Following the Money II: The Role of Intermediaries in Adware Advertising

CENTER FOR DEMOCRACY & TECHNOLOGY

A Report by the Center for Democracy & Technology (CDT)
August 2006

Note: There are many different forms of advertising display software. This report focuses on a particular form we call *nuisance and/or harmful adware*. This form of adware may be deployed without appropriate user consent; may be a nuisance and impair productivity; may display objectionable content, can slow users' computers down or cause crashes and loss of data; may not provide users with adequate removal tools; and may be associated with security risks.

Executive Summary

Potentially harmful advertising software has grown from an annoying computing issue into a serious computer security risk. Well-known companies are helping to spread this unwanted adware, often unwittingly, by paying to have their ads displayed by nuisance or harmful adware programs. Many high-profile companies are unaware of this problem because the chain of intermediaries involved in moving ads from marketers to adware applications can be incredibly complex.

We distinguish three different types of intermediaries: affiliate networks, ad networks, and ad-serving platforms. Although affiliate and ad networks operate differently, both contribute in similar ways to the problem of funding nuisance and harmful adware by facilitating the matching of ads to ad space and taking a cut of the ad revenue generated in the process. Ad-serving platforms, meanwhile, merely provide the technology needed to track ads, and thus do not contribute financially to nuisance and harmful adware.

In order to help marketers, ad agencies, and intermediaries gain a better understanding of the online advertising marketplace, CDT conducted a study in which we collected 380 ads served by Zango and Direct Revenue, two adware makers that we believe have engaged in unfair and deceptive practices. We found that 73 intermediaries were involved in displaying these ads, and these intermediaries together made a total of 280 appearances across all the ads. Our analysis revealed the following:

- **55 percent of ads used no intermediaries at all, and an additional 5 percent used only an ad-serving platform,** indicating in those cases that the marketers most likely had direct relationships with the adware makers. This number was higher than expected, in part because CDT's previous study focused on higher-profile marketers that tended to use multiple intermediaries.

- **Another 20 percent of the ads involved only a single intermediary,** in which case the marketers may have been aware that their ads were appearing in these adware programs.
- **Several of the intermediaries that appeared most often in our study are also some of the industry's largest.** Intermediaries that work with thousands of marketers and tens of thousands of affiliates may be more likely to end up in adware advertising chains, but regardless of their size or complexity, there are steps that they can take to limit their involvement with nuisance and harmful adware.
- **Ads for high-profile brands (those familiar to most consumers) tended to use more intermediaries than the ads overall.** High-profile brand ads averaged 2 intermediaries, while the overall average was 0.7.
- **8 percent of the ads we found were *self-targeted*, where the ad that pops up is the same as the page that the user was already visiting.** Self-targeting is often a sign that marketers are getting bilked by their intermediary or adware partners. High-profile brands were much more likely to be the victims of self-targets than less familiar brands.

In light of these findings, CDT recommends that marketers, ad agencies, and intermediaries:

- **Establish and enforce ad placement policies.** Having a policy that explicitly states which ad placements are considered acceptable will provide a standard to which all advertising partners can be held.
- **Require all advertising partners by contract to adhere to those policies.** All partners must also require their partners to include these ad placement terms in *their* contracts with *their* partners, essentially forcing the contractual bind all the way down the advertising chain.
- **Monitor ad placements and flag policy violators.** Hands-on testing, private brand protection services, and/or third-party monitoring should be used to ensure that partners who violate the terms of their agreements can be identified and punished.
- **Research potential advertising partners.** Marketers, ad agencies, and intermediaries should gain as much information as possible about (a) the identities of other intermediaries their potential partners work with and (b) the quantity of other intermediaries their potential partners use.
- **Stay as informed as possible about the parties who are actually displaying the ads.** The more that is known about specific locations where ads are appearing, the less time will be spent worrying about having ads show up unexpectedly in nuisance or harmful adware.
- **Increase transparency in ad placement models.** Intermediaries that actively avoid nuisance and harmful adware should be anxious to explain to marketers how their systems work as proof that they can be trusted to protect brand integrity.
- **Work with each other and industry groups to establish best practices and share information.** The IAB, NAI, DMA, and AAAA are all good vehicles for convening parties in the online advertising space around a set of best practices for both ad placement and transparency.

1 Introduction

Unwanted advertising software has evolved from an annoyance into a serious threat to the future of Internet communication. Every day, thousands of Internet users are duped into downloading nuisance or harmful adware programs they neither want nor need.[1] Once installed, the programs bog down computers' normal functions, deluging users with pop-up advertisements, creating privacy and security risks, and generally diminishing the quality of the online experience. Some users simply give up on some functionality of the Internet altogether after their computers are rendered useless by the installation of dozens of unwanted programs.[2]

In a March 2006 report, *Following the Money: How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend*,[3] CDT showed how well-respected companies are helping to fund the virulent spread of unwanted and potentially harmful adware by paying for advertisements generated by those programs. The report described how the involvement of a complex chain of intermediaries in an advertisement's journey from its original source to a user's computer may cause legitimate advertisers to lose track of where their ads are being displayed. This confusion can result in legitimate advertisers' ads appearing in illegitimate adware. While the first *Following the Money* report dealt with the general complexities of the adware business model, this report focuses on the specific portion of the chain involved in moving ads and payments from marketers to adware applications.

Marketers looking to advertise online face a bewildering array of choices. Not only are there an incredible variety of locations in which to advertise (in banner ads, alongside search results, or in third-party software, for example), but also a huge diversity of means for conducting ads to these locations. A crop of new companies has emerged to serve as intermediaries between marketers and the customers they are trying to reach. While some marketers may continue to favor buying ad space directly, and others may use this wealth of choices to their advantage, this diversity also contributes to the unwitting growth of nuisance and harmful adware. With little in the way of industry self-regulation, marketers are left without clear guidance to judge which intermediaries can be trusted.

In this report, CDT seeks to help marketers, Internet companies, and the general public gain a better understanding of the online advertising marketplace and how ads end up in nuisance and harmful adware programs. Section 2 provides an in-depth description of how an advertisement may travel from a marketer to an adware program. Section 3

---

[1] Our definition of nuisance and/or harmful adware – as presented on in the note on page 1 of this report – is based on the Anti-Spyware Coalition definitions of spyware (and other potentially unwanted technologies) and unwanted advertising display software. See http://antispywarecoalition.org/documents/DefinitionsJune292006.htm and http://antispywarecoalition.org/documents/GlossaryJune292006.htm.

[2] Susannah Fox, *Spyware: The threat of unwanted software programs is changing the way people use the internet*, Pew Internet and American Life Project (Jul. 6, 2005) at http://www.pewinternet.org/PPF/r/160/report_display.asp.

[3] Available at http://www.cdt.org/privacy/20060320adware.pdf.

explains the results of a recent CDT study of the ads generated by two well-known deceptive adware programs. Section 4 provides CDT's recommendations to marketers, ad agencies, and intermediaries on how to avoid advertising in nuisance and harmful adware, and Section 5 provides a conclusion.

2 An Advertisement's Journey

In some cases, the journey that an advertisement takes from a marketer to an adware program is straightforward. The marketer makes a direct arrangement with the adware company, paying the adware maker each time a user clicks on one of the marketer's ads. As the results of our study show, many marketers do use this kind of direct arrangement. For the rest, however, the journey that their ads take may be far more complex, often involving a host of other parties and business models.[4]

To aid our discussion of the variety of parties and business models that may be used, CDT has worked with industry experts in developing the terminology below.[5] An updated, standard set of definitions has not yet been adopted across the online marketing industry. Our terminology is not meant to be a comprehensive set of definitions to describe all online advertising, but rather a subset of terms that we use to clarify concepts within this report.

2.1 Terminology

Ad agency
A business that handles the advertising needs of other companies. In this report we will refer to them simply as *agencies*. The amount of oversight that a marketer has over its agency varies – some marketers provide substantial guidance about how they want their campaigns to be run, while others leave the decision-making to their agencies. Marketers most often pay agencies a specific percentage of what they spend on their advertising overall, although other pricing models are sometimes used. Larger marketers are more likely to use agencies than smaller ones.

