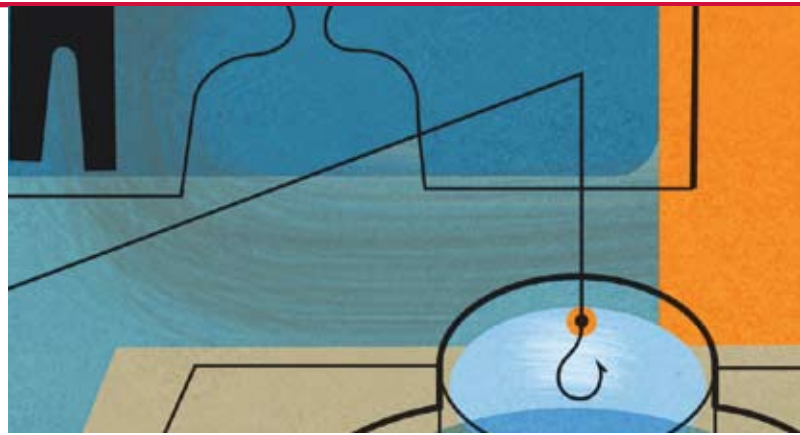


# Whatever Happened To Adware And Spyware?

By Aditya Kapoor



Adware and spyware are two of the primary tools used for the online promotion of advertising and marketing.

These applications often benefit from social engineering methodologies and often piggyback on an otherwise useful freeware or shareware application that a user wants to download. These unwanted applications typically come with end-user license agreements (EULAs) that are supposed to define their behavior. However, these descriptions are normally not explicit or useful, causing confusion for users and opening the door to further social engineering traps.

In the first half of this decade, adware and spyware—often called potentially unwanted programs, or PUPs—grew exponentially. After 2005, however, we have seen a constant decline in their numbers. In this article we'll highlight the key changes in online compensation models that are the driving factor of this decline. Adware and spyware have mostly split into distinct fields: the former with cleaner applications and a better user-consent model developed by key adware players and the latter sometimes malicious and frequently defined as Trojan malware. This comparatively clean divide has helped keep the numbers of adware and spyware applications low. So if these PUPs are no longer a threat, will they soon be gone for good? To answer that, we will discuss the changing threat landscape and the role social engineering plays.

## Seeking Clarity

The terms *adware* and *spyware* are frequently used loosely and interchangeably and often create confusion. We'll follow definitions supplied by the Anti-Spyware Coalition (ASC).<sup>1</sup>

- **Adware** A type of advertising display software that delivers advertising content potentially in a manner or context that may be unexpected and unwanted by users. The ASC's Risk Model document details many of the behaviors that may be considered unexpected or unwanted. Many adware applications also perform tracking functions and, therefore, may also be categorized as tracking technologies. Some consumers may want to remove adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for.
- **Spyware** In its narrow sense, spyware is a term for tracking software deployed without adequate notice, consent, or control for the user. In its broader sense, spyware is used as a synonym for what the ASC calls "Spyware (and Other Potentially Unwanted Technologies)": technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:
  - Material changes that affect their user experience, privacy, or system security
  - Use of their system resources, including what programs are installed on their computers
  - Collection, use, and distribution of their personal or other sensitive information

Acknowledging that the common term spyware has now largely drifted from its exact meaning, the members of the ASC have decided to use “spyware” (in its narrow sense) for technical documents. Recognizing further that it is impossible to avoid the wider connotations arising from popular usage, the ASC also notes the existence of a general interpretation that includes all PUPs. In this article, the term *spyware* is never used in its broad sense, but always in the narrow sense, namely, as software that is related to marketing. We use the term *monitoring software* to define pure spy programs such as keyloggers.

## A Fast Takeoff

Adware and spyware grabbed our attention in the year 2000 with the appearance of Adware-Aureate, which employed the user’s browsing history to display ads. This move led to the creation of one of the first anti-spyware applications, Gibson Research Corp.’s OptOut.<sup>2</sup>

Adware and spyware started growing prominently around late 2004 and peaked in 2005. (See Figures 1 and 2.) The primary motive was to generate revenue via millions of installations on users’ desktops (via the pay-per-installation model) as well as to display advertisements (via the pay-per-click model). The adware and spyware industry flourished in these years due to the large amount of revenue generated from ads. Every time a user clicked a certain ad, the ad provider received a commission.

