From: Just1Vet
Posted At: Tuesday, April 13, 2004 10:13 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

Spyware is a gigantic problem. I am the IT person for a three county area. We have over 60 public access machines and around 100 employee's machines. I spend about 8 hours a week removing this crud. The public access machines I have locked down as tight as I dare to go before they become unusable. HOST files are close to 50 pages in length, Spyware Blaster installed, as well as Spybot Search and Destroy.

Still they get through every safeguard I can put on it. I am about as techno savvy as you can get. And if I am having this much problems, I pity the poor common user. Many of these programs all you have to do is type a web sites name in error and your machine is infected big time. No warning, nothing noticeable when it first happens.

For the life of me on Gator, I have never figured out why virus scanner makers were so scared of picking the gatortrickler as a Trojan. The sole purpose of the Gatortrickler was to download Gator onto your machine with out your knowledge or permission. If you went to the Gators website and downloaded the program, trickler was not part of the download. I can provide you a long list of sites that all you need to do is hit the site and you're infected. Some of these sites are quite legit and a person would never think about it trying to download an unwanted program on you.

Gator is quite tame as far as removal goes to the rest of the malware out there. Huntbar, for example installs some registries that can not even be removed through Regedit, you have to use the reg32edit and take control of the object or the thing will continue to re-download on you. Cool Web Search is about as tenacious as it gets, now it even targets Spybot S&D and Adaware to cause them not to run. NewDotNet ingrains itself so much into winsock that the removal of it will cause you to lose connection to the internet even a reinstall of your operating system won't cure. You either have to do a format c:\ or get a special LISPfix program to regain connection.

I have just listed a few, there are many-many more. My question is: How many billions of dollars is it costing we the users and taxpayers just to keep these programs off of the machines just in the Federal, State and Local Government areas (including Libraries and Colleges)? I am sure the time it takes to remove these viruses and the loss of man hours and production are astronomical.

I feel very sorry for all the home users that have had their machines infected. Many don't even have a clue as to why their machines are slowing to a crawl. I have seen machines that over 70% of all the CPU cycles went to just feeding the malware. I have seen both machines at my work and at peoples home turned into a server do to a Trojan just so some sleazy outfit could use it as a server to send out Viagra e-mails. I've seen telephone bills of 900 numbers because a dialer snuck in. All this done without our knowledge or consent.

Do we need to do something about it? A most definite Yes. I see this Adware, Malware, and Spyware as a war we need to win. And right now the bad guys are winning.

Thanks

Roger Frederick
KS