Ad-based payment
Payment directly correlated to the display of ads. This transfer of money may occur based on a variety of different pricing models, such as CPM, CPA, or revenue sharing (defined below). However, this term does not cover payments for services not directly correlated to the display of ads (e.g., money paid for tracking services or for the use of ad-serving technology).

---

[4] Previous work by spyware researcher Ben Edelman pioneered the effort to shed light on the workings and complexity of adware advertising. See *Intermediaries' Role in the Spyware Mess* (May 28, 2005) at http://www.benedelman.org/news/052305-1.html.

[5] Our terminology is based in part on entries from the Internet Advertising Bureau's *Glossary of Interactive Advertising Terms* available at http://www.iab.net/resources/glossary.asp.

Ad inventory
The ad space available for sale at a particular online location.

Affiliate
An individual – or, less frequently, a business – that agrees to feature an online ad designed to drive traffic to a particular Web site. In return, the individual receives compensation based on the traffic generated by the ad.

Impression
The display of an ad at an online location.

Intermediary
An entity that sits between a marketer or agency and the party that eventually displays the marketer's ad. Intermediaries can be grouped into three categories:

> *Ad network*
> An aggregator or broker of advertising inventory for many online locations. Ad networks are sales representatives for the online locations within the network. Smaller locations that do not have the resources necessary to maintain their own sales teams can join ad networks in order to compete with more established sites for ad content. Ad networks generally operate on a CPM basis, although other pricing models are sometimes used.
>
> *Ad-serving platform*
> A business engaged in the delivery of ads by a server to an end user's computer on which the ads are then displayed or cached. Ad-serving platforms provide the technology used to deliver ads.
>
> *Affiliate network*
> An intermediary that provides services to broker advertising offers between marketers or agencies and affiliates. Marketers and agencies use affiliate networks to find new outlets for their ad content, while affiliates use them to find profitable advertising to display. Affiliate networks generally operate on a CPA or revenue sharing basis, although some may use a CPM pricing model.

Marketer
The company paying to place its own advertisements. The marketer is the entity at the top of any advertising chain who pays others to display its ads.

Online location
A location such as a Web site, email message, or software application where an ad may be displayed.

Pricing model
The structure used by a marketer, intermediary, affiliate, or adware maker to charge for or pay for advertising. We define three types of pricing models:

> *CPA (Cost-Per-Action)*
> The cost of advertising based on a visitor taking some specifically-defined action in response to an ad. "Actions" include such things as sales transactions, customer acquisitions, and clicks. Entities that run ad campaigns based on a CPA pricing model get paid based on the number of actions taken by ad viewers. In the specific case where the action is a click, this model is known as *Cost-Per-Click (CPC)* or *Pay-Per-Click (PPC)*.
>
> *CPM (Cost-Per-Thousand)*
> The cost of 1,000 impressions. For example, a Web site that charges $1,500 per ad and reports 100,000 site visits has a CPM of $15 ($1,500 divided by 100). Entities that use a CPM pricing model charge their customers based on the delivery of ad impressions. This model may also be called *Pay-Per-Impression (PPM)*.
>
> *Revenue sharing*
> A pricing model most often used for retail marketing wherein the revenue that is generated when a customer views a marketer's ad is shared between the marketer and another entity that was involved in the display of the ad. If a marketer is advertising a particular product, and a person who views one of the marketer's ads decides to purchase that product after having seen the ad, the profit that is gained from that particular purchase will be shared between the marketer and another party that helped to display the ad.

2.2 From marketer to adware

Three different types of intermediaries are defined in our terminology. The following sections serve to illuminate how each type of intermediary may be involved in the journey that an advertisement takes from a marketer (a company called Acme in our examples) to a nuisance or harmful adware program (known as NOHAP in our examples). It is important to note that our focus is on how nuisance and harmful adware companies ultimately profit from displaying ads. The sections below reflect that focus, and may thus exclude certain unrelated aspects of the online advertising marketplace.

2.2.1 Affiliate networks

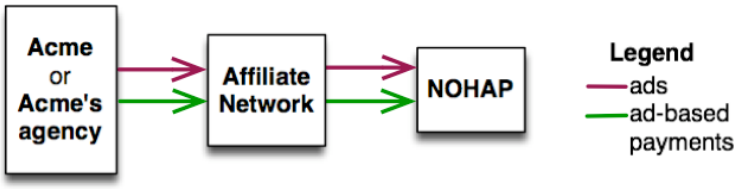
Affiliate networks broker advertising offers between marketers (or their agencies) and affiliates. After joining an affiliate network, a marketer or agency can publish a specific advertising offer – Acme, for example, may agree to pay out $20 for each new customer

generated through the display of a particular ad.[6] The affiliate network will then re-broker this offer to its affiliates, perhaps offering $15 for each new customer generated. Affiliates who have previously signed up with the network can browse the available advertising offers. When an affiliate (known as Dyn-a-site.com in our examples) signs up for Acme's offer, it will display Acme's ad and earn $15 for each new Acme customer the ad generates.

The example above illustrates the CPA pricing model, where the "action" is defined as a new customer acquisition. Affiliate networks and the marketers who use them may pay out based on other kinds of actions, or they might use a revenue sharing model. In the latter case, consider an Acme ad that intends to persuade viewers to buy a particular product. When a viewer does purchase the product, a specified portion of the revenue generated by that purchase will go to the affiliate network, and a sub-portion of that will go to Dyn-a-site.com. A less common scenario makes use of a CPM model, where the affiliate network coordinates the purchase of ad space on Dyn-a-site.com with the sale of Acme's ads into that space.

The most obvious way that nuisance or harmful adware can enter the picture is if a nuisance or harmful adware maker signs up as an affiliate in the network. The flow of payments and ads in such a situation is shown in Figure 1 below:

Figure 1: Adware As an Affiliate



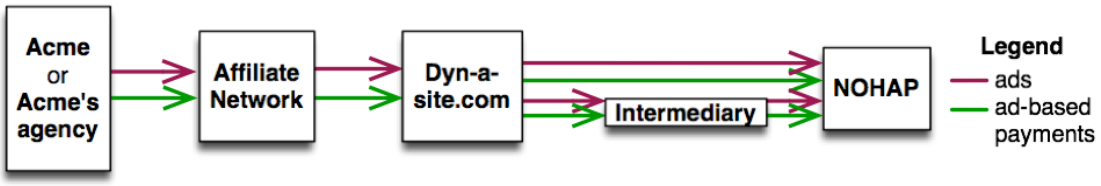
In this case ad-based payments (and the ads themselves) go directly from Acme to the network, and directly from the network to NOHAP. Due to growing awareness about the unseemly practices of some adware makers, many affiliate networks have begun a more rigorous affiliate screening process to keep bad actors out of their affiliate pools. Some marketers and agencies also like to know the identities of the affiliates that sign up for their offers, and some refuse to work directly with nuisance or harmful adware makers. Thus, the situation depicted above is becoming less common because nuisance and harmful adware makers are prevented from joining affiliate programs or from signing up for particular affiliate advertising offers. However, as revealed by the results of our study (in Section 3), a substantial number of marketers are still using this fairly direct approach.

A more complex scenario where nuisance or harmful adware may appear involves the re-brokering of marketers' offers beyond the affiliate network. Imagine that after Dyn-a-

[6] The dollar amounts used in the examples throughout this report are fictitious and are not meant to represent actual payment amounts used in online marketing.

site.com signs up for Acme's $15-per-new-customer deal, it turns around and offers an intermediary or an adware maker $10 for each new customer generated by the ad. Instead of displaying the ad, Dyn-a-site.com passes it on, as shown in Figure 2 below:

Figure 2: An Affiliate Re-Brokering An Advertising Offer



In this case each party in the chain, including NOHAP, earns a commission when Acme acquires a new customer. There are two main reasons why Dyn-a-site might decide to re-broker the Acme offer. The Dyn-a-site owner may discover that he or she lacks the space to display Acme's ads on Dyn-a-site.com. Or the owner may believe that passing the offer on will be more profitable than displaying Acme's ad and hoping to acquire new Acme customers.

