은 비디오만 보여줍니다. 단지 하나의 광고밖에 되지 않는데 왜 이렇게 다양한 코드를 허용해주는 것일까요? 기본적으로 광고는 어느 정도의 제한을 받아야 하는데 플래시는 광고에 상당한 자유를 주고 있습니다. 안타깝게도 새로운 보안 모델은 Adobe 사에 의해 플래시 구조에 대대적인 변화가 요구됨에도 Adobe 사는 현재까지는 이런 방어에 별로 관심이 없어 보입니다.

다행히 분산된 발전은 두 가지 가능한 방안을 제시합니다. 첫째 플래시의 "AllowScriptAccess" 태그는 광고 네트워크가 드러나지 않은 공격적인 광고를 방어 할 수 있도록 광고 스크립트를 차단할 수 있습니다.[10] 광고 네트워크는

---

[10] “Using AllowScriptAccess to Control Outbound Scripting from Macromedia Flash.” http://kb.adobe.com/selfservice/viewContent.do?externalId=tn_16494.

이런 속성을 플래시 배너를 페이지에 띄우는 PARAM 이나 EMBED 태그에 놓으면 됩니다. 이런 속성이 제 위치에 있는 한 해당 광고는 밖의 코드를 인용할 수 없으므로 공격이 상당히 많이 줄어듭니다. 어떤 광고주들은 자신의 다양한 미디어는 외부 스크립트가 필요하다고 주장합니다. 하지만 높은 명성과 책임감 있는 행동으로 신뢰를 쌓은 광고주들은 자신의 광고에 스크립트를 운용할 수 있게끔 광고 네트워크를 설득할 수 있는 반면에 일반적인 혹은 잘 알려지지 않은 광고주들은 제한된 명성에 맞는 제한된 허가를 얻을 수 있을 것입니다.

다른 방법으로는 광고 네트워크가 광고를 테스트하여 악성프로그램 설치자를 찾아낼 수 있습니다. 이런 분야에서 제일 유명한 제품은 다양한 장소에서 다양한 컴퓨터를 사용하여 광고를 검색할 수 있는 자동화 시스템인 Right Media 사의 Media Guard 입니다. 이는 Right Media 사가 상당한 비용을 들여 만든 중요한 자동화 기술이었고 매우 힘든 일이었습니다. 하지만 본 시스템은 Right Media 사가 자신의 광고의 속성에 대해 제대로 파악을 할 수 있으며 문제가 발생하지 않는다는 자신감을 주었습니다. 점점 많은 광고 네트워크가 Right Media 사의 시스템을 통해 inventory 를 교환하고 있고 이는 매우 중요한 일이라 할 수 있습니다. 구글도 현재 비슷한 실험을 하고 있으며 exploit 를 광고주의 페이지와 검색결과에 표시를 하고 있습니다. 하지만 소규모의 네트워크를 비롯한 다른 광고 네트워크는 악성광고를 찾아내거나 추적할 수 있는 효과적인 도구가 여전히 부족합니다. 결국 광고주를 제대로 평가하지 못한 네트워크들의 무능함으로 인해 이용자들만 곤란한 상황에 처하게 되는 것입니다.

사기성 광고

30 년 전 브리태니커 백과사전은 끈질긴 판매원이 집집마다 방문을 해서 제품을 판매했었습니다. 소비자들이 권유를 거절할 것이라고 잘 알고 있었기 때문에 소비자들의 이목을 사로잡기 위해서 판매원들이 속임수를 사용하였습니다. 그 후 관련 소송에서 판사가 이러한 속임수를 묘사했습니다.

소비자의 집에 들어갈 수 있는 교묘한 수단 중에 하나가 광고 리서치 분석 설문조사입니다. 이런 설문조사는 판매원의 신분을 숨기며 광고 리서치에 종사하는 직원으로 가장 할 수 있게끔 작성이 되었습니다. 브리태니커는 설문조사에 대해 의심을 가진 사람에게는 홍보담당책임자 명의의 서한을 보여주면서 기만성을 높였습니다. 이런 설문조사는 이후에 아무런 분석작업에 이용되지 않으면서도 판매원에 의해 이용하고 있었습니다.

미국 연방거래위원회는 브리태니커의 판매 방식에 대해 제동을 걸었고,[11] 브리태니커가 연방대법원까지 상고를 했음에도 불구하고 패소를 했습니다.[12] 미국 연방거래위원회는 결국 "문을 열도록 하는 사기행위" 금지 원칙을 확립했습니다. 이 원칙에 의하면 초반의 허위 설명으로 인해 판매원이 소비자에게 부정확한 인상을 심었더라면 해당 사기행위가 매우 심각한 것으로 보아 그 후에 이뤄진 설명으로도 소비자가 착오에서부터 벗어나 정확한 판단을 내릴 수 있는 능력이 없다고 보는 것이었습니다. 이런 원칙을 브리태니커의 판매 전략에 적용한다면 판매원이 나중에 자기의 본래의 신분을 밝혔더라도 초반에 설문조사 분석 직원이라고 주장하는 것만으로 소비자의 구매 "동의"는 무효인 것으로 보는 것입니다.

---

[11] Encyclopædia Britannica, Inc. 87 F.T.C. 421 (1976).

[12] Encyclopædia Britannica, Inc. 445 U.S. 934 (1980).