## Compensation Models and Caveats

Adware and spyware use two major compensation models for online advertisements. Both models work well in a perfect world, but how do they fare in a world that includes people with malicious intent? Let’s take a look at how these models can be exploited.

### Pay-per-install: The client-side model.<sup>3</sup>

In the pay-per-install (PPI) model, companies selling products or services pay the adware provider to display ads. The adware provider in turn pays individuals or affiliates to distribute its adware using bundling or other means. (ZangoCash, for example, pays from \$0.75 to \$1.45 in the United States for each piece of adware installed.<sup>4</sup>) The software finally has to be installed on the client machine.

The PPI model normally tracks installations of software by using a particular referrer. So, if John Doe hosts a PPI-based adware installer on his web site and some other user downloads and installs that software via the site, John will receive a certain amount of money. To increase the downloads from his site, John might try to increase traffic using attention-getting content such as catchy titles, adult images or videos, free games, or ringtones.

As traffic and payments increase, John could decide to use an exploit to install the adware application without the users’ being aware of the installation. Many such applications display a EULA before installing, but this would only alarm visitors, so John might further decide to tweak the application to suppress the EULA and increase his installation score. Now if John is a seasoned hacker, he could replicate this model on thousands of compromised sites to exponentially increase his installations and payoff. Fellow *McAfee Security Journal* author Benjamin Edelman describes a similar, real scenario on his web site.<sup>5</sup>

**Adware**

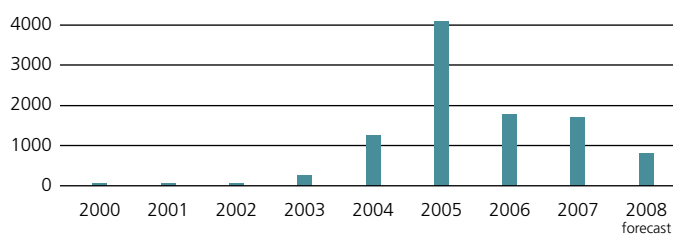


Figure 1: Adware growth reached its peak in 2005. (Source: McAfee Avert Labs).

**Spyware and monitoring software**

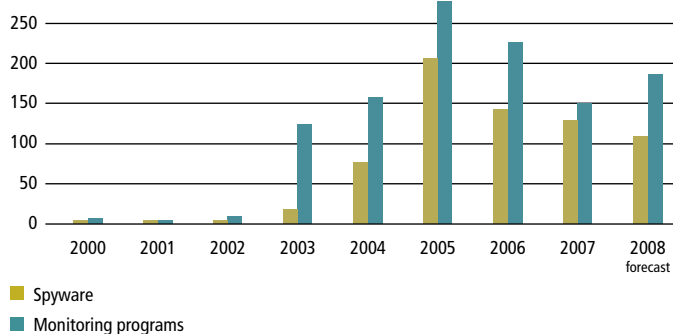


Figure 2: Spyware and monitoring programs have also seen a general decline since 2005, but we anticipate an upturn in the latter in 2008. (Source: McAfee Avert Labs).

The PPI model of compensation proved very lucrative for programmers as well as for people with malicious intent—thus contributing to the fantastic growth of adware and spyware. Many installation vectors support this model. These vectors can be broadly divided into two categories:

- **Social engineering** This requires user interaction and relies on the user to install and, in some cases, even propagate the software. The number of social engineering methods is limited only by the imaginations of attackers, who can often lure even the most vigilant users. In the example of John Doe, offering free games or ringtones is bait that many people cannot resist. Ultimately, the user decides to take the risk or leave the free goodies on the table.
- **Exploits** Installation of adware through exploits may not require any human interaction at all; however, in many cases the user is lured by social engineering techniques to malicious web sites that host these exploits.