The example above can become even more complex if Dyn-a-site sells the ads to a chain of intermediaries, the last of which eventually sells the ads to an adware vendor (this is explained further in Section 2.3). The results of our study reveal that these complicated arrangements appear more frequently for ads marketing well-known brands, whereas the simpler arrangement pictured in Figure 1 is more often used by smaller marketers.

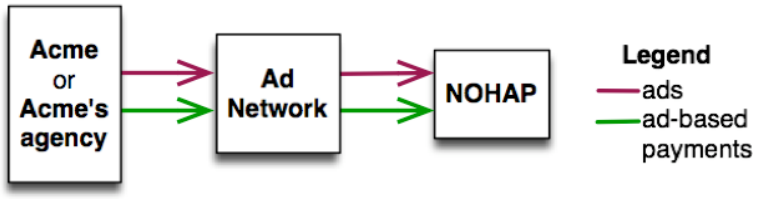
2.2.2 Ad networks

Ad networks are sales forces for large groups of online locations. Whereas high-profile news Web sites and Web portals have the resources to maintain their own ad sales forces, smaller sites may not be able to afford in-house sales teams. By joining an ad network, they can increase their visibility with marketers they may have otherwise never been able to reach. Marketers benefit by diversifying the locations where their ads may be displayed.

A typical ad network will buy inventory from the online locations in the network at a fixed rate. Consider, for example, an ad network that buys 1 million impressions at a CPM of $15 on Dyn-a-site.com, which is one of the locations in the network. The ad network will then work to find a marketer in the network who is willing to pay a slightly higher price, perhaps a CPM of $20, for 1 million impressions on Dyn-a-site.com. If Acme agrees to such a deal, Acme will pay the ad network and the Acme ads will run on Dyn-a-site.com. Ad networks may employ other kinds of pricing models, but CPM is the most common.

In a scenario similar to that depicted in Figure 1, NOHAP can get involved if the network buys inventory directly from it, as shown in Figure 3 below:

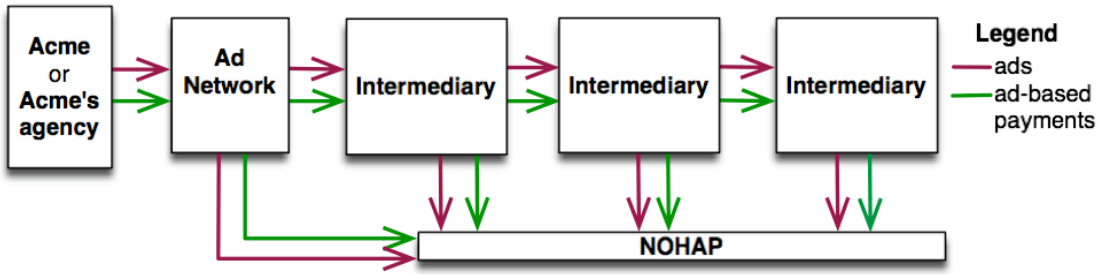
Figure 3: An Ad Network Buying Inventory Directly from Adware



Here the ad network buys inventory from NOHAP and sells that space to Acme or Acme's agency. Again, with increased awareness of deceptive and illegal practices that players like NOHAP engage in, this scenario is becoming less common. However, there are major ad networks that still deal directly (and publicly) with nuisance and harmful adware makers, one of which is featured in Section 3.2.

Ad networks buy inventory not only from Web sites like Dyn-a-site.com and adware makers like NOHAP, but also from other intermediaries. If these intermediaries (or their partners) have dealings with nuisance or harmful adware makers, Acme's ads may appear in their adware programs. The flow of money and ads in such a situation is shown in Figure 4 below:

Figure 4: An Ad Network Buying Inventory from an Intermediary



Instead of having a direct or nearly-direct relationship between Acme (or its agency) and NOHAP, in this case a chain of intermediaries has made agreements with each other, and somewhere down the line one of them passes Acme's ads on to NOHAP. Just as with affiliate networks, this scenario is more common for ads from higher-profile marketers.

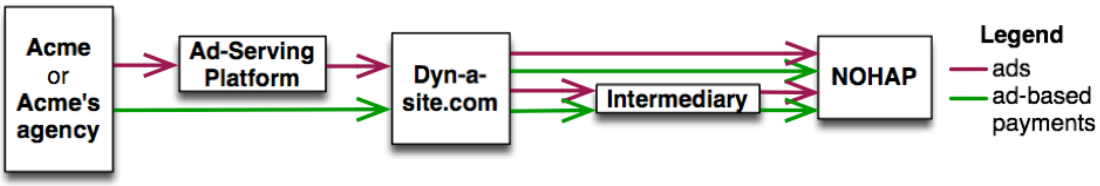
Although the services they offer and the pricing models they use may differ substantially, from our perspective ad networks and affiliate networks both contribute in similar ways to the problem of funding nuisance and harmful adware. Both types of networks facilitate the matching of ads to ad space, taking a cut of the ad revenue generated in the

process. Both types of networks may also appear in advertising chains of varying lengths and complexities wherein the final member in the chain brokers a deal with a nuisance or harmful adware maker.

2.2.3 Ad-serving platforms

In contrast to affiliate and ad networks, ad-serving platforms merely provide the technology that allows the transfer and tracking of ads, and they do not participate in any ad-based payments. Marketers or their agencies determine which other parties they wish to work with in order to display their ads, and the ad-serving platform facilitates that display, as shown in Figure 5 below:

Figure 5: An Ad-Serving Platform's Involvement in Adware Advertising



In this case, Acme or its agency makes an agreement with Dyn-a-site to display Acme's ads on Dyn-a-site.com. Dyn-a-site uses technology supplied by the ad-serving platform to find and display Acme's ads, which were previously provided to the platform. Dyn-a-site gets paid directly according to the pricing model offered by Acme or its agency. As noted in the previous examples, Acme or its agency may pay the ad-serving platform for other services, but in this case the ad-serving platform does not earn a commission correlated to the display of ads. Thus, from our perspective, ad-serving platforms do not contribute monetarily to the problem of nuisance and harmful adware.

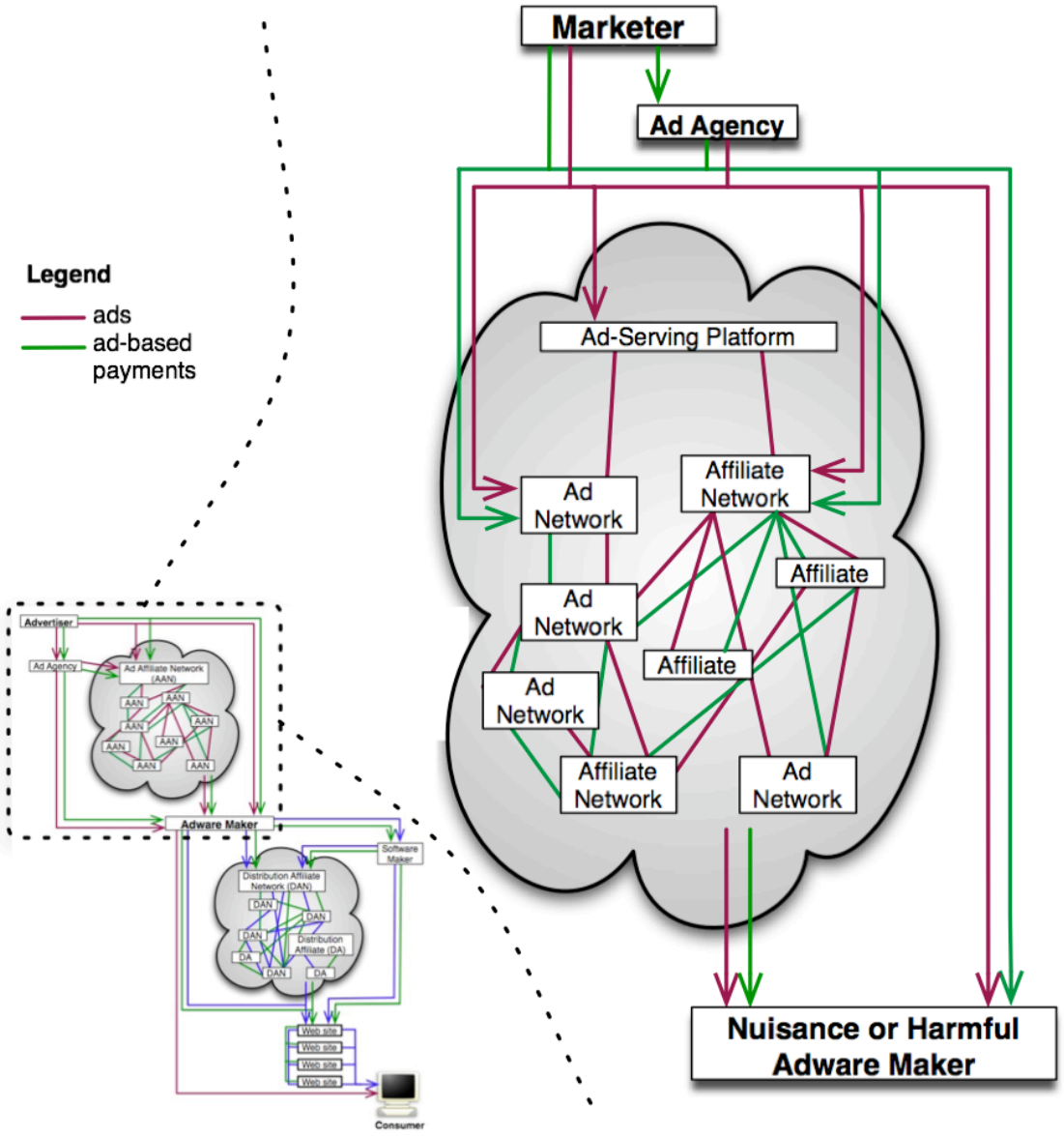
Aside from the case where Acme deals directly with NOHAP, there are two other reasons why Acme's ads may end up there: Dyn-a-site may have excess impressions that it cannot display, or it may decide that passing the ads on is more profitable.

