From:
Posted At: Tuesday, April 06, 2004 8:48 AM
Posted To: spywareworkshop2004
Conversation: Information Highway Robbery
Subject: Information Highway Robbery

Hi!

I'd like shopping application parasites *gone*. I have replaced my computer twice because of having it rendered inoperable by stealth downloads of remotely updateable shopping applications.

It should be made a criminal offence to profit from this in any way. If it is only a crime to make the actual software, the process will be farmed out overseas.

It needs to be so that anyone with a connection to it - writer, seller, promoter, merchant advertising on it, affiliate network hiding these people, host hosting a site where it is downloaded from - *all* of these people need to be criminalized, and you might think about including the shopper who knowingly has it on their machine too.

It should be noted that a 'tracking cookie' is perfectly acceptable. A tracking cookie allows site preferences to be remembered and commissions awarded. They are not a security risk. Tracking cookies save everyone time and effort and if anyone doesn't want cookies they can switch them off quite easily. Anyone claiming Adware is good and Spyware is bad is trying to divert attention away from their computer hijacking antics. They rely on your ignorance of what a cookie really does. There is a big difference between a site using a cookie to greet you by name and remember your login details and when it was you last visited, and a parasite following you *wherever* you go and altering your computer to its liking.

You can delete a cookie or tell your computer to not accept them. Cookies cannot hijack a machine and turn it into a weapon. A software parasite is far more complex and can do whatever it likes.

Just try deleting the new shopping parasite from 180 solutions! It is physically impossible. The files are 'invisible'. You need to buy a new computer if you want it gone, and if installed on a government or military network is a security risk worse than Osama Bin Laden.

It is hidden, nasty and unlike a cookie *completely* remotely updateable at any time. It could be used to create havoc - bringing websites or computer networks down (because of the way several million computers can be made to instantly act in concert at the whim of a parasite) hack into a network, steal sensitive data, execute whatever commands the parasite company wants to execute, or merely for extortion. It is a backdoor into any machine it is on - and the user 'consented' to this. Allegedly. But who is going to have to explain things when you have a body count on your hands?

Its not the user, is it? Its the government.

The people behind these applications are not the kinds of people who would ever be granted security clearance, so why they are getting carte blanche to do as they wish with the worlds IT infrastructure is beyond me.

There is a disaster here waiting to happen worse than anything you could ever imagine, and I would respectfully suggest you don't want it happening on your watch!

If you want to see how prevalent these parasites are, check out my site at http//cleanmerchants.com and click on some names. These are the companies whose affiliate managers are funding the parasites by paying them commission every time they steal a sale (from one of their real salespeople). The information on their backers is collected from the parasites own websites.
You might be surprised to see some well known names behind the info terrorists.

Alex Miles
(webmaster)

London