### Pay-per-click: The server-side model.<sup>6</sup>

The pay-per-click (PPC) model has two variations: sponsored ads and content-based ads.

The PPC model does not require any adware or spyware software to be installed on the user's system, but the model may depend on the user's input for context—for example, from search engine results—to provide relevant ads. Google content-based ads, for example, work by using the PPC model.

Some of most common delivery mechanisms for PPC content are:

- **Banner ads** Ads are shown within a banner or predefined space. This content can change.
- **Pop-up or pop-under ads** Ads are delivered in separate windows, creating an annoying user experience.
- **Flash-based ads** These are similar to banner ads but use flash animation to vary the ad content.

The PPC model can work in a much more controlled environment, in which in the web site hosting these ads may choose the delivery mechanism. Although the PPC model is server based and would seem more secure, it's not entirely foolproof. Scammers can still use deceptive practices to trick users.<sup>7</sup>

Because most of the ad content is stored on servers and uses JavaScript, Flash, and other rich-content technologies, inserting malicious ads in the ad stream is not difficult.<sup>8,9</sup> In one such case, a Yahoo-owned ad network unknowingly distributed malicious banner ads that eventually downloaded Trojans on users' machines. In this particular scenario, banner ads were shown on web sites such as MySpace and PhotoBucket. These malicious ads were slipped into Yahoo's ad network undetected. We've also seen user clicks hijacked by DNS cache poisoning.<sup>10</sup> However, users are not directly affected in these cases; the ISP or server hosting the ads is more vulnerable to these threats.

To better mitigate the attack vectors exploiting these compensation models, let's take a brief overview of how social engineering plays a role in this online market of endless revenue-generation possibilities.

## Social Engineering Aspects

*Hackers are going to go after the weakest link in the security chain, which is always the people. — Kevin Mitnick (2007)<sup>11</sup>*

Regardless of the model adware developers use, their primary success factor is users. In our example of John Doe, people were infected because they visited the malicious web site driven by Doe's social engineering tactics. One reason social engineering is frequently successful is because many people trust what they see and are, by nature, not suspicious of certain online activities. Malicious social engineers know how to exploit human nature. A case study conducted by the U.S. Department of the Interior, points out that 84 percent of government departments attribute various security breaches to human error; 80 percent of the departments attribute these errors to a lack of security training, security knowledge, or failure to follow procedures.<sup>12</sup>

Hundreds of thousands of malware use social engineering to get installed on users' machines: this is one of the most common vectors of malware delivery. Matthew Braveman categorizes various installation vectors in four major categories.<sup>13</sup> According to his study, almost one-third of the malware was installed by leveraging social engineering methods.

Adware and spyware have adopted many popular social engineering methodologies and have come up with new techniques to distribute their software. Social engineering is the favored installation vector of the PPI model, which offers broader options for delivering adware and spyware. These applications can be delivered using apparently innocuous mechanisms, such as bundled freeware or by suspicious mechanisms, such as spam or email attachments with deceptive text. A user who wants freeware, for example, can knowingly install adware to use the free services. Even if an installation occurs via an exploit or direct spam, security companies may still not determine that the software is malicious because of vendor claims that they have no role in this distribution and that other people are exploiting their software.

Because most of the ad content is stored on servers and uses JavaScript, Flash, and other rich-content technologies, inserting malicious ads in the ad stream is not difficult.