온라인 배너 광고가 미국 연방거래위원회의 1976 년 브리태니커사건과 매우 흡사하다는 것을 쉽게 알 수 있습니다. 사진 6-2 에서 볼 수 있는 것처럼 설문조사 질문("당신은 조지 부시를 좋아합니까?")을 소비자에게 묻는 광고도 있고 사진 6-3 에서 보시다시피 연예인을 식별("이것은 누구의 입술입니까?")하라는 질문도 있습니다. 이런 질문들에도 불구하고 광고주들은 이용자들이 누구를 선호하든지 누구를 인식하든지 관심이 없습니다. 왜냐하면 그들은 시장조사를 하지 않고 있기 때문입니다. 소비자의 주목을 얻기 위해 "조사"를 진행 중인 것으로 가장한 브리태니커 판매원처럼 이러한 광고들은 단지 광고주가 이용자들에게 전혀 관계없는 마케팅 제안을 받아들이도록 이용자들이 광고에 클릭을 하도록 유도하는 것입니다.

사진 6-2 설문조사 문제

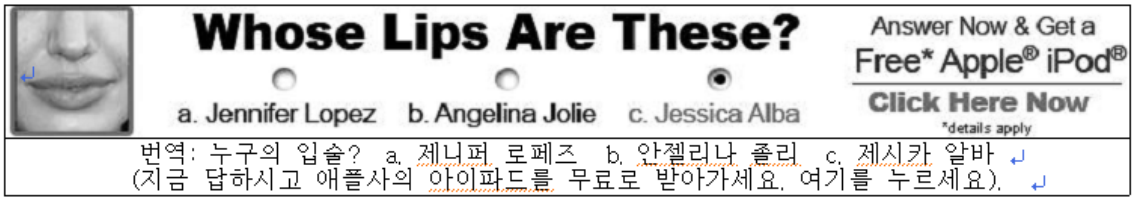

사진 6-3 퀴즈 문제

하지만 "문을 열도록 하는 사기행위" 광고들은 설문조사형 배너 이외인 것도 있습니다. 적지 않은 광고들은 거짓 주장까지 합니다. 광고에서 "벨소리 무료로

받기"라고 해도 "무료"의 반대인 한 달에 $9.99 를 부과합니다(사진 6-4 와 6-5 참조). 혹은 "무료 신용조회" 광고를 생각해보십시오. 하지만 강매하는 서비스는 무료도 아니고 신용조회에 관한 것도 아닙니다. 일반적으로 무료로 받을 수 있는 소프트웨어를 판매한다는 사기 광고도 있습니다. 파이어폭스, 스카이프 또는 윈집 등을 검색해 보십시오. 일반적인 공짜 프로그램을 유료로 제공하려는 광고도 볼 수 있을 것입니다(사진 6-6 참조).

수십 년간의 소비자 보호법에도 불구하고 이러한 사기행위는 여전히 많이 남아있습니다. 그러한 이유 중에 하나는 법상의 모든 조항이 반드시 집행 가능하지 않기 때문입니다. 특히 중요한 조건은 작은 활자로 쓰이면 안되고 명확하고 명료해야 합니다[13](예를 들어 아이스크림은 98% 무지방이라고 하면서 각주로 제품의 지방 함량이 낮지 않다고 적시한 광고에 대해서 사기성이 있다고 미국 연방거래위원회는 결론을 내렸습니다[14]). 하지만 온라인 광고주들은 "무료 전화벨" 혹은 "무료 아이팟을 드립니다"라고 적으면서 작은 글씨로 "세부사항 별도 적용"이라고만 하면 괜찮다고 생각할 때가 많습니다.

---

[13] “FTC Advertising Enforcement: Disclosures in Advertising.” http://www.ftc.gov/bcp/workshops/disclosures/cases/index.html.

[14] Hägen-Dazs Co. 119 F.T.C. 762 (1995).

사진 6-4 무료가 아닌 "공짜" 전화벨

사진 6-5 $7.99 이 부과되는 "무한 무료" 전화벨

사진 6-6 스카이프와 윈집의 판매

다행히 단속자들이 문제를 인식하기 시작했습니다. 예를 들어 미국 연방거래위원회는 "설문조사로 플레이스테이션 3 을 무료로 받으세요"와 “무료 플라즈마 TV 를 고르세요”같은 ValueClick 의 사기성 배너와 팝업에 제동을 걸었습니다. 미국 연방거래위원회는 약속된 상품을 받아가기 위해서는 매우 복잡하고 거의 불가능한 노력과 과정을 거쳐야 한다고 판시했습니다. 이러한 근거로 미국 연방거래위원회는 결국 ValueClick 에게 2,900 만 달러의 벌금을 부과했으며 그러한 행동을 중지할 것을 요청했습니다.[15] 플로리다주 법무장관도 시스템을 통해 사기성 광고를 내보낸 광고 네트워크에게 책임을 지게 하는 등 사기성 전화벨 광고에 대해 부정적인 시각을 가지고 있습니다. [16] 개인

[15] ValueClick, Inc. Case No. CV08-01711 MMM (RZx) (C. Dist. Cal. 2008).

[16] “CyberFraud Task Force.” Office of the Attorney General of Florida. http://myfloridalegal.com/.