In the diagram above, an ad-serving platform might be used to reach a particular ad or affiliate network instead of an affiliate like Dyn-a-site. This is not an uncommon approach for marketers. In this case Acme ads may end up at NOHAP if the network makes deals with NOHAP or other intermediaries who work with NOHAP. In all cases, though, the ad-serving platform is merely a conduit for ad content.

2.3 The big picture

With all of these different pieces working together, the big picture of online advertising can become incredibly complex, and does so most often for well-known brands. In the first *Following the Money* report we included a general illustration of how a marketer's advertising dollars fuel the problem of nuisance and harmful adware. Using our terminology defined above, we can now expand the top portion of that illustration to more accurately reflect the parties involved, as shown in Figure 6 below:

Figure 6: The Practical Complexities of Adware Advertising – Expanded



A marketer may either handle its advertising in-house or outsource it to an agency, which may get paid (at least in part) in correlation to the display of online ads. Marketers and agencies work directly with ad-serving platforms, ad networks, affiliate networks, or perhaps even adware makers. In the case of ad-serving platforms, ad-based payments go directly to the next intermediary in the chain. Beyond the initial intermediary, ads and ad-based payments may go through any number of other networks. Affiliates may even re-broker deals with additional networks. Eventually the final intermediary or affiliate cuts a deal with a nuisance or harmful adware maker. Thus, all of the previously discussed components may fit together in any number of ways, forming a chain of parties through which ads and payments are passed until they reach their final destination – nuisance or harmful adware.

2.4 Challenges for Marketers and Intermediaries

There are obviously a plethora of ways for an advertisement to make its journey from a marketer to an adware program. Marketers, agencies, and intermediaries that choose to work with nuisance or harmful adware – of which there are many – avoid this complexity altogether by dealing directly with the adware makers. For the rest, however, avoiding nuisance and harmful adware can be a critical and challenging component in running a successful ad campaign. With thousands of intermediaries and affiliates working in online advertising and minimal industry self-regulation, it can be difficult to determine which partners can be trusted to avoid nuisance and harmful adware. The long chains of intermediaries through which an ad may pass create serious complications in monitoring where ads are displayed.

3 CDT Study: The Role of Intermediaries in Adware Advertising

In order to help inform marketers, agencies, and intermediaries who are looking to avoid nuisance and harmful adware, CDT conducted a study of the ads generated by two adware programs: the Zango Search Assistant (distributed by Zango, formerly known as 180solutions) and the Best Offers Network (distributed by Direct Revenue). CDT considers the Zango Search Assistant to be nuisance or harmful adware because we believe that Zango has engaged in a pattern of unfair and deceptive practices in the distribution and operation of the program, as outlined in recent complaints we filed at the FTC.[7] Likewise, we consider the Best Offers Network to be nuisance or harmful adware based on a lawsuit recently filed against Direct Revenue by the New York Attorney General in which the adware company is alleged to have committed millions of surreptitious installations and engaged in other deceptive practices.[8] Both adware companies have been widely criticized by computer security experts and consumer

[7] See http://cdt.org/headlines/851.
[8] See http://www.oag.state.ny.us/press/2006/apr/apr04a_06.html.

advocates for their illicit behaviors related to notice and consent, installation, system resource consumption, and uninstallation.[9]

3.1 Methodology

In order to get an accurate picture of the advertising involved in these two programs, CDT set out to collect a substantial group of pop-up and pop-under ads from the two adware applications. We used two machines to do the ad collection at our offices in Washington, D.C.. Each machine contained a freshly-installed Windows XP operating system (Service Pack 1), a packet logger, and a script for generating ads. Each machine was running a single instance of an adware program – one machine had the Zango Search Assistant,[10] and the other had the Best Offers Network.[11] No other adware was installed.

We used a simple script to trigger the display of pop-up and pop-under ads. The script would select a URL from a list of 400 popular Web and e-commerce sites and open an Internet Explorer window directed at the selected site.[12] We used the Windows Task Scheduler to run the script once every 8 minutes for 7 hours per day. We generated ads this way from May 15 to May 19 and from May 22 to May 26, 2006.

During the ad collection period, we used the packet loggers to record all network activity on the machines. For each adware-generated pop-up or pop-under that appeared, we recorded all URLs listed in the re-direction path leading up to the display of the ad. We did not follow any links displayed in the popped window; we considered the pop-up or pop-under ad to be the end of the re-direction path.[13] Our conclusions about which intermediaries were involved in the display of each ad were based on the re-directions we recorded. As an example, consider the following simplified list of URLs that our packet logger could have recorded for an imaginary Acme ad:

```
http://www.AdNetwork-1.com/Acme?id=Zango
http://www.AdNetwork-2.com/Acme?id=AdNetwork-1
http://www.AdServingPlatform.com/Acme?id=AdNetwork-2
http://www.Acme.com/id=AdServingPlatform[14]
```

In our calculations, we would consider this Acme ad to have gone through three intermediaries before being displayed. The intermediary closest to Acme was

---

[9] See, e.g., *180solutions in 365 Days* (Dec. 11, 2005) at http://www.spywarewarrior.com/elh/180-summ.htm; Ben Elgin and Brian Grow, "The Plot to Hijack Your Computer," *BusinessWeek* (Jul 17, 2006) at http://www.businessweek.com/magazine/content/06_29/b3993001.htm.

[10] CDT downloaded the Zango Search Assistant from the 180solutions Web site.

[11] CDT downloaded the Best Offers Network as part of a bundle with a Fun Screenz screensaver.

[12] The list of URLs was chosen based on traffic rankings and also included specific sites the we believe tend to trigger adware ads.

[13] Other researchers have used a slightly different methodology, following contextual or syndicated ad links appearing within popped ad windows and counting the re-directions involved therein. See Ben Edelman, *Intermediaries' Role in the Spyware Mess* (May 28, 2005) at http://www.benedelman.org/news/052305-1.html.

[14] The "id" value helps each party track which previous party should be credited with the display of the ad.

