Spyware poses a significant threat on the Net

February 3 2006

Spyware is alive and well on the Internet. That's the overall message of a new study by University 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:

-- More than one in 20 executable files contained piggybacked spyware.
-- 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.
-- 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.
-- 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 Hank 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 Steven Gribble and graduate students Alexander Moshchuk and Tanya 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 eight 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 percent of the spyware contained potentially malicious functions.

In terms of drive-by download attacks, the researchers found a 93

percent 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."

Source: University of Washington

Citation: Spyware poses a significant threat on the Net (2006, February 3) retrieved 30 April 2024 from https://phys.org/news/2006-02-spyware-poses-significant-threat-net.html