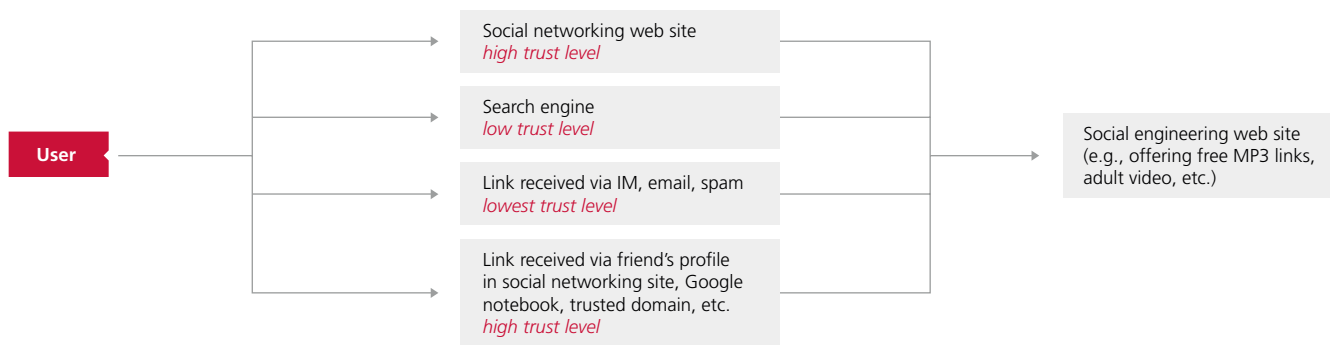


Figure 3: Several vectors expose users to unwanted and malicious programs.

## It's about trust

Figure 3 depicts four scenarios for user exposure to a social engineering site. Although the illustration is simple, it can help us understand the following real-world cases. The key is that the higher the trust level, the more likely a particular social engineering technique will succeed. We'll explain further using three brief case studies.

### Case 1: Social networking web sites

Social networking sites are a boon to social engineers because most people on these sites are looking to make or stay in touch with friends. Social engineers may create relationships to increase the trust factor, as shown at the top of Figure 3. The trust level is usually very high for this category.

A number of notable social engineering attacks have exploited this trust to install adware on users' machines:

- MySpace Adult Content viewer (*trust level: medium*). This incident relied on a user clicking a pop-up ad featuring young people with title such as "I want to be loved."<sup>14</sup> Clicking on these ads downloaded the MySpace Adult Content software that reportedly downloaded adware.
- MySpace Fraudulent YouTube Video (*trust level: high*). WebSense reported in late 2006 a fraudulent YouTube video that was posted on multiple fake profiles at MySpace.<sup>15</sup> Attempting to view the video required installing Zango Cash.
- Facebook Secret Crush Application (*trust level: very high*). In January 2008, Fortinet generated an advisory about a malicious widget called Secret Crush that was trying to install adware.<sup>16</sup> This social engineering tactic worked by first sending a Facebook request with the title "1 secret crush invitation." Upon opening this request, the user had to install a widget to find out who sent the secret crush. The request further prompted the user to forward it to five friends before it would display who sent the crush. Naïve users forwarded this message to friends, making this a social worm. After taking these steps all that users saw was a message to download Adware Zango. Victims were easily lured by this scenario because the trust level was very high.

### Case 2: Banner ads

Banner ads lie in the domain of the PPC model. The trust level in these real-world scenarios was very high, as users were visiting trusted site that they visited frequently.

- In 2006, *The Washington Post* reported a malicious banner ad in MySpace that served adware as well as Trojans to millions of users using Microsoft Windows Metafile exploits; this did not require any user intervention.<sup>17</sup>
- In 2008, we've seen an increase in malicious banner ads. The latest at the time we wrote this article was a Flash-based ad at *usatoday.com*.<sup>18</sup> Just by visiting the page, users were socked with multiple malware as well as fake alerts (a popular social engineering tactic) to download a rogue antispyware application called Malware Alert. (Rogue programs can include PUPs as well as Trojans.)

### Case 3: Other intriguing tactics

- Spoofed email (*trust level: low*). In one case, spoofed emails from eBay were spammed with the links pointing to download adware.<sup>19</sup> The social engineering aspect occurred in the content of the email, which "warned" unsuspecting users that there was a problem in their billing information and that they needed to update the data by downloading particular software.
- Fake error pages (*trust level: medium*). Certain web sites displayed fake "page not found" error messages and offered to resolve the situation by downloading an ActiveX component that installed WinFixer.<sup>20</sup>
- Google notebook spam (*trust level: high*). In a recent development, scammers used yet another social engineering technique by spamming links to Google notebook pages.<sup>21</sup> The hyperlink is in the format `www.google.com/notebook/public/[UserID]/[blocked]`. The domain `google.com` makes people less suspicious and encourages them to click on the malicious web pages, which host multiple links to adult sites or fake videos. These eventually download various rogue anti-spyware apps.