변호사들도 도움을 주고 있습니다. 예를 들어 허위광고를 내보내고 방치해둔 구글을 상대로 소송을 거는 일입니다.[17] 또한 EU 소비자 위원은 2008 년 7 월 보고서에서 80% 이상의 전화벨 사이트가 부정확한 가격, 혼동케 하는 청약 또는 부정확한 연락 정보 등을 담고 있었다고 하였습니다. 이 모두 법적대응의 근거가 될 수 있습니다.[18] 새로운 사기성 광고는 날마다 발생하기에 제안 자체가 의심스러울 정도로 좋은 광고에 대해서는 이용자가 항상 주의를 해야 합니다. 의심스럽다면 이용자는 신속하게 웹 검색을 이용하여 해당 사이트 이름을 입력해 다른 사람들의 불만 사항을 확인할 수 있을 것입니다. 사기성 사이트는 개인정보보호 또는 멀리 떨어진 주소를 활용하기에 이용자는 Whois 를 사용할 수도 있습니다. 자동화된 도움이 필요하다면 사기성 광고를 찾아내는 McAfee SiteAdvisor[19]의 도움을 받을 수도 있습니다.[20]

사기성 광고가 과연 "컴퓨터 보안"의 문제입니까? 보안 전문가들이 이러한 문제를 다룰 수도 있겠지만 소비자 보호 변호사들도 많은 도움을 줄 수 있습니다. 하지만 속임수에 빠진 이용자에게는 이런 차이는 그리 중요하지 않습니다. 보안 위협에 대한 방어로서 이용자의 훌륭한 판단이야말로 사기성 광고의 피해를 줄일 수 있는 가장 좋은 방법이기 때문입니다.

피해자가 된 광고주

---

17 Goddard v. Google, Inc. Case No. 108CV111658 (Cal. Super. Ct. 2008).

18 "EU Crackdown of Ringtone Scams." EUROPA Memo/08/516. July 17, 2008.

19 "SiteAdvisor FAQs." http://www.siteadvisor.com/press/faqs.html.

20 Disclosure: I am an advisor to McAfee SiteAdvisor. John Viega, editor of this volume, previously led SiteAdvisor's data team.

온라인 광고에서 발생한 모든 문제들을 광고주에게 책임을 떠넘기고자 하는 경우가 많습니다. 왜냐하면 결국 광고주들의 자금으로 이런 시스템을 작동시키기 때문입니다. 더군다나 광고를 좀 더 조심스럽게 디자인하거나 구매를 할 경우 광고주들은 사기성 광고 상습으로 인한 피해를 줄이는데 큰 역할을 할 수 있습니다.

하지만 광고주들이 피해자라는 생각이 들 때도 있습니다. 광고 네트워크에 의해 광고주들이 과도한 요금을 부과 당하면서도 그들이 대우 받기로 약속한 것보다 훨씬 못 미치는 결과를 얻을 때가 있기 때문입니다.

잘못된 결과

저는 2006 년에 Hula Direct 라는 온라인 광고 브로커를 검사했었습니다. Hula 의 국제영업지점인 Inqwire 와 Venus123 사이트들은 상당히 많은 양의 광고를 띄웠습니다. 한 페이지 당 6 개 또는 더 많은 광고 배너를 띄웠습니다. Hula 는 때로 일부 배너를 다른 배너 뒤에다 위치를 하게 하여 뒤에 위치한 배너가 결국 가려져 있어서 보이지 않는 경우도 있었습니다. Hula 의 사이트가 가치 있는 컨텐츠가 있는 상태에서 다량의 배너를 띄웠다면 이용자들이 용서를 할 수도 있었겠지만 Hula 의 사이트는 광고 빼고는 중요한 정보가 별로 없었습니다. 광고 전문가들은 이러한 웹 페이지를 농장에서 한 종류의 농작물만 심는 것처럼 배너만 생산하는 “배너 농장”이라고 부릅니다.

Hula 의 광고주들은 보통 Cost Per Thousand Impressions(CPM) 방식으로 광고를 구매하였다고 산업 보고서에서 지적하고 있습니다. 즉 각 이용자가 광고를 보았다고 추정되면 광고주들이 일정 수수료(1 센트도 달하지 않은 적은 수수료)를

지불하는 방식입니다. 광고주들은 이런 구조로 인하여 현저한 위험에 처하게 됩니다. Hula 같은 웹사이트가 광고를 대거로 띄워놓는다면 이용자가 인식할 수 없거나, 클릭을 하지 않거나 또는 구매를 하지 않아도 광고주들은 그만큼의 돈을 지불해야 하기 때문입니다. 배너 이외에 아무런 정보가 들어있지 않은 웹 페이지는 이용자의 주목을 끌 수 없기에 여기에 띄운 광고들은 거의 관심을 받기 힘듭니다. 무엇보다도 다른 광고에 의해 가려진 광고들은 전혀 쓸모가 없어집니다(사진 6-7 참조).

