

RE: Spy-Ware Detection for Small Networks

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-04/0331.html>

From: Bob Beck (*goodfela26_at_finneganfamily.net*)

Date: 04/26/04

To: <security-basics@securityfocus.com>

Date: Mon, 26 Apr 2004 13:50:49 -0400

SpyBot and Ad-Aware seem to work well in tandem.

I haven't tried Ad-Aware Pro, but since it has the ability to monitor the pc in the background, I would have to say it's at least as good as the free personal version. Downside to the personal version is that it's for personal use only.

As for Spybot, you can schedule a job on each pc, which is time consuming at first. In the command line, you use the following options: /autoupdate /autoimmunize /autocheck /autofix /autoclose and then either /minimized or /taskbarhide.

Go to <http://www.safer-networking.org/index.php?page=faq&detail=30> for a list of command line parameters for spybot.

Go to <http://www.lavasoftsupport.com/index.php?showtopic=19588> to see some examples of command line parameters for Ad-Aware.

Hope that helps,

Bob Beck

-----Original Message-----

From: Thiago Lima [mailto:thiagolima@webforce.com.br]

Sent: Sunday, April 18, 2004 11:16 AM

To: security-basics@securityfocus.com

Subject: Spy-Ware Detection for Small Networks

I run several small networks using a Linux Server to act as a Firewall/Proxy HTTP/Mail server/Caching DNS/DHCP/Samba File Server for Windows networks (98/XP/2000).

I also do desktop maintenance and I'm seeing a growing problem in Spy-wares and malware. It is becoming unmanageable to deal with it.

I've tried to educate users, but they really seem not care, they click on everything they can.

RE: Spy-Ware Detection for Small Networks

SecurityFocus BASICS: RE: Spy-Ware Detection for Small Networks

So I'm looking for some solutions that can make my life easier, and I want some comments on what I've come thru to try to find a balance between all solutions that can prevent most infections and keep the usability of the system.

1) Spy-bot : Looks to me that it is the best tool to remove spyware/malware, but it is host directed. It's hard to run it on all machines periodically. There's any way to centralize it ? Or there's any other program that will run in a centralized way?

2) Firewall blocking List : I've seen some IP lists that will prevent spywares to "call home". It is usefull to detect machines that are infected and blocking spyware to call home, but it does not prevent users from getting dirty. It helps a lot and I'm using <http://www.geocities.com/yosponge/> list. Does anyone knows others lists?

3) Content filtering : Viruses spreads by mail, spyware/malware spreads mostly by HTTP. Maybe filtering some words/patterns in HTTP Proxy I could block some problems. Dans-Gaurdian seems to be a solution for this. Does any one knows any list of words/sites, file extensions or any alternative to this?

4) Removing user access to his own machine : Removing users privileges (at least in XP/2000) will make spyware/malware infection harder or not? Looks to me that at least IE infections still contiunes. At opinion on that?

5) IDS : Using snort or any other IDS will help me with malware/spyware detection?

Is that all I can do? I'm open to any tip, solution or reading that can help me with this annoying problem.

Regards and thanks in advanced for all replys,
Thiago Madeira de Lima.

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at: http://www.infosecinstitute.com/courses/ethical_hacking_training.html

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors.

SecurityFocus BASICS: RE: Spy-Ware Detection for Small Networks

Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

Visit us at:

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
