

Ohio University Computer Services Center October, 2004 Spyware, Adware, and Virus Guide



Definitions

Malware – is term meaning malicious software. Malware is software designed to disrupt a computer system. A trojan horse , virus , or worm would be classified as Malware. Some advertising software is malicious in the way it installs without permission and can try to reinstall itself after you remove it.

Spyware – is a term for software that collects personal data like names and e-mail addresses without a user's consent. It is usually installed on a computer as the result of downloading a new program. It can often cause system slowness, crashes, and problems in general.

Adware - gathers user information for the purposes of advertising, installing programs, and sending cookies to other spyware programs. Some adware will push popup windows based on keyword searches and visited websites.

Virus – A parasitic program written intentionally to enter a computer without the user's permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Some viruses do little but replicate others can cause serious damage or effect program and system performance.

Trojans –destructive programs containing hidden code which can view, modify, and delete data; monitor your actions online; and use one computer to attack other computers. They often can have backdoors that allow hackers access to your computer.

Computer Worm –A self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another

Computer Services' Central Technology Services http://www.ohio.edu/cts executable program; however, a worm is selfcontained and does not need to be part of another program to propagate itself.

Web bugs - are tiny graphics placed on a website or e-mail designed to monitor who is reading the web page or e-mail message.

Key logging - software can record each keystroke made on a computer. The data it gathers, which often includes passwords and screen names, can be stored for later retrieval.

Phishing - programs use fake web sites and emails (spam) to trick users into giving away private information like credit card numbers, account usernames and passwords, and social security numbers. Phishers lure users to harm by mimicking the names and appearance of trusted web sites and organizations. Once the user feels safe, they often unwittingly give up personal information to the "phishers."

Symptoms

The following are possible symptoms to watch for to determine if your machine has Malware problems. They are not 100% certain indicators of an infection or software problem since some hardware problems could also produce similar problems. Also normally installed software can conflict as well.

Slow Computer – Slower then normal when opening and exiting programs and going to the Internet. Perhaps starting up and shutting down is slower or not working properly.

CPU and **Hard Drive** – If the CPU is in constant use or hard drive constantly spinning and in use your computer may be infected.





Popup Ads – If the popup ads seem out of control perhaps spyware is to blame.

Hijacked – Some adware takes control of your web browser and takes you to pages not of your choosing.

E-mail – Some viruses will use your email account to propagate. If you see out look opening unexpectedly or get bounced messages you may be infected.

Computer Crashes – Some Malware can even cause the computer to be unstable and crash. In the past referred to as the Blue Screen of Death.

Windows 95, 98, ME, and 2000



Windows XP



Downloading and Installing Spyware and Adware Tools

Computer Services' Central Technology Services http://www.ohio.edu/cts

The two software programs suggested by the Ohio University help desk for spyware and adware removal are Ad-Aware by lavasoft and Spy Bot - Search and destroy by PepiMK Software. The help desk suggests you install both programs and run them once a week to keep your system clean. You should also check for updates weekly as well. These two programs used in tandem seem to do a good job of catching and removing these forms of malware. The best part is they are free.

The Sites:

http://www.download.com/

http://www.lavasoft.de/ - Ad-Aware

<u>http://spybot.safer-networking.de/en/index.html</u> -Spybot - Search & Destroy

Installing and Running Ad-Aware

The file you download will be named something like aawsepersonal.exe, find where you downloaded this to and double click it.



You will see the intial install screen appear. Click Next



License Agreement		
	LAVA	so
Nicolas Stark Computing AB - Software Lic	ense Agreement	^
Please read the terms and conditions of this installing the computer software (the "Softw accept and agree to the terms of this Licen concerning the Software between you and any prior proposal or representation. If you promptly uninstall the Software and, if you refund of the amount that you paid.	is license agreement (the "License") before ware"). By installing and using the Software you see. This License constitutes the entire agreement I Nicolas Stark Computing AB and it supersedes do not agree with these terms and conditions, paid for a License, contact your distributor for a	
The term "Software" includes, and these te modifications and upgrades to the Software	erms and conditions also apply to, any updates, e that you may receive from time to time.	
1. License Grant. This License permits you	to use one copy of the Software solely for your	~
T I accept the	license agreement	
asoft Installation Wizard		

You must accept the license agreement to install the software so click in the box. It is not a bad idea to read license agreements on software some even reveal that spyware is going to be installed. The problem is most people just click yes and next and move on. After you have agreed to this one and check the appropriate box click next.



If you have a previous version of Ad-aware installed allow it to be removed. Click next.