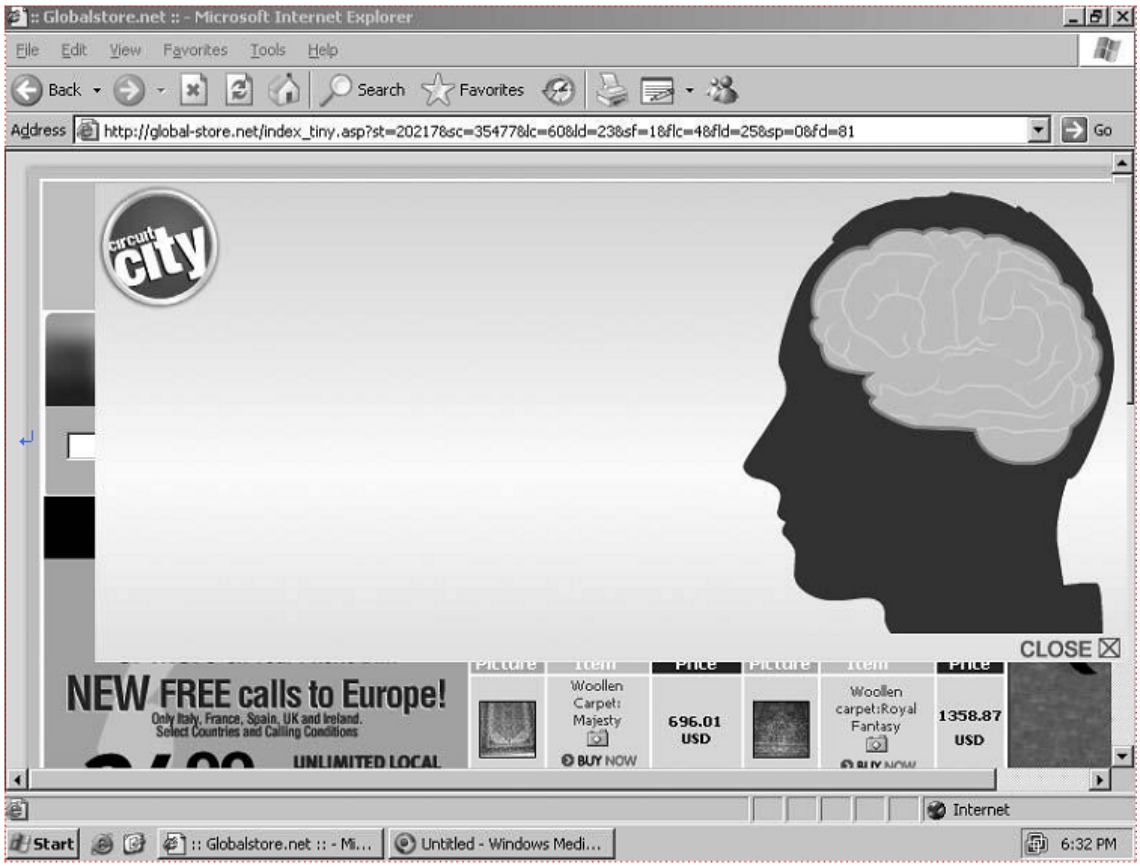

사진 6-7 잘못된 결과: Circuit City 의 큰 팝업은 다른 배너 광고들을 가리고 있습니다.

Hula 의 배너농장은 광고주들에게 과도한 요금을 부과할 수 있는 두 가지 방법을 보여줍니다. 첫째 Hula 는 광고를 이용자가 요청한 적이 없는 팝언더(웹 브라우저가 새로 열릴 때마다 새로운 창과 함께 창 아래로 나타나는 배너 광고로 팝업 광고의 변형된 형태)에 탑재를 합니다. 따라서 Hula 는 아주 많은 광고를 띄웠다고 주장을 할 수도 있고 이러한 광고를 스파이웨어, 애드웨어 혹은 품질 낮은 웹 사이트에서 구매한 저렴한 팝업 창을 통해 광고를 보여줄 수 있습니다. 둘째 Hula 는 광고들이 자주(때로는 9 초에 한번씩) 재로딩 하게끔 광고를 설계합니다. 결과적으로 이용자가 페이지를 계속 읽는 한 광고가 지속될 것으로 믿어 웹 페이지에 광고를 띄우기 위해 광고주가 돈을 지불했지만 Hula 의 배너농장에서는 불과 9 초의 광고만 나옵니다.[21] 다른 사기꾼들은 배너농장에 새로운 방법까지 동원합니다. 예를 들어 창에 1x1 픽셀의 작은 배너를 띄워 광고가 보이지도 않으면서 광고비는 챙기는 수법을 사용합니다. 사기행위가 CPM 을 통해 더 쉽게 이뤄질 수 있기에 다른 조건들이 같다면 광고주는 다른 지불방법을 선호합니다.

사기성 CPM 광고 피하기

CPM 에 대해 불만이 있는 광고주에게 온라인 광고 판매자는 두 가지 다른 선택을 제안 할 수 있습니다. 첫째 광고주는 이용자가 광고를 클릭해야 요금이 부과 되는 CPC(cost per click)를 선택 할 수 있습니다. 다른 방법은 판매가 성공적으로 이뤄질 때 요금을 지불하는 CPA(cost per action)가 있습니다.

---

[21] Edelman, Benjamin. “Banner Farms in the Crosshairs.” June 12, 2006. http://www.benedelman.org/news/061206-1.html.

얼핏 보기에 이런 선택들은 CPM 보다 사기성이 적은 것처럼 보입니다. 어떻게 보면 좀 더 괜찮은 방법일 수도 있지만 실제로는 이러한 방법도 문제를 일으키는 사기성 광고의 원인이 될 수 있습니다.

CPC 광고 이용하기

CPC 광고는 검색 엔진들의 금전적 토대이며 구글의 대부분의 수익도 여기에서 발생합니다. CPC 의 가장 좋은 장점은 고객이 무엇을 사야 할 지 고려할 때 광고주들이 고객에게 접근을 할 수 있다는 것입니다. 따라서 이는 매우 효과적인 마케팅 전략입니다. 하지만 CPC 광고 캠페인은 과도한 요금이 부과됩니다.

독립적인 웹 사이트 제작사가 CPC 판매자와 신디케이션을 체결했다고 가정해봅시다. CPC 판매자는 제작사에게 제작사 사이트에서 광고가 클릭될 때마다 일정한 요금(보통 광고주가 지불하는 금액의 일부분)을 냅니다. 따라서 제작사는 당연히 광고가 많이 클릭 된 것으로 보고를 하고 싶어합니다. 그렇다면 어떻게 할까요? 어떤 제작사는 이용자에게 광고들을 클릭하라고 알려줍니다. ("사이트 지지하기: 광고를 클릭하여 방문하세요.") 다른 제작사는 JavaScript 을 이용하여 이용자가 광고를 방문할 의사와 관계없이 브라우저가 광고를 "클릭"할 수 있게끔 만듭니다.[22] 악의를 가진 제작사는 심지어 좀비 컴퓨터를 일으키는 반복적인 코드를 이용하여 감염된 PC 가 다양한 CPC 광고를

---

[22] Edelman, Benjamin. “The Spyware –Click-Fraud Connection –and Yahoo’s Role Revisited.” April 4, 2006. http://www.benedelman.org/news/040406-1.html.

