



A Security Paper by GeoEdge

The Vulnerabilities in Native Advertising

About Us

GeoEdge is the premier provider of ad security and verification solutions for the online and mobile advertising ecosystem. The company ensures high ad quality and verifies that sites and apps offer a clean, safe, and engaging user experience. GeoEdge guards against malware (malvertising), non-compliance, inappropriate content, data leakage, operational, and performance issues.

Leading publishers, ad platforms, exchanges, and networks rely on GeoEdge's automated ad verification solutions to monitor and protect their ad inventory. To find out how GeoEdge can enhance your quality assurance and verify your online and mobile campaigns, head to www.geoedge.com.

A Critical Look at the Ethics, Technology and Security of Native Ads

Although the industry has historically struggled to cope with the effects of malvertising, the security implications of native advertising are being largely overlooked. Security concerns are being placed on the back burner, but we are here to shine a spotlight on them.

Introduction

In 2013, in a move aimed at countering sagging CPMs to engage better with a more sophisticated and selective audience, publishers and brands turned to native advertising. The new format, which typically mimics the form and function of the environment in which it appears, emerged as a powerful tool to drive revenue and improve the user's engagement experience.

However, as publishers soon found out, native advertising is a controversial and murky business. There are major issues that need to be addressed with native ads, from user security to ambiguity and proper disclosure. Critics believe this form of "disguised advertising" hurts the industry in the long term and adds significant Internet and computer security concerns.

The U.S. Federal Trade Commission (FTC) joined in the discussion by setting guidelines for native advertising, yet the debate about the advantages and disadvantages of native advertising continues. Nevertheless, it's clear that big-name brands and publishers continue to use the format heavily to push promoted videos, images, articles, commentary, music and various other media.

In this paper, we will cut through the hype surrounding native advertising, explain the ethical issues around proper disclosure and user privacy, and zoom in on some major web and computer-security concerns that are being overlooked. We will also present recommendations to help publishers improve their security posture through prevention and mitigation.

A Native Advertising Primer

Much like product placements (embedded marketing), native advertising is meant to mimic the form and function of the publisher's environment. The goal is to deliver paid ads that are so integrated into the page content, assimilated into the design, and consistent with the platform's behavior that viewers simply feel that it belongs and engage with it more seamlessly. In point of fact, research shows that customers prefer native ads and interact longer with them than with display ads. The more relevant the content for the user, the happier the user is.

At least six types of ad units are used – and heavily supported – in native advertising:

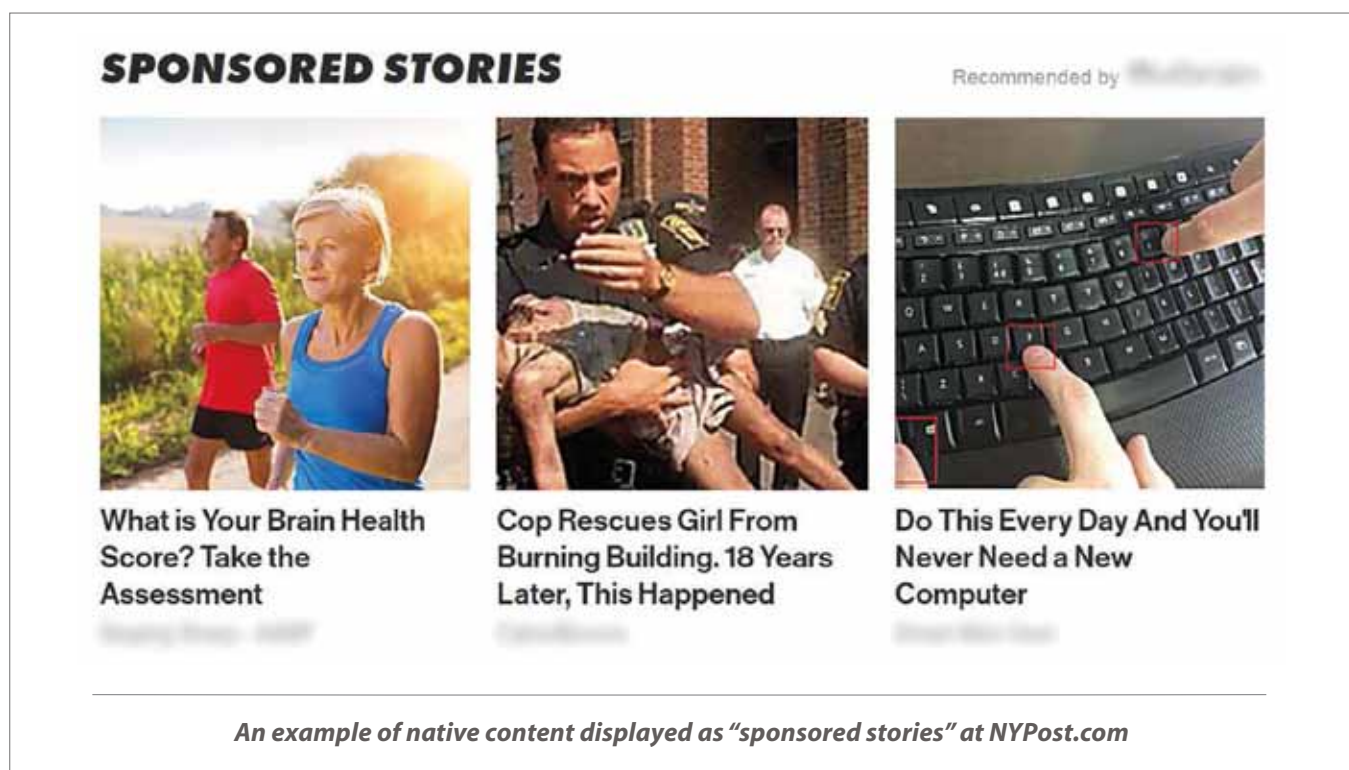
- **Social in-stream units:** Examples include Twitter's Promoted Tweets, Facebook's Sponsored Posts and Pinterest's Promoted Pins.
- **Paid search units:** The first few search results in Google, Bing, Yahoo, Ask.com are paid advertisements marked as "ad."
- **Recommendation widgets:** Driven by Outbrain, Taboola and Gravity, these often appear at the bottom of a web page displayed as "From around the web" or "You may also like..."
- **Promoted listings:** Examples can be found on Google, Amazon and FourSquare.

- **In-ad units:** These are used by Federated Media, Appssavvy and Martini Media, for example.
- **Custom units:** Spotify, Pandora, Hearst and Tumblr use custom units.

Whereas product placements (embedded marketing) place the product within the content, native advertisement seeks to merge the product and the content. On high-traffic web properties like The Huffington Post, Yahoo.com, AOL.com, NYPost.com and NBCNews.com, it's normal to see native ad units camouflaged as related news stories or "what to read next" content from around the web.

Because of this merger of advertising and content, displayed within the same publishing environment, there have been questions about the legal status of native advertising. Even among its practitioners, there is no consensus on the true value of native content. Some ad executives do not consider it advertising, and editorial departments go to great lengths to make sure it is not seen as editorial content.

This has led to a major debate about the legalities and ethical issues in a situation in which the lines are murky for the reader or consumer.




An example of native content displayed as "sponsored stories" at NYPost.com




Ethics and Disclosure

Clearly concerned that native advertising may be crossing the church-state separation between editorial and advertising content, the FTC got involved and held a workshop on advertorials.

In April 2016, it released a guide for native advertising that stressed the importance of consistent disclosure tags like "Ad," "Advertisement," "Paid Advertisement" or

"Sponsored Advertising Content." The commission also called attention to the shady use of tags like "Promoted Content" or "Partner Content" and called for the use of signifiers – different font colors, shading, audio disclosures – to clearly distinguish sponsored content from editorial content.