🖁 Ad-Aware SE Personal			
Uninstalling previous version of Ad-	Aware		
			LAVASOF
Uninstall Successful!			
AL 187 177 1			
avasort Installation Wizard			
	< <u>B</u> ack	<u>N</u> ext>	Cancel

Click next.

遏 Ad-	ware SE Personal 🛛 🔀
Desti	ation Location
	LAVASOFT
S	up will install Ad-Aware SE Personal in the following folder.
T	install into a different folder, click Browse, and select another folder.
Y	i can choose not to install Ad-Aware SE Personal by clicking Cancel to exit Setup.
	estination Folder
	\Program Files\Lavasoft\Ad-Aware SE Personal Browse
Lavasoft	stallation Wizard

If you are satisfied with the default install location click next.



🔏 Ad-Aware SE Personal	
Install to All Users menu	
	LAVASOFT
The settings for this application can be in share this computer. You must have admi and Ad-Watch. Install this application for:	stalled for the current user or for all users that inistrator rights to install and run Ad-Aware
Anyone who uses this computer	
C Only for me (grammer)	
Lavasoft Installation Wizard	
	< <u>Back Next></u> Cancel

This software I would normally leave open to anyone. Click next.

🔏 Ad-Aware SE Personal	
Start Installation	
a destance of the	LAVASOFT
You are now ready to install Ad-Awar	e SE Personal.
Press the Next button to begin the ins	stallation or the Back button to reenter the installation
Lavasoft Installation Wizard	
	< Back Next> Cancel

Click next

Ad-Aware SE Personal	Ad-Aware SE Personal has been successfully installed. Press the Finish button to exit this installation.
Ad-Awarese personal	 Perform a full system scan now Update definition file now Open the help file now
	< Back Einsh Cancel

Decide if you want to read the help file now and I would leave the update on and perform a full scan now by clicking finish. Ad-Aware will now do an auto update and then begin search your computer for spyware processes and files.

	Werese	w w w
nizacija (kala basis) [1] Status	Performing System Scan	
Scan now	Current Operation	
	Scanning local memory	Objects Scanned: 534
Ad-Witten	C:\WINDOWS\System32\Cabinet.d	Ш
😭 Add-one	Summary	
🕑 Holp	7 Running Processes 264 Process Modules	0 Processes Identified 0 Modules Identified
	0 Objects Recognized 0 Objects Ignored 0 New Critical Objects	0 Registry Values Identified 0 Registry Values Identified 0 Files Identified 0 Folders Identified
	New searches the "Cartal" to doe	V faced

As it progresses it will inform you of the number of objects found. It will identify if these are processes, Modules, Registry keys or values, files, or folders. If browse much on the internet you will invariably pick up some cookies that will be found and seen as files of an Ad-ware nature.



When it is done scanning you will see a window similar to the one below.



You can now learn more about the items detected and select which you want removed or quarantined. A fast way to select them all is click the scan summary tab and check each of the boxes. Then click next.



The status box above tells you what has been done. Clicking next would take you to the scan now screen. Since we have just scanned we do not need to do it again for a week or so.

Ad-Watch and Add-ons are additional features of the program that require you to purchase a commercial version. We are now done and can close the program by clicking the "x" in the upper right hand corner.

Installing and Running SpyBot: Search and Destroy

Find the file you downloaded, it should be something like spybotsd13.exe. Double click it to begin the installation.

Select S	Setup Language 🛛 🔀
12	Select the language to use during the installation:
	English 💌
	OK Cancel

Choose your language and click OK.

🕏 Setup - Spybot - Search & Destroy		
	Welcome to the Spybot - Search & Destroy Setup Wizard	
	This will install Spybot - Search & Destroy 1.3 on your computer.	
	It is recommended that you close all other applications before continuing.	
	Click Next to continue, or Cancel to exit Setup.	
	Next > Cancel	

Click next to move on from the intro screen.



j률 Setup - Spybot - Search & Destroy	
License Agreement Please read the following important information before continuing.	
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.	
Dedication Public License (DPL)	^
By downloading the archive, you confirm your agreement in this license.	
I. Freeware First of all, the reasons why Spybot-S&D is free:	
I.a. Dedication Spybot-S&D is dedicated to the most wonderful girl on earth :)	~
accept the agreement	
◯ I <u>d</u> o not accept the agreement	
< <u>Back</u> Next>	Cancel

You must accept the license agreement in order to install the software. It is good practice to read these. Click next after accepting.