로드하게 합니다. 이 모든 것이 이용자가 광고를 요청하지도 않았고 심지어 대부분은 광고주의 사이트를 보지도 못한 채 발생합니다.[23]

추적 방법을 속이기 쉽기 때문에 CPC 광고는 이런 공격에 취약합니다. 이용자가 과연 광고를 진짜로 보았는지 CPM 광고 네트워크가 쉽게 확인할 수 없듯이 CPC 판매자도 광고 "클릭"이 유저가 사실상 마우스를 광고에 이동하여 버튼을 눌렀는지 아니면 클릭을 가장한 일정한 코드로 인한 것인지 구별 할 수 없습니다. CPC 판매자는 제작사의 아이디를 포함한 특별한 코드 HTTP 요청이 검색 엔진의 웹 서버에 전송되었을 경우에만 클릭을 추적합니다. 하지만 악의의 제작사들은 이러한 요청을 이용자의 클릭 없이 조작이 가능합니다. 또한 일부 개발도상국에서는 저렴한 요금으로 해당 사이트의 광고를 하루 종일 클릭해주는 서비스마저 존재합니다.[24]

걱정스러운 CPC 네트워크로 말미암아 신디케이션 제휴 대신 자신이 소유한 사이트에만 광고를 보여주는 방법도 있습니다. 예를 들어 마이크로소프트는 2008 년도 중반에 Live.com, 마이크로소프트 사이트, 믿을만한 최상의 파트너를 통해서만 광고를 내보냈습니다. 하지만 이런 전략은 CPC 네트워크의 접근성을 제한하고 네트워크가 광고주에게 제공하는 활동범위를 현저하게 줄여놓습니다. 이와 대비되게 구글은 상반된 방법을 선택했습니다. 구글은 2008 년 2 분기 때 파트너들의 사이트에 광고공간을 확보하기 위해 파트너들에게 14 억 7 천만 달러를 지불했습니다.[25] 이러한 어마어마한 돈으로 구글의 접근성은 향상되었고

---

[23] Daswani, Neil and Stoppelman, Michael. “The Anatomy of Clickbot.A.” Proceedings of the First Workshop on Hot Topics in Understanding Botnets. 2007.

[24] Vidyasagar, N. “India’s Secret Army of Online Ad ‘Clickers.’” The Times of India. May 3, 2004.

[25] Google Form 10-Q, Q2 2008.

이로 인해 잠재 광고주들에게 큰 매력으로 다가왔습니다. 마이크로소프트가 왜 2008 년 7 월에 신디케이션을 더 넓게 개방한다는 계획을 발표했는지 충분히 이해가 되는 대목입니다.[26]

CPC 판매자는 IP 주소, 복제 및 다른 패턴의 감시를 포함하는 허위 클릭 행위를 확인할 수 있는 강력한 방법이 있다고 주장합니다.[27] 하지만 그들의 접근 방식에 대해 확신이 가지 않습니다. CPC 판매자가 확인하지도 못한 것들을 어떻게 알 수 있겠습니까? 컴퓨터 한 대당 한 달에 한 번씩 광고 몇 개만을 클릭하는 영악한 좀비 PC, 정상클릭과 부정클릭의 혼합, 정상적인 모든 HTTP 헤더를 속이고 심지어는 각 광고주들의 사이트에서 몇 페이지 정도만 열람하기까지 하는데 CPC 판매자가 어떻게 방어를 하겠다는 것인지 잘 모르겠습니다. 이러한 허위 클릭이 유효한 클릭과 구별이 잘 안되기 때문에 신디케이션 가담자들은 아무런 제재 없이 추가금액을 받을 수 있습니다.

광고주와의 거래에서 사기클릭을 방지하는데 노력을 하지 않았다는 이유로 구글, 야후 등 대형 검색 엔진을 상대로 2005~2006 년 사이에 집단소송이 있었습니다. 명목적 합의금은 1 억 달러였지만 사실상 광고주에게 돌아가는 실질적 가치는 실제로 적었다고 합니다(하지만 만약 광고주가 소송을 걸지 않았다면 그가 받을 수 있는 합의금은 없습니다). 대형 검색엔진은 합리화를 하기 위한 보고서를 작성하여 부정클릭이 큰 문제가 아니라고 주장합니다.[28] 하지만 근본적인 보안 결함은 바뀌지 않았습니다.

---

[26] Microsoft adCenter Publisher Program (http://advertising.microsoft.com/publisher).

[27] See, for example, "How Does Google Detect Invalid Clicks?" https://adwords.google.com/support/bin/answer.py?answer=6114&topic=10625.

[28] See, for example, Tuzhilin, Alexander. "The Lane's Gifts v. Google Report." June 21, 2006.

부정 클릭으로부터 방어를 하기 위해 광고주는 종종 웹 서버 로그파일을 검토하여 의심스러운 활동을 찾아내는 제 3 자 부정 클릭 탐지 서비스를 이용할 때가 있습니다.[29] 구글은 이러한 서비스 중 다수를 분석상 오류를 이유로 조롱했습니다.[30] (예상대로 구글은 이러한 서비스의 결점은 구글이 그들에게 준 제한적인 데이터 때문이라며 그럴듯한 말로 얼버무렸습니다) 더 나아가 부정 클릭 탐지 서비스가 클릭 후 브라우징이 포함되는 좀비 PC 근거의 부정 클릭인지를 발견할 수 있을지도 의문입니다. 부정 클릭 탐지 서비스의 이러한 한계에도 불구하고 검색 엔진이 요금을 과다하게 부과할 경우 제한적이나마 확인 작업을 진행하여 명백한 부정 클릭 사건들을 몇 개 적발했습니다.