AdServingPlatform, and the intermediary closest to Zango was AdNetwork-1, with AdNetwork-2 in the middle. We consider each intermediary to have made one *appearance* in this re-direction chain. Some intermediaries use internal re-directions in order to find the appropriate ad to display, as shown below:

```
http://www.AdNetwork-1.com/Acme?id=Zango
http://www.AdNetwork-2.com/redirect=Acme?id=AdNetwork-1
http://www.AdNetwork-2.com/Acme?id=AdNetwork-1
http://www.AdServingPlatform.com/Acme?id=AdNetwork-2
http://www.Acme.com/id=AdServingPlatform
```

In this case, we once again consider three intermediaries – AdNetwork-1, AdNetwork-2, and AdServingPlatform – to have been involved since the extra URL re-direction was internal to AdNetwork-2. Again, each of the three intermediaries made one appearance in this chain.

3.2 Results

We made 520 Web site visits over the course of the 10-day test, leading to the display of 380 ads. Thus, an ad was generated approximately 73 percent of the time when visiting a Web site. Both types of adware showed an average of approximately 19 ads per day.[15] The sections below highlight specific characteristics of the ads we found.

We understand that our sample is not necessarily representative of nuisance or harmful adware advertising activity. The ads that are displayed in a particular instance of an adware program can be influenced by a variety of factors, including the physical location and IP address of the machine hosting the adware, the speed and type of Internet connection used, and the Web browsing activity on the machine. Although there are many adware vendors, we focused on only two of the largest ones. However, we believe that we gathered a sufficient number of ads to at least begin to shed some light in this space, and we acknowledge that we were without the resources to setup a testing environment that could fully address the diversity of nuisance or harmful adware ads.

3.2.1 Quantity of intermediaries

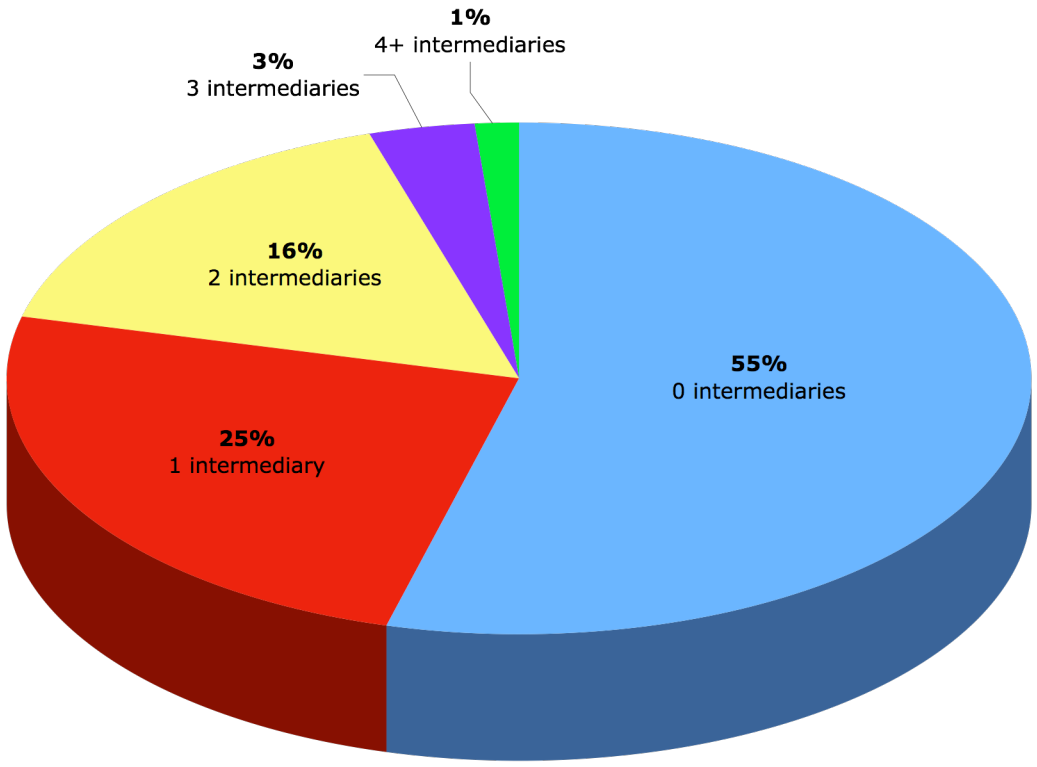
As described in Section 2, the journey that an ad takes from its original source to a user's computer can vary from short and simple to long and complex. The level of control that

[15] It is important to note here that CDT did not change any default settings, such as blocking cookies or concealing our IP address. Therefore, these results seem directly at odds with Zango's claims that "Zango Search Assistant displays 2-3 advertisements per day from paid sponsors" (see the copy of the Zango FAQ page cached by Google on August 2, 2006 at http://cdt.org/privacy/spyware/20060809zangofaq.html). Suggesting to consumers that they will receive fewer ads than they do would seem to be yet another of Zango's deceptive practices.

marketers have over their advertising content is often closely tied to the number of intermediaries involved.

Figure 7 below shows the breakdown of the ads we collected based on the number of intermediaries involved. It is important to note that the data we collected reveals only the intermediary steps that are physically traceable on the computer of the adware user. Marketing content is often passed between intermediaries and affiliates via email or through other means, and these informal transactions are not represented here. Thus, the actual number of intermediaries involved in the display of an ad may be greater than what we can measure. In our study, the average number of intermediaries for all 380 ads was 0.7, which, as explained below, was much lower than we expected.

Figure 7: Breakdown of Ads Based on Number of Intermediaries



Slightly more than half of all ads collected involved no intermediaries at all, indicating that the marketers in those cases had direct relationships with the adware companies. Direct relationships may also exist when the only intermediary involved is an ad-serving platform; 5 percent of our ads were delivered in this manner. Thus, for 60 percent of the ads, marketers most likely made direct deals with either Zango or Direct Revenue. Another 20 percent of the ads involved a single intermediary. These intermediaries may also have direct relationships with adware vendors. Unless the marketers and agencies

using these intermediaries specifically requested to remain unaware of the placements of their ads, the marketers likely knew that their ads were placed in an adware rotation.

These facts came as a big surprise to us. In conducting our research for the first *Following the Money* report we focused on generating ads for high-profile brands – marketers whose products are familiar to the average consumer. However, in conducting our most recent research we found that high-profile brand ads tend to involve multiple intermediaries (as described in Section 3.2.5). We did not specifically focus this study on high-profile brands, and thus a majority of the ads were marketing relatively unknown products and services. These marketers seem far more willing to make direct deals with nuisance and harmful adware vendors.

The final 20 percent of the ads involved two or more intermediaries. In these cases, it may be much more difficult for marketers and agencies to determine where their ads are displayed or how they end up in an adware rotation. With each intermediary added to the chain, the job of policing ad placements becomes exponentially more difficult for the marketers.

The quantity breakdown for the ads delivered by each individual adware program is shown in Figure 8 below:

Figure 8: Breakdown of Ads Based on Number of Intermediaries, by Adware Program

Number of Redirections (N)	*Percentage of Zango Search Assistant ads with* N *re-directions*	*Percentage of Best Offers Network ads with* N *re-directions*
0	59%	49%
1	27%	23%
2	11%	21%
3	2%	5%
4 or more	1%	2%

More marketers seem to have direct relationships with Zango, where the ads averaged 0.6 intermediaries per ad, than with Direct Revenue, which averaged 0.9 intermediaries per ad.

3.2.2 Intermediaries ranked by number of appearances

During our test we found 73 distinct intermediaries involved in displaying the ads we viewed. These intermediaries together made a total of 280 appearances in the URL re-direction chains for all 380 ads. Figure 9 below shows the intermediaries that had 4

percent or more of the total number of appearances across all re-direction chains. The overall percentage of ads in which these intermediaries appeared is also listed.