🕼 Setup - Spybot - Search & Destroy		
Select Destination Location Where should Spybot - Search & Destroy be installed?		
Setup will install Spybot - Search & Destroy into the following folder.		
To continue, click Next. If you would like to select a different folder, click Browse.		
C:\Program Files\Spybot - Search & Destroy Browse		
At least 8.9 MR of free disk space is required		
At least 0.5 Mb of free disk space is required.		
Cancel		

If the default install directory is okay click next to go on. Next will be an options menu for the default selections will be okay for most users.

👘 Setup - Spybot - Search & Destroy			
Select Components Which components should be installed?			
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.			
Custom installation	<u> </u>		
Main files Icons for starting blind user mode Additional languages	2.4 MB		
Skins to change appearance	0.3 MB		
Current selection requires at least 9.2 MB of disk space.			
< <u>B</u> ack Next	Cancel		

Click next to continue.

🚯 Setup - Spybot - Search & Destroy
Select Start Menu Folder Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Spybot - Search & Destroy Browse
Don't create a Start Menu folder
< <u>Back</u> Next> Cancel

The start menu selection should be okay click next.

Computer Services' Central Technology Services http://www.ohio.edu/cts





More options the default selections should be okay click next to continue.



Click install.



Click finish to run Spybot: S&D.

Computer Services' Central Technology Services http://www.ohio.edu/cts



This is not a bad idea click the "Create registry backup" button. When finished click next.

Spybo	t-S&D Wizard
Before sugge the bu new u	e you start your first scan, for your own safety it is strongly isted that you look for updated files and download them! Just click itton below to go to the updates page and let the program search if ipdates exist.
	Search for updates
	Download all available updates
0	N <u>e</u> xt

Click the search for updates button. Then click download all available updates, if any were found.



The Mode Largeour	10 Undate			24431-2740	
-	Get the newsel threat recognition rules online				
Lauri L Contra Contra Stationer	🔊 Search for Updates 🗿 S	ale: Nativotking #1 (Ex	rope) 🔹 🌏 Dowelland Updates 📑 Show Log 🔞 Help		
	Use this option	n if you want to know	Spybot SUD Wizard		
	This program will not send any initial (You'l need an open internet conver-		Before you shart your less scan, ho your own safety it is storydy suggested that you look for updated likes and downlaud them hart click the hutth solution to go to the updates page and let the program search if new updates exist.	atlin hon ny seborron.	
	Update	into		Date	
Update	Cetection siles	Updated detection Encloh help Sir (12)	Search for updates	2004-05-14 2004-05-30	
&	English help for TeaTimer	English help file for Updated Invision	Download all available updates	2004/05/25 2004/10/14	
	C A starbus	oppared manufi en		20041014	
			O Nor		
		1.0			





Click immunizes this system.

Spybot-S&D Wizard
Now that you are up-to-date, it is recommended that you apply some basic Immunization. Just click the button below to do this. If you do not want to immunize at this point, you can do this any later time by clicking on Immunize in the program toolbar at the left.
Immunize this system
Immunization has finished. 2254 bad products are now blocked.
N <u>e</u> xt

Click next.

Computer Services' Central Technology Services http://www.ohio.edu/cts

Spybot-S&D Wizard
All initial settings have been done. For more information, it is recommended you read the help file. After that, you can start using Spybot-S&D.
Read tutorial
Read help file
Start using the program

Choose if you wish to read a tutorial or the help file. Finally click start using the program.

Soybet - Search	a Destroy	L 🖉 🐹
File Mode Language	: Meb	- and the second
= Seybor S4D	Scan for problems and remove them	
Samth L Centry	P Deck for problem 🖓 Der 😢 Beb	
	This is the name score page of Spitol 55D. Here you can you when "Devis to problem" buried and he way publies that were based (This when the buried) life if you based down to get, we accompany when the buried and the score induction to the during the score induction.	d problems"
and the second	The second se	-
		4

Click the search and destroy icon on the top left of the screen. Then click check for problems.

The program will begin looking for potential problem files and list them in the box. These two programs used in combination offer a good approach to catching many spyware and adware programs.





A few files were identifier as potential problems and marked to be fixed. If they seem to be programs you want fixed or removed click fix selected problems.

Confirm	nation 🛛 🔀
2	You are about to remove the checked entries. Do you want to continue?
	Yes No

This warning is to make sure you are sure. Click yes.



These were all missed by the Ad-Aware program, glad I got a second opinion. Click ok. You are done now and can click the "x" in the upper right hand corner to close the program. Again you might want to run it again in about a week. Computer Security and Info Website Links

http://www.microsoft.com/security/

http://www.spychecker.com

http://www.spywareinfo.com/

http://cexx.org/adware.htm

http://www.securityfocus.com/

http://www.ftc.gov/ (Some Info)