CPA 가격 부풀리기

CPA(Cost-per-action) 광고는 광고주의 사이트에서 이용자가 물건을 구매할 때에만 광고주에게 비용을 부과하기에 사기성이 제일 적은 것으로 알려져 있습니다. 여기에서 중요한 것은 광고를 보는 이용자가 없거나 광고를 클릭한 이용자가 없는 경우 혹은 이용자가 클릭한 후에 구매를 하지 않을 시 광고주에게 비용이 부과되지 않기에 CPA 는 광고주의 위험부담을 줄여줍니다. 따라서 LinkShare 와 Commission Junction 같은 협력 네트워크는 다른 종류의 온라인 광고보다 CPA 의 위험부담이 적다고 이야기를 한 적이 있습니다.[31]

---

http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf.

[29] See, for example, Click Defense (http://www.clickdefense.com) and Click Forensics (http://www.clickforensics.com).

[30] "How Fictitious Clicks Occur in Third-Party Click Fraud Audit Reports." August 8, 2006. http://www.google.com/adwords/ReportonThird-PartyClickFraudAuditing.pdf.

[31] See, for example, "pay affiliates only when a sale…is completed" within "LinkShare –Affiliate

하지만 CPA 라고 해서 사기광고로부터 완전히 자유롭지는 않습니다. 판매자가 물건 주문이 이뤄지는 당일에 수수료를 지불한다고 가정해 보겠습니다. 공모자가 공격자의 CPA 링크를 통해 물건을 구입한 후 물건을 돌려주고 환불요구를 한다고 해도 광고주는 수수료를 지불을 해야 하고 공격자는 환불에도 불구하고 수수료를 돌려줄 필요가 없습니다. 또 다른 방법으로는 승인거절된 신용카드 혹은 입금취소의 확인이 며칠 걸린다면 그 사이에 공격자들은 판매자가 눈치를 채기 전에 수수료를 가지고 도주할 수 있습니다. 큰 규모로 이룰 수 없더라도 이러한 사기행위는 실제로 일어나고 있습니다(현재 발생건수는 예전에 비해 줄었습니다).

더 복잡한 사기 계획에서는 이용자가 링크를 클릭하지 않아도 CPA 링크를 자동적으로 이용하는 웹 페이지 혹은 배너 광고를 공격자가 만듭니다. 그 후 만약 이용자가 해당 판매주로부터 물건을 구입하게 되면 공격자는 수수료를 받게 됩니다. 이를 Amazon, eBay 및 그와 유사한 웹 상에서 가장 큰 판매주들에게 적용을 하면 많은 이용자가 광고에 상관 없이 이 곳에서 물건을 구매하기에 이러한 "효율적인 쿠키"는 높은 수수료 수익을 챙겨갈 수 있습니다.[32] 이는 어마어마한 숫자입니다. 예를 들어 eBay 가 2008 년 8 월에 Digital Point Systems 와 몇 개 회사를 상대로 한 소송에서 볼 수 있다시피 eBay 는 이러한 사기행위가 연방법원에 소송을 걸어야 할 정도로 심각하다고 생각합니다. 해당소송에서 피고인들이 eBay 추적 쿠키를 이용자 컴퓨터에다가 강제적으로

Information." http://www.linkshare.com/affiliates/affiliates.shtml.

[32] See, for example, Edelman, Benjamin. "CPA Advertising Fraud: Forced Clicks and Invisible Windows."http://www.benedelman.org/news/100708-1.html. October 7, 2008.

입력하여 성실한 마케팅 서비스를 제공하지도 않고 eBay 를 광고해주지도 않으면서 eBay 로부터 수수료를 요청했다고 eBay 가 주장했습니다.[33]

유별나게 복잡한 CPA 사기 사건에서는 공격자가 제일 먼저 스파이웨어 혹은 에드웨어를 이용자의 컴퓨터에 입력합니다. 이러한 추적 소프트웨어가 이용자의 브라우징 활동을 계속 관찰한 후 CPA 링크를 이용하여 수익을 올리는 방법입니다. Dell 웹사이트에서 노트북을 구입하고자 하는 이용자의 브라우징 활동이 공격자에 의해 관찰되고 있다고 가정해 보겠습니다. 공격자는 Dell 에 대해 CPA 링크를 열어서 만약 이용자가 Dell 로부터 물건을 구입하게 되면 공격자는 2%의 수수료를 챙겨가게 됩니다. (새로 Dell 을 구매할 고객을 찾으려면 새 Dell 을 사이트에서 찾아 보는 이용자보다 더 좋은 곳이 어디 있겠습니까?) Dell 입장에서 보면 이용자가 CPA 링크를 클릭하여 물건을 구매했기에 전혀 문제가 없어 보입니다. 하지만 Dell 이 모르고 있는 것은 이용자가 아닌 스파이웨어에 의해서 링크가 클릭되었다는 것입니다. Dell 은 이용자가 어차피 노트북을 샀을 것이라는 점에 대한 고려는 하지 못했습니다. 즉 2%의 수수료는 불필요한 것이었고 오히려 낭비였습니다. 하지만 안타깝게도 Dell 의 추적 시스템은 이용자의 컴퓨터에 무슨 일이 일어나고 있는지 알 수가 없어서 Dell 은 이 사실에 대해 전혀 모르고 있는 것입니다. Dell 은 "클릭"행위가 이용자가 아닌 스파이웨어에 인해 이뤄진 것이고 CPA 수수료의 지불 없이도 이용자가 물건 구입을 했을 것이라는 사실을 알 수가 없습니다.

