

20 November 2008

By: Lucian Constantin, Web News Editor



RemoteSpy website
shut down by a judge
CyberSpy Software

Commercial Spyware Vendor Hit with Restraining Order

The software sold by the company displayed rootkit and antivirus evading behavior

A federal judge has signed a temporary restraining order, prohibiting CyberSpy Software, LLC to sell its popular RemoteSpy product, after the Federal Trade Commission (FTC) filed a [complaint](#) (PDF file) against the company for violating the fair trade law. The company advertised their software as being 100% undetectable, and instructed their customers on how to install it on the computers of their unsuspecting victims.

CyberSpy Software, LLC is based in Florida, and is owned by Tracer R. Spence, who has also been cited as a defendant in the complaint submitted by the FTC. "Spence, individually or in concert with others, has formulated, directed, controlled, or participated in the acts and practices set forth in this complaint, and has done so at times pertinent to this action."

According to the company, the RemoteSpy program has the possibility to "record keystrokes, screenshots, email, passwords, chats, instant messenger conversations, websites visited and more." In the complaint filed by the FTC it was noted that the "defendants provide RemoteSpy customers with instructions on how to disguise the software as an innocuous file, such as 'photos' or 'music' attached to an email, in order to send the software to another computer."

The program sends collected information about everything the victim does online, to the company's server, at every 10 minutes. The information is then made available to the company's clients to see and use. The offline activity of owners of the infected computers is not safe either, because if there is no Internet link, the program stores the data locally, and waits for an uplink to be restored. It will then proceed to upload the stored information on CyberSpy's servers as usual.

"The invasion of privacy and security resulting from collecting and disclosing confidential consumer information, without the computer owner's knowledge and authorization, causes, or is likely to cause substantial harm to consumers and the public," claims the FTC. "Defendants' actions cause, or are likely to cause substantial injury to consumers that cannot be reasonably avoided, and is not outweighed by countervailing benefits to consumers or competition," the complaint adds.

As CyberSpy Software is not the only company selling what they refer to as "legitimate" spyware, further similar actions are expected from other businesses as well. The Electronic Privacy Information Center has previously submitted a complaint to the FTC regarding several online websites marketing such products, including CyberSpy Software, complaint that might have prompted this lawsuit.

"Such products typically promote themselves as a way for wives to spy on philandering husbands, or for concerned parents to keep an eye on what their babysitter is up to, rather than more traditional identity theft - but it's clear that they can be used with a wide variety of motives," explains Graham Cluley, senior technology consultant at Sophos, with regard to why these programs are dangerous.