## A Silent Retreat

The initial lack of laws regulating adware and spyware applications gave lots of freedom to their developers, whether their motivations were merely financial or actually malicious. At first, users seemed protected because they had EULAs to warn them of any unwanted effects from these applications. But the EULAs were often confusing, incomplete, or unseen. Once found, they're hard to read—often enclosed in tiny windows that display only a few words at a time. With such an effective smokescreen, why have adware and spyware declined? Several factors have contributed.

- **Law suits** Due to an increase in abuses by adware and spyware apps, consumers and other plaintiffs have filed multiple lawsuits against some big distributors.<sup>22 23 24 25 26 27</sup>

Various court rulings have helped to limit the numbers of adware and spyware. In the settlement against Zango,<sup>12</sup> for example, the court “requires that Zango monitor its third-party distributors to assure that its affiliates and their sub-affiliates comply with the FTC order.” The ruling also “bars Zango, directly or through others, from exploiting security vulnerabilities to download software, and requires that it give clear and prominent disclosures and obtains consumers’ express consent before downloading software onto consumers’ computers.” Such orders have helped to weaken the PPI method and have driven ad distributors to clean up their acts.

- **Public awareness and industry groups** The Federal Trade Commission has an informative web site<sup>28</sup> that provides tips on how to protect against spyware and how to report abuses. The Anti-Spyware Coalition also offers a lot of information and details about this threat.<sup>29</sup> Due to the efforts of these organizations, both consumers and lawmakers have a much better understanding of the issues and rules related to online advertising. This increased awareness has helped to lower the occurrence of these unwanted applications.

- **Bad publicity and potential lawsuits against advertisers having association with adware companies** The money that drove the adware and spyware market initially came from advertisers that used adware companies to show the ads. These product and service companies did not at first fully investigate how the adware firms distributed their ads. In a historic settlement published on January 29, 2007,<sup>30</sup> the agreement stated that “prior to contracting with a company to deliver their ads, and quarterly thereafter, the companies must investigate how their online ads are delivered. The companies must immediately cease using adware programs that violate the settlement agreements or their own adware policies.” Because advertisers now understand the risks (invasion of privacy, improper consent, and others) associated with the PPI model, they are moving toward the PPC model, which requires no applications on users’ systems.

## Rogue Applications

Because malware authors gain easy money using scare tactics, there is an increasing trend to distribute rogue applications and fake “alert” Trojans, which display bogus error or infection messages. In most cases, the fake alert Trojans are the downloaders of the rogue applications that detect false registry keys and files as malware. Sometimes, these rogue applications drop the files just to detect them later; in these cases, the rogue application warrants a “Trojan” classification (such Trojans are included in Figure 4).

We have also observed many cases of adware installed by Trojans. The Downloader-UA Trojan category is one such family that uses social engineering tactics to download fake programs. Discovered in late 2004, this family employs loopholes in the way Microsoft Windows Media Player uses digital rights management technology by luring users to download specially crafted media files.<sup>31 32</sup> In 2008, the same family of Trojan was involved again in luring users to download a fake MP3 player to play a canned selection of songs; it also downloaded heaps of adware to their systems.<sup>33</sup>

The growth of rogue applications (PUPs and Trojans) has been exponential in 2008 when compared with previous years. (See Figure 4.)

To gauge the frequency of rogue anti-spyware products distributed via downloader Trojans, we analyzed a set of IP addresses involved in initiating these downloads. A query executed at domain hosts-files.net returned 158 domains associated with the same IP address.<sup>34</sup> (See Figure 5.)

