Who's Seeding the Net With Spyware?

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Young surfers pick up paychecks for posting misleading pitches armed with invasive programs.

It's tough enough sometimes to figure out where you picked up that spyware, but have you ever wondered who planted that digital parasite?

It's likely a young man, maybe a college student, just making a few bucks spreading pop-up ads that contain a package unwelcome by many. And it's a growing cottage industry.

How It Works

Spyware follows your Internet surfing habits and serves up advertisements. You typically pick up spyware by clicking on links, which may not make it clear that you're downloading a "bonus" program when you read an ad or download a program you want.

The Federal Trade Commission defines spyware as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." The federal government and several states are considering antispyware laws, and Utah recently enacted one.

FTC and industry leaders have urged Congress to resist spyware legislation, instead pushing for the industry to adopt self-regulatory practices. They fear that proposed laws define the practice too vaguely, and would prohibit other marketing practices that benefit consumers. But some lawmakers worry that the tech industry will not regulate spyware aggressively enough to protect consumers.

Meanwhile, computer users continue to face the side effects of spyware on their systems: bogged-down Internet connections, identity theft, lost documents, system problems, and potential loss of privacy.

Who's Behind It

The people distributing the links for spyware downloads are paid about 15 cents every time an unsuspecting surfer clicks on their misleading bait.

"Friends signed me up one night, after we'd been drinking," says one twenty-something man, who plants spyware for pay. "They said it was an easy way to make some money."

"All I had to do was sign up and post fake ads, saying things like 'to see my picture click here.' Then when they clicked, it told them they had to download software to see the pictures."

But the user downloaded no pictures; instead, they got the greeting, "Come back later to see my photo." The ad is bogus, but the contamination of the computer is real.

He says open forums and other unregulated sites are the best places to post ads, because large numbers of people are likely to click on the phony links.

"You have to move around," he says, noting that if users complain, he'll be kicked off a site, or a section of a site. For example, he will just move to a different part of a classified advertisement site, he says. "It's really easy, so reposting your ad is not a big deal."

At 15 cents per hit, he got checks every two weeks for a few hundred dollars each.

"I could have made a lot more," he says, adding that he really isn't doing it anymore. "All I had to do was put more ads up and I would have doubled or tripled my profits."

What's the Risk?

The foot soldiers who spread spyware may also become victims of the companies behind the software.

Many companies paying individuals to spread spyware post a disclaimer on their own Web site. It often contains a clause telling readers that if they commit fraud the company has the right to pull their paycheck.

However, the new Utah Spyware Control Act and other privacy laws sometimes invoked to combat spyware consider posting spyware to be fraud.

The spyware spreaders may not be reading the disclaimer themselves. But they do understand the company is paying them to trick people into downloading software, the young man says.

Does he feel any remorse for contaminating the computers of naive users? "Look, they're perverts if they click on my ads," he says, noting that the ads imply pornographic pictures await. "I say some nasty stuff, so, no, I don't feel bad." Anyone online should have a spyware blocker, spam blocker, and a firewall anyway, he said. "If they don't, they're just stupid."

A Challenging Battle

Placing ads online can be a tempting and easy way to make money from home, notes Ray Everette-Church, chief privacy officer for antispam product vendor Turn Tide.

"It is very successful," Everette-Church says. "Hundreds of thousands of dollars a month is generated in this tiered structural referral." He is serving as an expert witness for the plaintiffs in an ongoing adware case arguing against pop-up ads.

Millions of Americans online haven't protected their PCs, and pursuing perpetrators of spyware is more complicated than in other criminal investigations, according to Mozelle Thompson, an FTC commissioner.

"It's hard to identify how many companies are engaged in dangerous spyware, or spyware in general," Thompson says. "The definition of spyware is too broad."

The surreptitious nature of spyware makes it more difficult to track who, where, and how the spyware is disseminated, Thompson told a House subcommittee at a recent hearing.

"Consumer complaints, for instance, are less likely to lead directly to targets than in other law enforcement investigations, because consumers often do not know that spyware has caused the problems or, even if they do, they may not know the source of the spyware," he said at the April hearing.