

**Spyware poses a significant threat on the Net, according to new study**  
**Rob Harrill, rharrill@u.washington.edu**

Spyware is alive and well on the Internet. That's the overall message of a new study by Univ. of Washington computer scientists who sampled more than 20 million Internet addresses, looking for the programs that covertly enter the computers of unwitting Web surfers to perform tasks ranging from advertising products to gathering personal information, redirecting Web browsers, or even using a victim's modem to call expensive toll numbers. They examined sites in a set of popular Web categories, such as game sites, news sites and celebrity-oriented sites. Within these, they found that: (α) More than one in 20 executable files contained piggybacked spyware, (β) On average, one in 62 Internet domains performed drive-by download attacks -- a method for forcing spyware on users who simply visit a Web site, (c) Game and celebrity Web sites appeared to pose the greatest risk for piggybacked spyware, while sites that offer pirated software topped the list for drive-by attacks, (d) The density of spyware seemed to drop from spring to fall of last year, but remained "substantial." The research is being presented today as the opening paper for the 13th Annual Network and Distributed System Security Symposium in San Diego, Calif. "For unsuspecting users, spyware has become the most 'popular' download on the Internet," said H. Levy, professor and holder of the Wissner/Slivka Chair in the UW's Department of Computer Science & Engineering and one of the study's authors. "We wanted to look at it from an Internet-wide perspective -- what proportion of Web sites out there are trying to infect people? If our numbers are even close to representative for Web areas frequented by users, then the spyware threat is extensive." The consequences of a spyware infection run the gamut from annoying to catastrophic. On the annoying end, where most spyware falls, the stealthy programs can inundate a victim with pop-up advertisements. More malicious programs steal passwords and financial information. Some types of spyware, called Trojan downloaders, can download and install other programs chosen by the attacker. In a worst-case scenario, spyware could render a victim's computer useless. In conducting the study, the UW researchers -- Levy, associate professor S. Gribble and graduate students A. Moshchuk and T. Bragin -- used a computer program called a Web crawler to scour the Internet, visiting sites to look for executable files with piggybacked spyware. The team conducted two searches, one in May and the other in October, examining more than 20 million Web address. They also did additional "crawls" of 45,000 Web addresses in 8 subject categories, looking for drive-by download attacks. In the first two crawls, the researchers found that approximately one in 20 executable files contained piggybacked spyware. While most of those were relatively benign "adware" programs, about 14% of the spyware contained potentially malicious functions. In terms of drive-by download attacks, the researchers found a 93% reduction between May and October -- a finding they say may in part be attributed to the wider adoption of anti-spyware tools, automated patch programs such as Windows Update and the recent spate of civil lawsuits brought against spyware distributors. Despite that drop, the public should still be vigilant, they said. "Plenty of software on the Web contains spyware, and many Web sites are infectious," Gribble said. "If your computer is unprotected, you're quite likely to encounter it." There are a few steps that people should take to protect themselves, according to Gribble. "First, everybody should install one

or more anti-spyware programs," he said. "There are several high-quality free or commercial software packages available." It's also important to keep those tools up-to-date so new threats can't get around one's cyber defenses. Finally, Gribble said, people need to use common sense. "You should download software only from reputable sources," he said. "And it's a good idea to avoid the more shady areas of the Web."

### **Forum tackles Internet regulation**

**ISN SECURITY WATCH (31/01/06), E. Lyman, Rome**

The future security of the Internet does not depend on increased government regulation, according to a group of private sector representatives at a conference held on the future of the digital economy in Rome. Attendees included senior officials from some of the world's leading high-tech companies, including British Telecom, Deutsche Telekom, Electronic Arts, IBM, Intel, Google, Technorati, Wikipedia, and Yahoo!. They bristled whenever the issue of Internet regulation was brought up in a panel discussion. The symposium, dubbed the International Conference on the Future of the Digital Economy, was held between 30-31 January at the headquarters of Italy's Ministry of Culture, and hosted by the Organization for Economic Cooperation and Development. Several representatives said that individual companies had to take security-related steps on their own in order to avoid the risk of government intervention. "I hope we won't have to deal with an aggressive kind of government looking to regulate where there is no need - we haven't had that problem so far," D. Sifry, the president of Technorati, a company that monitors traffic on Internet blog sites, told ISN Security Watch on the sidelines of the conference. "If companies take steps to assure security and legal issues, then there will be no need for government regulators," he said. F. Brioschi, the president of Wikipedia-Italia, agreed: "I don't think any of the companies here want to see government regulation [...] but it's up to us to avoid it." Online security issues encompass several areas: the integrity of online financial transactions, the protection of personal information, and safeguards against the abuse of intellectual property. Issues related to the abuse of intellectual property have received the most attention in recent weeks, especially with regards to Google. The company's Google Book Search program aims to scan as many of the world's books as possible - regardless of whether the publications are in-print, or copyright protected - and make their contents available online. The initiative has attracted criticism from those who believe it infringes on the copyright of protected books. J. Redmer, the European director for Google Book Search, told the conference that the company saw the Book Search project as a way to call attention to books available for sale or in libraries, but not as a substitute for the books themselves. Only in the case of books in the public domain are complete texts available online, he said, and there are safeguards in place to ensure that information found using the Book Search technology cannot be printed or downloaded. P. Moll, Google's European policy manager, told ISN Security Watch that the company's policy in this area should protect it against government regulators. "We are operating on the assumption that regular copyright law is the regulatory structure that is relevant here," she said in an interview held between sessions. "We are not breaking any copyright laws and we don't see there being a need for additional regulation in this area." Other representatives took similar stances regarding other potential areas of regulation. "We believe the government should step in only when there is no other way," said Jung Ju Kim, the CEO of South Korean multiplayer game developer Nexon Corporation. Italian government officials and EU representatives largely sidestepped the issue of increased online regulation. However, Italy's Innovation and Technologies Minister L. Stanca told the conference that Italy, at least, would not shy away from considering regulation of the Internet if it was required - adding that for the most part it has not been necessary. "The government's job is to protect its citizens in every way pos-

sible," Stanca said. "If the need arises in the future, that could include increased regulation of the online world." Italy has previously taken some regulatory steps online, putting in place strict rules limiting the use of Internet domain names ending in ".it", policing defamatory web sites hosted in Italy, and limiting the online sale of illegal products and paraphernalia related to extreme political groups.