From: Mary Winfield
Sent: Tuesday, April 06, 2004 7:59 PM

Dear

I responded to the FTC call for security panelists for its April 2004 Spyware Workshop in Washington DC.

Here is the content of my email which was sent last week:

I am responding to the FTC agency's announcement of a Spyware workshop scheduled for April 2004 in Washington DC and would like to participate as a panelist. My background includes over 20 years of computer security in both mainframe and small system client/server technology. My firm, Platinum Precision Software Inc was founded in 2001 to respond to the demands of North American IT users who required a better security architecture and management of their critical data center resources.

My firm's recent accomplishments include Wireless 802.11 and Bluetooth security lab testing for the Windows XP and Linux Platforms, mainframe security integration of a new IBM LDAP and Firewall offering to be available for its large scale MVS systems (co-exist with traditional RACF, Top Secret and ACF2 mainframe security environment), security assessment planning techniques for enterprise computing environment and recent Canadian Government mainframe assessment for its Public Works PWGSC agency. My lab performed research in the Spyware tools area for today's internet user, both business and residential activity, and came up with a portfolio machine build containing spyware cleanup, spyware prevention and spyware interactive detection. Many of the customer accounts I have consulted in do not have these tools installed on their corporate desktop deployment "build".

Spyware is an intrusive maeasure which violates the PC desktop ownership by installing

My professional interest as a security practitioner with Spyware is both of a technical and legal nature. It is electronic trespassing on the PC owner's hard drive and operating system, secretive and its marketing ends do not justify the means. If legislation is going to be constructed and passed to prevent its activity in the US and Canada, then the FTC must define certain desktop computing environment components and of course the idea of "ownership" of the desktop resource.

Spyware is only prevelant in PC desktop computing as opposed to mainframe or mid-range computing platforms. It affects the consumer, both private and business user. It must be stopped dead in its

tracks.

I would like very much to be in Washington DC as an active participant in this workshop and can offer pro-bono the benefit of my experience as a security professional.

Just to outline my past
projects, my resume is attached for your review. It is a history of my project work, I am very busy with this Canada Public Works security project but wanted to email your office when I learned of the April workship.

Warm Regards,

Mary

Mary B. Winfield
Platinum Precision Software Inc.

PLATINUM PRECISION SOFTWARE, INC.
Mary B. Winfield
Statement on Spyware: Calling for Federal Statutes Banning PC Spyware
Submitted to the Federal Trade Commission
Spyware2004 Conference - April 2004 Washington DC

Spyware is an intrusive technology tool which is responsible for privacy loss affecting both business and consumer Internet users. It is unique to the widespread use of the Internet and is a mechanism which sends private information back to its “sender” about the desktop user's purchasing activity, personal data and other information.

Platinum Precision Software has a strong interest in pushing for preventive, restrictive statute law preventing Spyware at the federal and state/province level. Banning Spyware activity by legislative means will classify this intrusive technology activity as a crime.

Spyware is a technical and consumer threat unique to the Internet explosion. Its activity is an invasive electronic trespassing with cookie and executable objects on the PC owner's hard drive and operating system. Spyware is designed to be secretive and operationally clandestine. However its marketing ends do not justify the means.

Spyware process is not merely limited to a PC owner's Internet browser session. Spyware operation involves the secret embedding of cookies into system directory on the PC hard drive, installs programs without the PC owner's permission and all of this activity is behind the scenes.

It cannot be controlled with commercial Virus prevention software. "Malware" is planted behind the scenes of an average browser session using Internet Explorer or Netscape. Most of the aggressive tools to filter Spyware activity and complete a thorough cleanup are found as free tools, such as SpyBot Search and Destroy. And Spyware is responsible for CPU performance degradation and poor response for PC systems if it is not removed.

Federal legislation must be quickly constructed and enforced to prevent Spyware activity in the US and Canada; other countries must address this threat as well.

Additionally both private sector and the FTC must define certain desktop computing environment components which are technology based including Information Security.

Information Security policy is based on the principle of data “ownership” and any “access” to data being granted permission solely by the owner. “Access” is not something which can be stolen: no marketing company has the right to burglarize a private citizen’s personal computer using the Internet. Yes, it is electronic burglary. The privacy and data integrity of a business or consumer PC desktop are important and are attributed to the idea of "ownership". Access should only be granted by the desktop owner, not invaded by an advertising process which silently, secretly climbs into the boundary of a private citizen's hard drive like a burglar.

Spyware is only prevalent in PC desktop computing as opposed to the traditional mainframe or mid-range computing platforms. It affects all consumers, whether private citizen or business user. It must be stopped dead in its tracks and outlawed by federal statutes.