

# Spyware poses identity-theft risk (Update)

September 15 2005

---

A new study finds that a growing amount of Internet spyware -- programs downloaded to users' computers without their knowledge -- is designed specifically to steal personal information that could be used for identity theft.

The study, conducted by Aladdin Knowledge Systems, a digital security company, found that 15 percent of spyware transmits users' keystrokes, user names, administrative passwords, e-mail addresses, contacts and instant-messenger login names and usage. The study was released Wednesday.

Aladdin's study looked at the top 2,000 known spyware threats and was conducted over two months. An Aladdin lab downloaded various types of malicious spyware, and then the company analyzed the spyware behavior, explained Shimon Gruper, vice president of Internet security technologies for Aladdin.

SurfControl, a theft-protection Web site, also announced this week that spyware and hacking sites grew by a rate of 90 percent over the last year.

Alladin's Gruper said spyware can be downloaded from Web sites that offer assistance cracking passwords to illegally downloaded software. Spyware can also come from advertisements for free software that purportedly eliminates spyware but actually installs it.

Programs can track keystrokes and analyze numbers to obtain PIN codes and passwords. Spyware can also be inside of an Internet browser so that

it traces and transmits information typed into forms, such as credit-card numbers.

Claudia Farrell of the Federal Trade Commission said nobody knows exactly how much identity theft is a result of spyware.

"We're not sure what the owners of those Web sites, what they will be doing with (the information) but ... this (personal) information is being sent out, and I'm sure that they will easily find out what to do with it," Gruper said. "If they know you access your bank's Web site with a username and password, it's a no-brainer what they'll do with it."

Some Web sites that release malicious spyware are run by individual hackers, but most are more sophisticated and organized, Gruper said.

The survey also found that 25 percent of spyware poses a moderate threat, transmitting information such as users' Internet Protocol addresses and logs of their memory processes.

Gruper said such programs are illegal because they invade users' privacy. Some free programs require users to sign an agreement saying that in exchange for the program, they agree to allow non-malicious spyware to monitor using habits. But others don't disclose anything.

"I'm not sure anything can be done about it because from what we've checked, the majority of these sites are in strange countries," Gruper said. "They disguise themselves as legitimate Web sites. I'm not sure anything can be done to block them," Gruper said.

Internet Service Providers could help the problem, Gruper said, explaining that they have more of an ability than Internet users to know which sites are safe and which aren't. Gruper said that such a system is feasible, but ISPs must be willing to establish those safeguards.

"Maybe they should put up some fences and maybe display a warning ... or edit security so that by mistake you don't go to places that can be potentially dangerous," Gruper said.

*Copyright 2005 by United Press International*

Citation: Spyware poses identity-theft risk (Update) (2005, September 15) retrieved 26 June 2024 from <https://phys.org/news/2005-09-spyware-poses-identity-theft.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.