

Fighting Spyware: An Encouraging Case Study



Spyware -- a term that defines the wide range of programs that are installed without appropriate user consent or which impair users' control over their computers and their personal information -- has emerged as a major threat to the continued health and evolution of the digital world. By compromising privacy and, in many cases, rendering users' computers useless or severely impaired, has created a troubling barrier to the free flow of information online and user control.

Although the term "spyware," and the technology it defines, emerged in 2000, it has become an exponentially larger problem in recent years as more activities are taken online. In 2003, the Center for Democracy & Technology suggested that spyware was becoming a major problem and suggested policy approaches to address it.

One in three consumers polled in 2006 by Consumer Reports had dealt with a spyware infection; one in 11 suffered serious damage as a result. Shockingly, this represents an improvement from past polls.

No single tool or solution has been developed to defeat spyware, combined legal, regulatory and technological efforts have shown some positive effect. In 2006, Consumers Report estimated that spyware cost consumers \$2.6 billion. In 2007, this cost is expected to drop to \$1.7 billion.

Work in these following areas can continue to help build on the recent successes in addressing the spyware problem and can serve a model for responding to other electronic threats.

For more information:

Ari Schwartz
(202) 637-9800

Technology

The most powerful tools we have in the fight against spyware are anti-spyware products. These programs right the balance between software distributors and consumers, by alerting users when a program tries to install itself on their computer, and giving them the choice of whether to accept it.

In 2005, CDT convened the Anti-Spyware Coalition (ASC). The ASC brings together anti-spyware software companies, academics, and consumer advocacy groups to develop best practices and standards for the anti-spyware industry.

Enforcement

The active enforcement of civil and criminal anti-fraud legislation is a critical deterrent in the war against spyware. High profile arrests and prosecutions of spyware distributors have shown that spyware is no longer an easy road to a big payoff. Settlements have reached as high as \$7.5 million, in the New York settlement with Intermix Media. There have been state, and federal (Federal Trade Commission and Department of Justice) actions against spyware distributors.

Legislation

Legislation enacted at the federal level allows American law enforcers to collaborate with foreign law enforcement. The U.S. SAFE WEB Act facilitates the arrest and prosecution of developers and distributors of spyware many of who operate internationally.

State legislation also allows prosecution of spyware distributors and developers. Washington State, for instance, has aggressively used legislation to pursue spyware vendors.

Market Pressure

By tracking the money from adware, consumer groups and governments can identify the advertisers who are taking advantage of spyware tools to market their products and services. In response to pressure from consumer groups and consumer protection agencies, many of these advertisers develop new policies for their advertising in order to ensure that they are not associated with spyware and unwanted programs. Specifically, the New York Attorney General has settled with advertisers who knowingly advertised through spyware.

Public education

All of the weapons that have been developed in the war against spyware are useless without education. Users need to know about the tools that can protect them, and wrongdoers need to know about the penalties they face for violating users' privacy and personal property.

Many educational sites help to keep the public informed and protected. Notable are GetNetWise (getnetwise.org) and OnGuard Online (onguardonline.gov).