---

[33] eBay, Inc. v. Digital Point Solutions, No. 5:08-cv-04052-PVT (N.D. Cal. complaint filed Aug. 25, 2008).

지난 4 년 동안 저는 이러한 방법을 이용하여 가짜 CPA 가입자를 만든 경우를 수백 건 찾아냈습니다.[34] 그렇게 많은 사기행위들을 일일이 수동으로 문서화하기에는 제 능력이 부족해서 작년에 사기행위를 스스로 찾아낼 수 있는 자동화 시스템을 제작했습니다. 제 소프트웨어는 스파이웨어로 감염된 가상의 기계로 웹을 브라우징하면서 예기치 않은 CPA "클릭" 사건들을 확인하여 packet logs 와 screen-capture 비디오로 이러한 조사자료를 보존합니다.[35] 요즘에도 매일 새로운 사기꾼을 종종 발견하고 있고 저 말고도 많은 사람들이 이러한 사기꾼들을 발견하고 있습니다. 그 좋은 예가 ValueClick 을 상대로 한 집단소송에서 판매자들은 지불할 필요도 없는 CPA 수수료의 반환청구를 한 사건입니다.[36] 최근에 발표된 합의로 끝난 사건에서는 공격자가 수수료 쿠키를 중복으로 덮어 써서 수수료를 잃어버린 판매자에게 100 만 달러의 부당이득을 반환해야 했습니다.

왜 광고주들은 더 강력하게 투쟁하지 않는가?

수년간의 온라인 광고 감사를 통해 많은 광고주들이 사기행위를 해결하는 것이 중요하다고 느끼지 않고 있음을 알게 되었습니다. 물론 사기행위로 인한 손해를

---

[34] See Edelman, Benjamin. "Auditing Spyware Advertising Fraud: Wasted Spending at VistaPrint." http://www.benedelman.org/news/093008-1.html. September 30, 2008.
See also "Spyware Still Cheating Merchants and Legitimate Affiliates." http://www.benedelman.org/news/052107-1.html. May 21, 2007.
See also "How Affiliate Programs Fund Spyware." September 14, 2005. http://www.benedelman.org/news/091405-1.html.

[35] Edelman, Benjamin. "Introducing the Automatic Spyware Advertising Tester." http://www.benedelman.org/news/052107-2.html. May 21, 2007. U.S. patent pending.

[36] Settlement Recovery Center v. ValueClick. Cen. Dis. Calif. No. 2:07-cv-02638-FMC-CTx.

받아들이지 못하는 중소 광고업체나 공정하고 윤리적인 영업을 중요시하는 대형 회사처럼 예외가 있습니다. 그럼에도 불구하고 사기행위로 인해 큰 손해를 입는데도 불구하고 다수의 대기업들은 별로 신경을 쓰지 않고 있습니다.

마케팅 담당자들은 사기 광고는 사업을 하면서 일종의 피할 수 없는 비용이라고 합니다. 저에게는 말도 안 되는 소리로 들립니다. 어떤 사기행위에는 제재를 가해야 하고 어떤 사기행위는 피할 수 없는 경영비용이라는 것을 누가 결정하는 겁니까? 저렴한 가격으로 사기행위를 찾아내고 피하는 등 효과적인 대응방법을 찾아낸다면 "피할 수 없는" 비용을 더 큰 순익으로 전환하여 진정한 경쟁력을 갖출 수 있다고 생각합니다. 하지만 이러한 경우를 찾아보기 힘든 바 제 생각에는 광고회사 직원에게 돌아가는 혜택이 없기 때문인 것으로 보입니다.

온라인 광고를 구입하는 회사에서는 직원 개개인에게 주는 보너스로 인해 사기광고로부터 회사를 보호하려는 노력에 방해를 줄 수 있습니다. 회사 공급자가 회사에게 수천 달러의 과도한 요금을 부과한 사실을 알게 된 광고 매수인을 생각해봅시다. 회사 자문이나 경영자에게 이 사실을 알리는 등 광고구매자가 이 문제에 대해 바로 추궁하는 것이 회사입장에서는 제일 좋을 것입니다. 하지만 이 문제가 직급이 높은 경영자에게 알려질수록 그러한 회사 공급자의 사기행위가 밝혀지기 전에 자기가 공급자에게 몇 개월 동안 돈을 지불했다는 사실, 즉 결국 자기 실수를 인정할 수 밖에 없을 것입니다. 광고 구매자와 이야기를 해 본 결과 이런 실수를 인정하는 것에 따른 부끄러움이 상당히 큰 것으로 파악되었습니다. 광고 구매자는 이런 문제를 더 빨리 알아내고 찾았어야 했는데 하며 본능적으로 스스로를 자책하거나 잘못된 일을 숨기려는 경향이 있습니다.

또 다른 심각한 상황은 어떤 광고주들은 구매자들이 사기사건을 문제삼지 않도록 구매자들에게 보상을 합니다. 회사 총 온라인 광고 지출 비용의 10%를 지불받은 광고 구매자가 있다고 가정해 보겠습니다. 이런 광고 구매자는 부정한 경로를 통해 온 광고를 거절할 이유가 별로 없습니다. 왜냐하면 회사가 1 달러를 지출할 때마다 광고 구매자는 10 센트의 수익을 올릴 수 있기 때문입니다. 이러한 보상은 외부사람들이 생각 하는 것보다 훨씬 많습니다. 그리고 광고주들은 이러한 방법으로 외부 광고 에이전시에게 보상을 합니다.