### Rogue applications

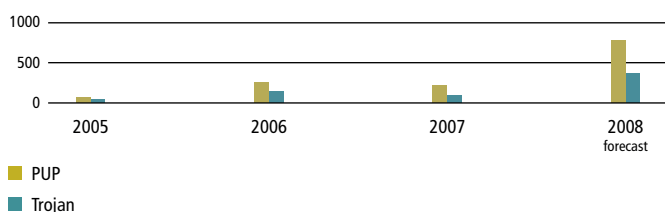


Figure 4: Unlike adware and spyware, rogue applications (PUPs and Trojans) have increased dramatically in 2008. (Source: McAfee Avert Labs).

This data has been pulled from the hphosts cache

Request removal | Report related site(s) | SiteAdvisor Report | Trusted Source

0 Additional match(es) found

No additional match found

158 Additional match(es) found for the specified IP address:

#	Hostname	IP	Class	
1	addioerror.com	67.55.81.200	FSA	Details
2	addioerrora.com	67.55.81.200	FSA	Details
3	anonymwinpc.com	67.55.81.200	FSA	Details
4	antispionagepro.com	67.55.81.200	FSA	Details
5	antispyswarecontrol.com	67.55.81.200	FSA	Details
6	antispyswareuite.com	67.55.81.200	FSA	Details
7	antiver2008.com	67.55.81.200	FSA	Details
8	barmedvirus.com	67.55.81.200	FSA	Details
9	bugdeestroyer.com	67.55.81.200	FSA	Details
10	confidentuser.com	67.55.81.200	FSA	Details
11	controlantispia.com	67.55.81.200	FSA	Details
12	defectlaworm2008.com	67.55.81.200	FSA	Details
13	defectshuri.com	67.55.81.200	FSA	Details
14	diannaoqingieji.com	67.55.81.200	FSA	Details
15	discozenzaerror.com	67.55.81.200	FSA	Details
16	disinfoc.com	67.55.81.200	FSA	Details
17	disinfectors.com	67.55.81.200	FSA	Details
18	disinfecturprotection.com	67.55.81.200	FSA	Details
19	disinfectur.com	67.55.81.200	FSA	Details
20	disinfecturhogo.com	67.55.81.200	FSA	Details
21	drive defender.com	67.55.81.200	FSA	Details
22	driveprotection.com	67.55.81.200	FSA	Details

Figure 5: Multiple hostnames map to a single IP address that distributes localized rogue applications.

Each of the domains shown in Figure 5 displays either a custom rogue anti-spyware or rogue “system cleaner” product. The pages appear in various languages, as well. In analyzing 620 pages, we found 24 languages used to create both pages and applications that show the threats have spread far beyond English-speaking countries. More than once, a single IP is associated with multiple domains; in some cases we saw up to 200 different domains. One query for the keyword “FSA” (which hosts-files.net describes as a class of domains hosting rogue applications) returned close to 3,600 domains distributing rogue applications.<sup>35</sup>

## Conclusion

Looking solely at an analysis of statistics suggests that the growth of adware and spyware is on the decline. However, the intriguing social engineering tactics that are used to distribute these PUPs are still with us, delivering rogue applications and Trojans. With the increase of the server-side model (PPC) of ad delivery, we will certainly see improved social engineering tactics luring users to click on these ads and generate revenue for the affiliates. The distribution of adware and Trojans will continue to gain ground at social networking sites. Although the overall number of adware and spyware has declined, we see no easy solution in the near future to the problem of unwanted programs. Because adware companies pay for such installations, their moral duty should be to keep track of each installation and quickly stop any potential misdistribution of their software. But will they really do this?

With the changing threat landscape and the increase in revenue-motivated Trojans, we have to remain vigilant and train employees and home users to better understand the threat of social engineering.



**Aditya Kapoor** is a senior researcher at McAfee Avert Labs. He was introduced to reverse engineering six years ago while researching at the University of Louisiana at Lafayette for his master’s thesis, which focused on a sliding disassembly algorithm to tackle code obfuscation. At McAfee, Kapoor developed skills in rootkit analysis, byte code comparison, and behavior analysis. He enjoys traveling and studying different cultures and architectures.