Sponsored Links by 

		
Animal Emerges from Sea, Isn't Friendly at All	Mom Thought She Had Stuffy Nose Until This Came Out	The Spice That's Healing Powers Date Back Thousands of Years

Native advertising appearing on CBSNews.com

Even with the FTC's involvement, the ethical and disclosure issues remain on the front burner. In August 2016, the non-profit Online Trust Alliance (OTA) found that web publishers were not properly marking native ad units, confusing web readers and essentially hurting the emerging advertising format.

The OTA examined 100 well-known news websites and found that 69 percent contained some form of native advertising, which was defined as "content that is funded and produced outside the publisher's editorial review or influence, yet is designed to appear similar or homogenous to editorial."

Technical Implementation (How It Works)

The creation and display of native advertising is a complex undertaking. It involves multiple technological layers to create the advertising content, set up parameters for targeting and run the content through platforms for pricing and bidding.

Even before the ad is served to the end user, an advertiser must use technology to handle geolocation

More worrying for the online ad industry, the OTA found that 71 percent earned "failing scores" for disclosures, delineation and discoverability, meaning that they did not provide consumers the ability to easily discern editorials from ads.

This distrust has pushed web surfers to use ad-blocking software on both desktop and mobile platforms. The Interactive Advertising Bureau (IAB), a trade group that represents the interests of the online ad industry, has estimated that about a third of U.S. Internet users employ ad blockers and 17 percent are "at risk" to begin using them.

targeting to reach users by country, state/province or city. Targeted native ads also allow the advertiser to choose the context of the page where ads will run and the types of devices (narrowed even to mobile operating system) and behavioral targeting that will push the ad to specific web surfers based on their browser or search history.

There are several categories of native advertising platforms:

- **Closed platform:** The most common is the “closed platform,” which is created by brands to promote their own content on their own websites. Advertisements seen on these platforms are designed to exhibit ad units within the confines of the website's specific agendas. Well-known examples of closed platforms include Promoted Tweets on Twitter, Sponsored Stories on Facebook and TrueView Video Ads on Google's YouTube.
- **Open platform:** This type of platform involves the pervasive promotion of the same piece of branded content across multiple platforms, but through some variation of native ad formats. Unlike closed platform content, open platform content itself lives outside any particular website that it appears on and is usually distributed across multiple sites by a third-party company. This means that most advertisements appearing on open platforms are placed there by an advertiser.
- **Hybrid platform:** With this category, the content publishing platforms can install a private marketplace

where advertisers have the option to bid on the inventory of ad space, either through direct sales or programmatic auction through real-time bidding (RTB). This means that advertisements distributed on hybrid platforms are placed there by the platform itself, the space having been sold to an open platform advertiser.

The majority of native ads are generated by reputable agencies and can be tailored to keep the ad unit within the publisher's website or serve the ad to a third-party landing page.

The native ad unit is powered by a script that is generated to handle all the targeting parameters. What is most important to understand is that the data within the “related content” or “news from around the web” is hosted in ad servers belonging to the publishing platform's ad servers.

This has major security implications, since the publisher has essentially outsourced control of content hosted on its site. In addition, there are significant risks involved when publishers take security into their own hands and struggle to cope with the epidemic of malvertising.

Security and Malvertising Risks

Unfortunately, the technical implementations of native advertising are largely overlooked by an industry that has struggled to cope with the deluge of malvertising attacks over the years. The new format relies on scripts to handle delivery and targeting, and these introduce a wide range of security risks that need to be addressed.

The current security problems are already severe. The IAB estimates that fraudulent impressions, infringed content and malvertising cost the U.S. digital marketing, advertising and media industry \$8.2 billion annually. The IAB blames badly designed business processes and flaws in the digital advertising supply chain for the skyrocketing losses.

Malvertising exposes web users to unknown or potentially dangerous third parties, and according to IAB estimates, losses from this threat surpassed \$1 billion in 2015, with \$781 million of this amount generated from ad blocking implemented due to security and malware concerns. The costs associated with investigating, remediating and documenting direct incidents of malicious advertising total \$204 million, the IAB warns.