내부 광고 구매자들에게는 그러한 동기가 더 클 수도 있습니다. 예를 들면 어느 CPA 프로그램 매니저는 연봉 5 만 달러를 받으면서 연 CPA 프로그램 성장의 20% 비율을 보너스로 추가로 받는다고 가정해 보겠습니다. 만약 프로그램을 50 만 달러에서 80 만 달러로 성장시켰다면 매니저는 6 만 달러의 보너스를 받는 셈입니다. 하지만 만약 매니저가 5 만 달러의 사기를 적발하면 매니저는 1 만 달러의 보너스 감소를 겪습니다. 이것은 가장 헌신적이고 성실한 직원에게도 가혹한 결과입니다. 이는 왜 수많은 특수 프로그램들을 통해서도 사기 및 부정행위를 퇴치할 수 없는지 잘 알려줍니다.

비슷한 동기 때문에 광고 네트워크가 파트너, 협력자, 신디케이터를 감독하는데 어려움을 겪고 있습니다. 광고 네트워크가 일부 분야의 사기 또는 부정을 인정한다면 관련 비용을 청구하지 못하고, 그만큼의 감소분은 감수해야 합니다. 반면 문제를 숨기거나 부인을 하면 광고 네트워크는 높은 비용을 그대로 유지하면서 청구할 수 있습니다. 물론 큰 문제는 영원히 숨길 수는 없겠지만 해당 사기 또는 부정을 늦게 인정하는 만큼 광고 네트워크가 단기적 이익을 챙길 수 있습니다.

조달 분야에서의 교훈: 온라인 조달의 특별한 시험

커다란 회사들은 필요 물품 조달시 보통 내부관리가 강한 조달부서를 설립합니다. 유명 제조업체들의 공급망에서의 감독행위를 생각해보겠습니다. 제대로 훈련 받은 회사직원들이 합법성과 완전성을 확인하기 위해 꼼꼼히 공급자를 평가할 것입니다. 온라인 광고에서는 회사들이 더 큰 공급 네트워크를 발전시켰습니다. 예를 들어 적어도 수 만개의 사이트가 구글의 AdSense 서비스에다가 광고 목록을 팔고 있습니다. 그런데도 불구하고 광고주나 광고 네트워크는 제작사를 평가하는데 엄격한 기준이 없습니다.

온라인 광고의 2 가지 측면에서 온라인 광고 조달이 다른 분야에서의 조달보다 힘든 상황을 만듭니다. 첫째 광고 중개자는 그들이 광고를 어디에 올렸는지 공개를 하지 않으려고 합니다. 경쟁사에 그들의 파트너를 빼앗길까 봐 네트워크들은 보통 그들의 광고 퍼블리셔 리스트를 공개하지 않습니다. 그래서 결과적으로는 광고주가 예를 들어 구글의 AdSense 혹은 ValueClick Media 에서 구매를 하더라도 어느 사이트가 개입했는지 알 수가 없습니다. 즉 광고주는 파트너 사이트를 확인할 수 없기에 그들의 적절성과 적법성을 검사할 수 없습니다.

더군다나 규정을 위반한 제작사가 적발되다 하더라도 제작사가 다른 이름 또는 URL 을 재등록하는 것을 막을 수 있는 방법이 별로 없습니다. 때문에 온라인 광고주들은 규정을 위반한 사람들을 적발하더라도 그들을 막는 데에 한계가

있습니다. 제가 쓴 “지불 지체를 통한 온라인 사기 광고 제제"[37]라는 제목의 보고서에는 다른 방법을 제안했었습니다. 사기행위를 저지른 광고 퍼블리셔가 적발되면 해당 퍼블리셔는 2~4 개월의 대금지급 연기와 같은 일정한 금전적 손해를 보아야 한다는 내용입니다. 하지만 지금까지는 대부분 광고주들은 날짜보다 더 빨리 지불을 하기에 퍼블리셔들의 제재의 위험부담 없이 사기행위를 계속하고 있습니다. 그리고 광고주들은 지불을 제 때 하게 되면 사기행위가 밝혀졌을 경우 아무 조치를 취할 수 없다는 것을 깨닫지 못한 채 빠른 지급을 관행이라고 생각하고 있습니다.

온라인 광고에 책임 부과

온라인 광고는 계속 험난한 곳으로 남아 있을 것입니다. 이용자는 믿어서 안 되는 광고들을 보게 되고 기업들은 약속된 것을 받지도 못하면서 광고를 위해 초과금액을 지불해야 합니다. 하지만 꼭 이래야만 하는 것은 아닙니다. 공공기관에 의한 단속은 장기적으로 지속된 소비자 보호법이 온라인에서도 광고주와 광고 네트워크에게 적용됨을 보여주고 있습니다. 그리고 광고주들이 더욱 현명해지면서 그들이 받을 수 없는 불확실한 서비스에 대해 책임지지 않으려고 하는 경향이 나타나고 있습니다.

온라인 광고는 창의적인 소프트웨어 개발자, 반드시 범인을 찾아내겠다고 의지에 불타있는 수사관과 공공을 위해 일을 열심히 하는 공무원 등 여러 분야에 관심이

---

[37] Edelman, Benjamin. “Deterring Online Advertising Fraud Through Optimal Payment in Arrears.” February 19, 2008. http://ssrn.com/abstract=1095262.

있는 자들에게 무한한 기회를 주고 있습니다. 여러분 모두 좋은 일을 하면서 번성하셨으면 좋겠습니다. 그 과정에서 사기꾼들도 잡으면 더 좋겠고요.