## ENDNOTES

- 1 <http://www.antispyswarecoalition.org/documents/2007glossary.htm>
- 2 OptOut, Gibson Research Corp. <http://www.grc.com/optout.htm>
- 3 [http://en.wikipedia.org/wiki/Compensation\\_methods](http://en.wikipedia.org/wiki/Compensation_methods)
- 4 Source: Zango web site. <http://www.cdt.org/headlines/headlines.php?iid=51>
- 5 <http://www.benedelman.org/news/062907-1.html>
- 6 [http://en.wikipedia.org/wiki/Compensation\\_methods#Pay-per-click\\_-\\_28PPC.29](http://en.wikipedia.org/wiki/Compensation_methods#Pay-per-click_-_28PPC.29)
- 7 <http://www.benedelman.org/ppc-scams/>
- 8 <http://msmvps.com/blogs/spywaresucks/archive/2007/08/22/1128996.aspx>
- 9 [http://www.theregister.co.uk/2007/09/11/yahoo\\_serves\\_12million\\_malware\\_ads/](http://www.theregister.co.uk/2007/09/11/yahoo_serves_12million_malware_ads/)
- 10 <http://www.secureworks.com/research/threats/ppc-hijack/>
- 11 <http://www.csc.com/cscworld/012007/dep/fh001.shtml>
- 12 <http://www.usgs.gov/conferences/presentations/5SocialEngineeringInternalExternalThreat%20Dudek.ppt>
- 13 [http://download.microsoft.com/download/c/e/c/cecd00b7-fe5e-4328-8400-2550c479f95d/Social\\_Engineering\\_Modeling.pdf](http://download.microsoft.com/download/c/e/c/cecd00b7-fe5e-4328-8400-2550c479f95d/Social_Engineering_Modeling.pdf)
- 14 <http://mashable.com/2006/10/11/myspace-adult-content-viewer-more-adware/>
- 15 <http://securitylabs.websense.com/content/Alerts/1300.aspx>
- 16 <http://www.fortiguardcenter.com/advisory/FGA-2007-16.html>
- 17 [http://blog.washingtonpost.com/securityfix/2006/07/myspace\\_ad\\_served\\_adware\\_to\\_mo.html](http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html)
- 18 <http://securitylabs.websense.com/content/Alerts/3061.aspx>
- 19 <http://securitylabs.websense.com/content/Alerts/738.aspx>
- 20 <http://www.avertlabs.com/research/blog/index.php/2006/12/04/404-not-just-file-not-found/>
- 21 <http://www.cantoni.org/2008/06/04/google-notebook-spam>
- 22 <http://www.benedelman.org/spyware/nyag-dr/>
- 23 [http://www.oag.state.ny.us/media\\_center/2005/apr/apr28a\\_05.html](http://www.oag.state.ny.us/media_center/2005/apr/apr28a_05.html)
- 24 [http://www.internetlibrary.com/cases/lib\\_case358.cfm](http://www.internetlibrary.com/cases/lib_case358.cfm)
- 25 <http://blogs.zdnet.com/Spyware/?p=655>
- 26 <http://www.ftc.gov/opa/2006/11/zango.shtml>
- 27 [http://www.ftc.gov/bcp/edu/microsites/spyware/law\\_enfor.htm](http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm)
- 28 <http://onguardonline.gov/spyware.html>
- 29 <http://www.antispyswarecoalition.org/>
- 30 [http://www.oag.state.ny.us/media\\_center/2007/jan/jan29b\\_07.html](http://www.oag.state.ny.us/media_center/2007/jan/jan29b_07.html)
- 31 [http://www.pcworld.com/article/119016/risk\\_your\\_pcs\\_health\\_for\\_a\\_song.html](http://www.pcworld.com/article/119016/risk_your_pcs_health_for_a_song.html)
- 32 [http://vil.nai.com/vil/content/v\\_130856.htm](http://vil.nai.com/vil/content/v_130856.htm)
- 33 <http://www.avertlabs.com/research/blog/index.php/2008/05/06/fake-mp3s-running-rampant/>
- 34 <http://hosts-file.net/?s=67.55.81.200&sDM=1#matches>
- 35 <http://hosts-file.net/?s=Browse&f=FSA>