When publishers use native ads powered by third-party agencies, they basically are ceding control of their property to outsiders and could be serving malware if a hacker successfully executes a malvertising campaign.

Malicious Post-Click Infections

While native ads have been shown to be low risk for malvertising pre-click, there is a high risk in the post-click, specifically in the landing page, which may be infected with malware. How could a native ad direct a user to a malicious landing page? This can happen when the final landing page is hacked, when a poisoned script is inserted into the delivery path to redirect the user to a different landing page, or when the whole campaign, including the ad, was designed by the cybercriminals themselves.

Landing Page Hijacking

Cybercriminals can employ automated tools to discover third-party landing sites used in native ad campaigns and hijack those pages. Popular platforms like WordPress are known to have vulnerabilities. Many of these types of platforms are unpatched, so it is relatively easy for a cybercriminal to use off-the-shelf exploits to take control of the landing site. Once this happens, the site silently serves malware without the knowledge of the publisher or the reputable ad network.

Delivery Path Corruption

Because native advertising units are basically scripts created to handle delivery and targeting, it is relatively easy for malware purveyors to insert third-party scripts and codes into native ads. Malicious actors hijack the delivery mechanism to serve scripts and use poisoned JavaScript to redirect users to sites hosting viruses, Trojans, spyware and ransomware. This is a threat closely associated with both closed and open platforms (see section above) that use third-party networks to handle the creation, targeting and distribution of native ads.

Landing Page Dirty from the Get-Go

Cybercriminals have been known to actually create an ad campaign with clean content and its corresponding landing page, then use content recommendation platforms to buy traffic. Since the content is clean, it passes the vetting process. Then, once the campaign is successfully running, the cybercriminal activates the malicious code in the landing page to infect the user. (See diagram 1 below.)