Figure 9: Top Intermediaries Based on Total Number of Appearances

Rank	*Intermediary*	*Number of Appearances*	*Percentage of Appearances in Re-Directed Ads*	*Percentage of Appearances in All Ads*
1	MyGeek	41	14.6%	10.8%
2	VendareNetblue	29	10.4%	7.6%
	eMarketMakers	15		
	Netblue	14		
3	ValueClick	27	9.6%	7.1%
	Webclients.net	12		
	ValueClick Media	7		
	Commission Junction	5		
	CJ's BFAST*	3		
4	aQuantive – Atlas*	20	7.1%	5.3%
5	LinkShare	14	5.0%	3.7%
6	DoubleClick	13	4.6%	3.4%
	DART*	7		
	Performics	5		
	Falk eSolutions*	1		
6	HydraMedia	13	4.6%	3.4%

*ad-serving platform (no ad-based payments)

The entries in this figure can be classified as follows:[16]

- **MyGeek**, the top intermediary listed, has a partnership with Direct Revenue, which explains its large number of appearances here.[17] MyGeek is an ad network.
- **VendareNetblue** is the result of a recent merger between two networks: Vendare Group, which runs the **eMarketMakers** affiliate network, and **Netblue** (formerly known as YFDirect), which is also an affiliate network. Although VendareNetblue operates other intermediaries, in our study only eMarketMakers and Netblue made appearances.
- **ValueClick** owns many different intermediaries which are often operated independently, which is why we chose to show the breakdown here. When their appearances are totaled together, ValueClick made the third highest number of appearances in our study.[18] **Commission Junction (CJ)** is one of the industry's

[16] These classifications were drawn from CDT's direct communications with intermediaries and advertising trade associations and from information found on the intermediaries' Web sites.
[17] See http://www.direct-revenue.com/news12.php.
[18] ValueClick contends that the number of appearance for Webclients.net in Figure 10 should be 5 instead of 12 due to the way that ValueClick's servers interact. While CDT does not disagree with ValueClick's

largest affiliate networks, and it operates its own ad-serving platform, **BFAST**. **Webclients.net** and **ValueClick Media** are ad networks.

- **aQuantive** also runs several kinds of intermediaries, but the only one that appeared in our study was **Atlas**, which is aQuantive's ad-serving platform.
- **LinkShare** is one of the industry's largest affiliate networks.
- **DoubleClick** operates several intermediaries, three of which appeared in our study. **DART** and **Falk eSolutions** are ad-serving platforms. **Performics** is an affiliate network.
- **HydraMedia** is an affiliate network.

As discussed in Section 2.2.3, ad-serving platforms do not receive ad-based payments from marketers or agencies, nor do they pay other intermediaries in correlation to the display of ads. Thus, although we include several ad-serving platforms in Figure 9 – Atlas, BFAST, DART, and Falk eSolutions – we do not believe that these intermediaries are fueling the problem of nuisance and harmful adware with their dollars. We list them in the study because their involvement helps to underscore the complexity of this marketplace. Ad and affiliate networks, however, are a different story. The networks listed above likely contributed the most money to nuisance or harmful adware programs out of all 73 intermediaries that we found.

To some degree, presence in Figure 9 can be correlated to the sheer volume of ad placements conducted by some of these companies – ValueClick, LinkShare, DoubleClick, and aQuantive are widely regarded as some of the largest players in online marketing, with thousands of marketers and tens of thousands of affiliates in some of their networks. In addition, many of the larger intermediaries have been formed through mergers and acquisitions of once-separate entities, leaving them with the task of integrating disparate sets of advertising contracts and ad placement policies into uniform standards for the company as a whole. Regardless of the size or complexity of their business, however, there are steps that intermediaries can take to limit their involvement with nuisance and harmful adware. There are large, multi-division intermediaries that are absent from this list because they seem to have taken such steps. Ultimately, even those intermediaries that are conglomerations must be accountable for the practices of the subsidiaries that they directly control.

Figure 9 also speaks to the vastly distributed nature of online advertising. The intermediaries in the figure comprised only about half of the total number of appearances, leaving the other 66 networks to comprise the remainder. Most of those intermediaries appeared only a small number of times (the median number of appearances for all intermediaries was 2). This clearly illustrates how the online marketing landscape is populated with a large volume of smaller players.

---

contention, we cannot independently verify their claim. For ValueClick's explanation of the discrepancy, see http://cdt.org/privacy/spyware/20060809valueclickcomments.pdf.

3.2.3 Intermediaries closest to marketers

Knowing that ads involving multiple intermediaries can be especially troubling, marketers and agencies may be interested to know which intermediaries are most often the ones at the top of a chain that eventually leads to nuisance or harmful adware. Out of 380 ads, 80 of them involved two or more intermediaries. Figure 10 lists the intermediaries with 4 percent or more of the total appearances closest to marketers in that group of ads.

Figure 10: Top Intermediaries Closest to Marketers

Rank	*Intermediary*	*Number of Appearances in Chains of 2 or More*	*Percentage of Total Appearances in Chains of 2 or More*
1	VendareNetblue	14	17.5%
	Netblue	9	
	eMarketMakers	5	
2	ValueClick	11	13.8%
	Webclients.net	7	
	Commission Junction	3	
	CJ's BFAST*	1	
3	LinkShare	9	11.3%
4	aQuantive – Atlas*	6	7.5%
5	DoubleClick	5	6.3%
	Performics	4	
	DART*	1	
6	eXact Advertising	4	5.0%
6	HydraMedia	4	5.0%

*ad-serving platform (no ad-based payments)

The only name that appears here but not in Figure 9 is **eXact Advertising**, which is an ad network by our definition.[19] A few of the others from Figure 9 have disappeared, most notably MyGeek due to its direct dealings with Direct Revenue. Most of the rest of the entries appear in roughly the same proportions as in Figure 9. We take this correlation to mean that the sheer volume of ads placed by an intermediary cannot explain their large involvement in chains leading to nuisance or harmful adware – if it could, then the intermediaries featured in Figure 9 would be spread throughout the chains instead of being clustered close to marketers.

Proximity to marketers means different things for different kinds of intermediaries. For the ad-serving platforms – Atlas, DART, and BFAST – we expect them to appear

[19] The eXact case is a unique one because in addition to its role as an ad network, it also distributes its own adware programs, including The Bullseye Network, eXactSearchBar, NaviSearch, and DealBar.

frequently closest to marketers, because they are merely facilitating the transfer of the ad content from a marketer to another party. In this case, it is likely that an intermediary further down the chain is the problem since the marketer or agency chooses the destination to which the ad-serving platform conducts its ads. With ad and affiliate networks, however, marketers may be trusting them to avoid handing ads off to other intermediaries that use nuisance or harmful adware.

3.2.4 Intermediaries closest to adware

Marketers, agencies, and intermediaries alike can benefit from knowing which intermediaries work closely with nuisance and harmful adware makers. Figure 11 lists the intermediaries with 4 percent or more of the total appearances closest to adware in chains of two or more intermediaries. Since these intermediaries appear closest to adware, it is clear that they work *directly* with adware companies, whether by choice or by mistake.

Figure 11: Top Intermediaries Closest to Adware

Rank	*Intermediary*	*Number of Appearances in Chains of 2 or More*	*Percentage of Appearances in Chains of 2 or More*
1	MyGeek	24	30%
2	IntegraClick (Clickbooth)	8	10%
2	ValueClick	8	10%
	ValueClick Media	5	
	Webclients.net	3	

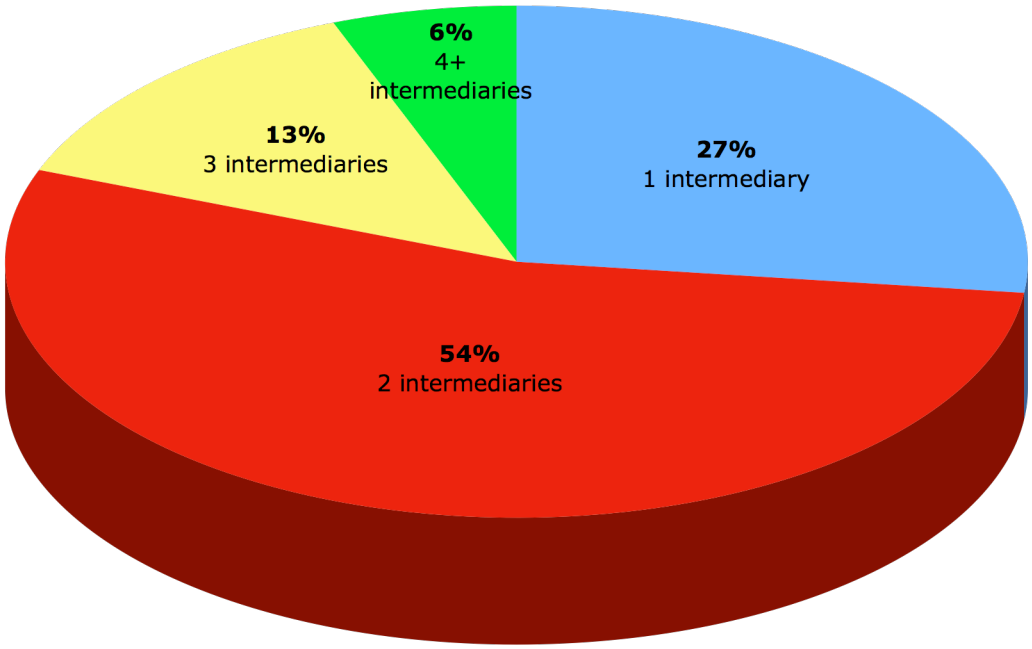
MyGeek tops the list based on its Direct Revenue deal. **IntegraClick** (also known as **Clickbooth**) is an affiliate network which seems to be either allowing adware vendors to sign up as affiliates or which has been duped into signing up affiliates who turn out to be adware vendors. ValueClick Media and Webclients.net, as ad networks, appear to have purchased inventory directly from adware vendors.