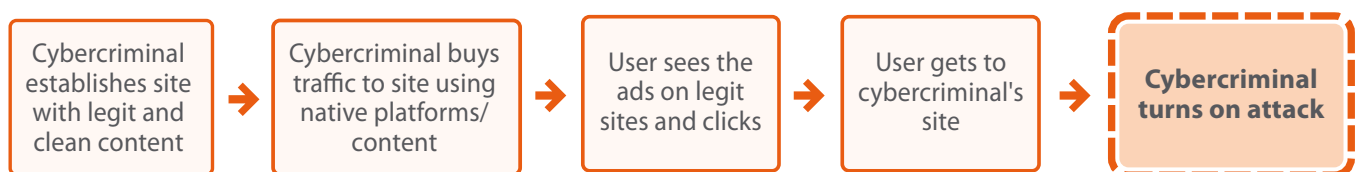
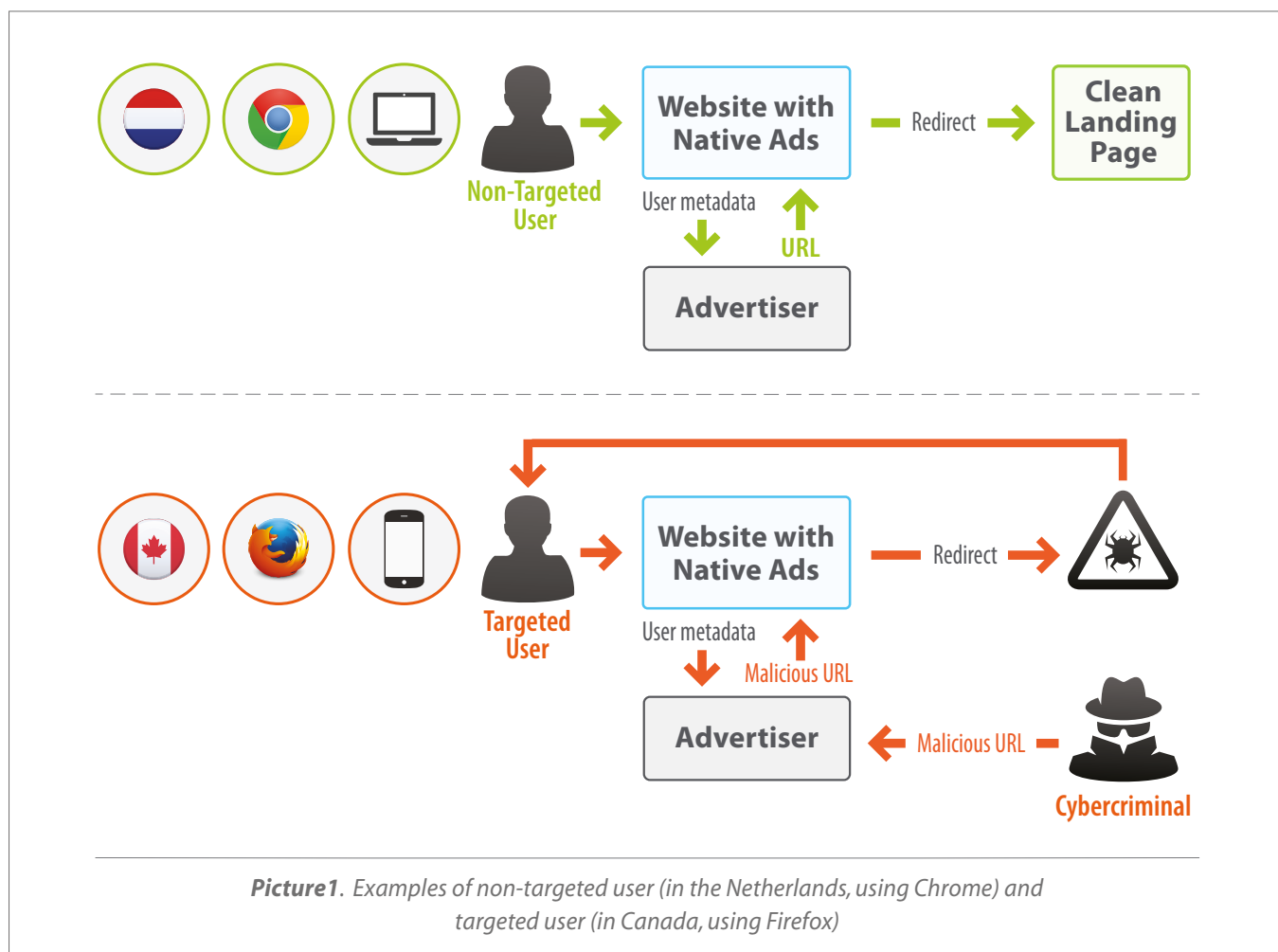


Diagram 1. Attack via cybercriminal's site

Often, the attacks are target-specific, for example, by geolocation or device. The landing page that was approved is still available and accessed by certain users, while other users, who fit the cybercriminal's profile, are directed to the malicious version of the landing page. For example, the cybercriminal decides that anyone coming from the United States or Canada with an iPhone 4 is ideal for infection. The native ad campaign will be clean for every user except those fitting the targeting criteria. (See picture 1 below.)



Native Ad Malware Protection

GeoEdge stands ready to prevent post-click malware in your native ads. We already work with leading content recommendation platforms and have developed agile technology that continuously scans native ads and their landing pages. Dynamically changing landing pages and malicious campaigns targeting certain users are detected and stopped. With GeoEdge, users are protected from malicious native ad campaigns.

Conclusion

The ad tech industry is looking to perfect a more targeted, more robust, more intelligent solution for users. Native advertising, when properly protected and implemented with adequate disclosure and church-state separation, can be a powerful tool for publishers and brands. However, it's important for publishers and native advertising platforms to fully understand the security implications. Post-click malware puts site visitors and end users at risk.

The industry needs to take a closer look at native advertising and its parameters to make sure the next big malvertising attack doesn't come from native. In the meanwhile, you can turn to GeoEdge to keep your site and your users protected.