Note that the three networks above are closest to the adware in only half of the multiple-intermediary ads. In fact, the closest-to-adware spot is occupied by 24 different intermediaries across the other half of the ads. We believe this shows that few intermediaries proactively and consistently seek out deals with nuisance or harmful adware vendors; instead, most intermediaries use nuisance or harmful adware as an occasional outlet or by mistake.

3.2.5 Ads for high-profile brands

The ads we collected were marketing a huge range of products, services, and Web sites. We noticed during the course of the test that ads for high-profile brands (those familiar to the average consumer) were characterized differently than the ads overall. Our data reveals that ads for high-profile brands (52 in all, or 14 percent of the total) tend to go through a greater number of intermediaries before being displayed, as detailed in Figure 12 below. The average number of intermediaries for high-profile brand ads was 2 (compared to 0.7 intermediaries for the ads overall).

Figure 12: Breakdown of High-Profile Brand Ads Based on Number of Intermediaries



Not a single ad for a high-profile brand was served directly by adware – all 52 ads involved at least one intermediary. And an overwhelming majority of the ads went through two or more intermediaries before being displayed.

This result is symptomatic of a problem we discovered while researching the first *Following the Money* report. As part of that research, we contacted marketers whose ads were known to be served by the Zango Search Assistant. Many of the more well-known companies contacted were unaware that their ads were being served by nuisance or harmful adware programs. This was due in large part to having multiple intermediaries involved in the ad placement. The more parties that are involved, the harder it is for

marketers and agencies to police the placement of their ads, and the more likely it is that an ad will show up in an unexpected location.

3.2.6 Self-targeted ads

Another group of ads that stood out from the rest were the *self-targeted* ads. Self-targeting occurs when an ad served by adware displays the same page as the underlying Web site that caused the ad to be displayed. This may cause a commission to be paid to the intermediaries who placed the ad even though the consumer was already at the marketer's site.[20]

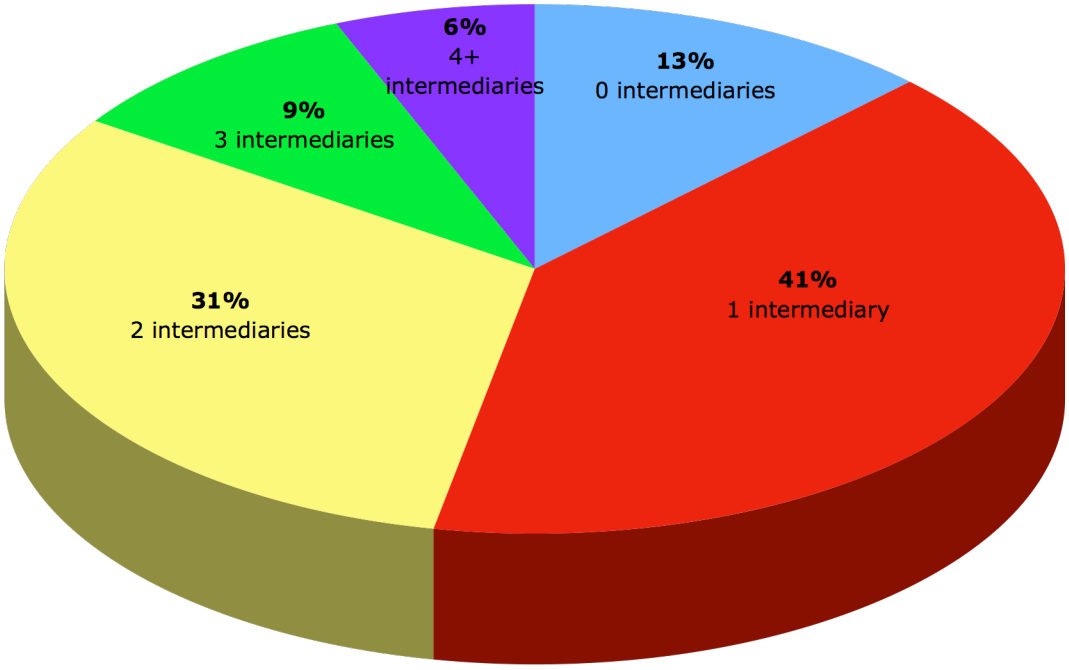
There are several different explanations for this behavior. It is possible that an intermediary or the adware maker is duping the marketer by agreeing to show the ads elsewhere but instead targeting the marketers' own sites in the hope of earning easy commissions. There is evidence that Direct Revenue has intentionally engaged in this kind of fraudulent practice.[21] Alternatively, it may be the case that the intermediaries involved need a way to dispose of excess impressions. If an intermediary needs to offload its extra ads, they may be sold into an adware company's rotation where they end up as self-targeted ads. It is also possible that the algorithm employed to deliver targeted advertising just happens to generate the most relevant ad possible – that of the underlying Web page. In this case, a technological flaw causes the display of the self-targeted ad.

We found 32 self-targeted ads (8 percent of the total). Their breakdown based on the number of intermediaries involved in each is shown in Figure 13.

[20] For a detailed explanation of how this works in some cases, see Ben Edelman, *The Effect of 180solutions on Affiliate Commissions and Merchants* (Oct. 20, 2004) at http://www.benedelman.org/spyware/180-affiliates/.

[21] See Ben Elgin, "A Software Hall of Mirrors," *BusinessWeek* (Jul. 17, 2006) at http://www.businessweek.com/magazine/content/06_29/b3993009.htm.

Figure 13: Breakdown of Self-Targeted Ads Based on Number of Intermediaries



Slightly less than half of the ads involved two or more intermediaries. This appears to once again be a matter of marketers and agencies having difficulty tracking their ad placements due to the complexity in the chain. If marketers and agencies were aware of where their ads were appearing, it is highly unlikely that they would allow their ads to target their own sites.

The other half of the ads, involving fewer than two intermediaries, are more puzzling. The lack of intermediaries would seem to imply that the marketers are aware of the locations of their ad placements, but it does not make sense that a marketer would want to target its own site. Thus, some intermediaries and adware makers may be duping marketers and agencies after they agree to the ad buy. This illustrates the lack of marketer awareness – even without a complex chain of intermediaries, and when it is in their best interest to do so, some marketers are not preventing self-targeted ads.

Interestingly, about 44 percent of the self-targeted ads were for high-profile brands, despite the fact that high-profile brands only accounted for approximately 14 percent of the ads overall. We believe this is a symptom of the lack of awareness among larger marketers about where their ads are appearing and what it takes to effectively police their ad placements. More popular companies tend to run broader ad campaigns that encompass many different mediums and third parties, leaving this kind of fraudulent adware behavior to fly under the radar.

4 CDT's Recommendations

Although the complexity of online advertising can be overwhelming, responsible marketers, agencies, and intermediaries seeking to avoid fueling nuisance and harmful adware with their advertising dollars have many tools at their disposal for doing so. We recommend the following for marketers, agencies, and intermediaries:[22]

- **Establish and enforce ad placement policies.** Having a policy that explicitly states which ad placements a marketer, agency, or intermediary does and does not consider acceptable will provide a standard to which all advertising partners can be held. A few prominent marketers and several of the intermediaries mentioned in this report already have or are working to establish ad placement policies.[23] Armed with a policy, marketers, agencies, and intermediaries should then:

    - **Require all advertising partners by contract to adhere to the policies.** When marketers, advertising agencies, intermediaries, and affiliates sign contracts with each other, adherence to the policy should be one of the terms of the contract. Even if marketers outsource their online advertising to an agency, that agency must be held accountable for avoiding unwanted ad placement locations. All partners must also require their partners to include these ad placement terms in *their* contracts with *their* partners, essentially forcing the contractual bind all the way down the advertising chain. This is an important step that most participants in online advertising have yet to take.

    - **Monitor ad placements and flag policy violators.** Simply having a policy is not effective unless it is enforced. Ad placements must be monitored and partners who violate the terms of their agreements should be punished. There are numerous ways that marketers, agencies, and intermediaries can go about doing this: through in-house, hands-on testing; by hiring private online brand protection services;[24] or by investigating whether a third party organization (such as TRUSTe) might provide this function. Perhaps the most effective monitoring will involve some combination of these solutions.

[22] These recommendations may not all be applicable to every entity involved in online advertising. For example, a marketer that does all of its own advertising can ignore our suggestions regarding holding ad agencies accountable. Similarly, an ad-serving platform that is not involved in choosing an ad's destination will not be able to contractually forbid that destination from using nuisance or harmful adware. In general, however, the recommendations should be applied as widely as possible.

[23] See the appendix for a discussion of marketers that have ad placement policies and the resources available to parties looking to draft such a policy. The following intermediaries have also made their policies available: aQuantive's Atlas (http://www.atlassolutions.com/privacy/), DoubleClick's Performics (http://www.performics.com/docs/code_of_conduct.pdf), and ValueClick (http://cdt.org/privacy/spyware/20060809valueclickpolicy.pdf).

[24] Some companies that offer online brand protection services include Adgooroo (http://www.adgooroo.com/), Cyveillance (http://cyveillance.com/), MarkMonitor (http://www.markmonitor.com/), and NameProtect (http://www.nameprotect.com/).

- **Research potential advertising partners.** Companies working together in the online advertising space need to agree not just on financial goals, but on ad placement quality goals as well. Marketers, agencies, and intermediaries can use the data presented in this report and consult with other marketers and industry groups to learn more about intermediaries under consideration. When evaluating intermediaries, recall that many have independent divisions whose policies can vary significantly. Marketers, agencies, and intermediaries should gain as much information as possible about (a) the identities of other intermediaries their potential partners work with and (b) the quantity of other intermediaries their potential partners use. The more untrustworthy intermediaries involved, the more skeptical marketers should be.

- **Stay as informed as possible about the parties who are actually displaying the ads.** It may be unrealistic to ask marketers, agencies, and intermediaries to know every affiliate and Web site showing their ads. However, the more that is known about specific locations where ads are appearing, the less time will be spent worrying about having ads show up unexpectedly in nuisance or harmful adware.

In addition to the suggestions above, there are several further steps that intermediaries in particular can take:

- **Increase transparency in ad placement models.** Some intermediaries claim that they are not responsible for ads that show up in nuisance or harmful adware because it is an algorithm, not a person, that matches ads with ad space. Responsible intermediaries should be as transparent as possible about that matching process so that marketers can determine their trustworthiness. Intermediaries that actively avoid nuisance and harmful adware should be anxious to explain to marketers how their systems work as proof that they can be trusted to protect brand integrity.

- **Work with each other and industry groups to establish best practices and share information.** The Interactive Advertising Bureau, the Network Advertising Initiative, the Direct Marketing Association, and the American Association of Advertising Agencies are all good vehicles for convening parties in the online advertising space around a set of best practices for both ad placement and transparency. Working together can also legitimize intermediaries and give marketers another tool to navigate the online advertising space.

5 Conclusion

Based on our recent discussions with marketers and intermediaries, it seems that some of them are taking the nuisance and harmful adware problem seriously. Although they have highlighted their difficulties in policing their ad placements based on the volume of ads they deal with (and, in the intermediary case, the disparate practices of their subsidiaries), many of them have also begun to cut their direct ties to nuisance and harmful adware vendors.[25] The full effect of these changes remains to be seen, and it is incumbent on all parties involved in online marketing to engage in similar efforts.

CDT began this work with two goals: to shed some light on how the extremely complicated world of online advertising works, and to provide information about which parties are involved in delivering ads to nuisance and harmful adware programs. Although the role of intermediaries in our study was less than we expected, we still believe that part of the problem with adware advertising today is a simple lack of understanding on the part of marketers, agencies, and intermediaries. They have the tools they need to stop the flow of their advertising dollars to nuisance and harmful adware vendors, and with increased understanding of who the players are and how the system works, we look forward to a time when transparency and trust rule the world of online advertising.

For further information, contact:
Ari Schwartz (202) 637-9800 x107.
Alissa Cooper (202) 637-9800 x110.
CDT appreciates the contributions of Dhruv Kapadia to this report.

[25] VendareNetblue began severing its direct ties to partners engaged in questionable practices in early 2006, and Webclients.net told us that it has recently ceased its dealings with some of the industry's worst offenders.

Appendix: Discussion of ad placement policies

The following section appeared in CDT's March 2006 report, *Following the Money: How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend*.

Solution: Adoption and Enforcement of Advertising Placement Policies

Dozens of well-known companies are in a position to make an immediate impact on the problem of nuisance or harmful adware by evaporating its funding source. A vital step toward that goal is the adoption and enforcement of advertising placement policies by companies that advertise online.[3]

Several organizations have taken the lead in establishing policies that discourage or prohibit the use of nuisance or harmful adware in serving ads. Others have established strict standards that adware makers must meet. Organizations leading the way in addressing the adware problem include the Interactive Travel Services Association (ITSA), the Direct Marketing Association (DMA)[4], Major League Baseball, Dell, and Verizon.

In 2004, CDT found that travel Web sites were the subject of some of adware maker 180solutions' most numerous and blatant ads. The recently established ITSA policy allows advertising only with adware vendors that follow best practices in installation of adware, labeling of ads, and uninstall capabilities. The policy appears to have already made a significant impact. Since ITSA adopted the policy, 180solutions adware generates far fewer ads for travel sites. By CDT's estimation, 180solutions' software clearly fails to meet the ITSA standards.

Other organizations are working to set parameters for how adware should and should not behave. The recently announced TRUSTe Trusted Download Program[5] has already

---

[3] This report focuses on the role of advertisers in stemming the tide of nuisance and harmful adware, but the role of ad networks is also significant and the remedies are similar for both parties. CDT chose to emphasize advertisers' responsibility because the variety of forms that ad networks take and the complicated ways in which they interconnect make it difficult to address them here. We expect to address their role in a future report.

[4] The DMA recently introduced a new guideline dealing with the use of software in advertising in its Guidelines for Ethical Business Practice (*see Article #40 in* http://www.the-dma.org/guidelines/EthicsGuidelines.pdf). The DMA has also outlined steps that marketers can take to ensure compliance with the guideline (*see* http://multichannelmerchant.com/mag/keeping_tabs_internet_03012006/index.html).

[5] *See* http://truste.org/trusteddownload.php.

issued specific criteria for acceptable adware, and StopBadware.org[6] has begun the process of developing guidelines against which adware may be tested. Both of these sets of criteria, in addition to the policies already in use by the organizations listed above, can serve as models for other companies looking to adopt their own adware advertising policies.

Of course, policies are useless unless they are enforced. Advertisers must insist that ad networks enforce their policies, and advertisers have to be prepared to take their business elsewhere if the complex tangle of ad network relationships makes it impossible to ensure compliance at every level. Monitoring will be necessary in order to identify affiliates that fail to adhere to the policy. The use of blind ad networks may be acceptable only if the blind network can be trusted to enforce the policy without the advertiser having the capability of checking up on the placement of its ads.

[6] *See* http://stopbadware.org/home/reports.