

# SpywareGuide

powered by actiance Security Labs

Home Access the Guide Tools Terms and Definitions

Search SpywareGuide Database & Site

Search

Try It Now

Actiance Security Labs provide a freeware product to help technical users regain control of their machines and to assist spyware researchers doing log analysis.

This tool is not meant to replace your standard anti-spyware scanner, but serve as diagnostic tool to help identify questionable processes on a machine.

## What and why?

As the spyware versus anti-spyware battle rages on, we were looking for good tools that allow a user to examine the contents of his or her machine and to take corrective actions against questionable programs. An excellent candidate for this is "HijackThis" by Merijn, which is already in use by many "anti spyware experts". We are a big fan of Merijn's work and we felt that HJT could be improved upon in some ways and thus the idea for X-RayPc Spyware Process Analyzer was born.

We took the best aspects of the HJT concept and linked it up to the [SpywareGuide Database](#). The result is something like a systems management tool with a built-in expert system.

If you can't wait to try it out, jump straight to the [download page](#). If not, read on. Please note that X-RayPC is not intended to replace your anti-spyware solution but to act as a useful research tool. Currently X-RayPC is free for non-commercial use.

## Features

### Functional

- Lists **active** processes
- List **auto starting** programs
- Lists BHOs, Download Program Files, IE Extension plugins, etc...
- Shows file size and **MD5** of all files instantly
- One-Click "**Triage**" : shows which items are "good", "bad" or "unknown"
- Integrated **file-uploader**
- Integrated **deactivation** and **removal** of an item or file
- Can **kill running processes** (within the limits of the OS security model)
- Can **delete in-use files** (after reboot)
- Can **export** the log file in **text** form, **Excel** format and in **HJT-compatible** format
- Detects **hundreds of suspicious programs**

### Technical

- Fully compiled Win32 executable
- **Single file** download: No external runtimes, DLL's, libraries,...
- **No install** needed. No installer to mess with. Grab the executable and run it. Delete it when done.
- **Fast!** Complete analysis of the system is done in a few seconds.

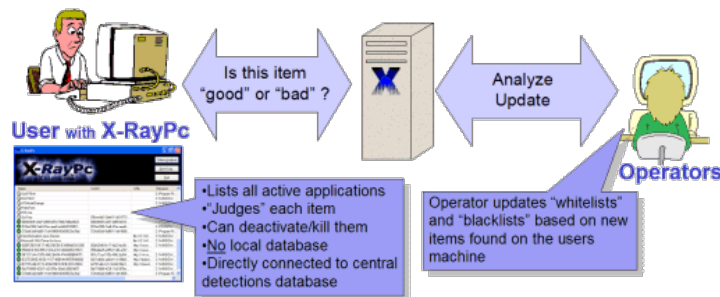
## Benefits

### Offline

X-RayPc Spyware Analyzer can be used as an interactive tool to to examine a users Windows environment and investigate and correct system malfunctions. Logs can be saved and/or uploaded to message boards.

### Online

It can also be used as an remote interactive support tool. Let have a look at the schema.



### Typical Usage Scenario

- A user has a problem with an infection, and cannot resolve it by himself or using an **anti-malware scanner**, so he contacts an "expert".
- The expert tells him to **download and run X-RayPc**.
- The user runs X-RayPc Spyware Remover, and uses the "**Triage**" system.
- X-RayPc Spyware Remover contacts the server, anonymously transmits the details of the items found the users Pc. The server returns "**Known**" or "**Suspicious**" status of "known" items and logs "**unknowns**".
- The user can **remove** the "suspicious" items **immediately**.
- If the problem is **solved**, the story ends here.

### Recent Modifications

2012-2-24 [Zango Times](#)  
 2012-2-24 [About Blank](#)  
 2012-2-23 [CoolWebSearch](#)  
 2012-1-30 [HostSeeker](#)  
[Toolbar](#)  
 2012-1-13 [2000Cracks](#)  
 2012-1-13 [7AdPower](#)  
[Dialer](#)  
 2012-1-13 [Absolu-trans](#)  
 2012-1-13 [AccessPlugin](#)  
 2012-1-13 [AcidBattery](#)  
 2012-1-13 [Acidoor](#)

- The **operator** looks at the reports of the unknowns, and **examines** what they are. She uses her expertise and tools to determine the status of the item. If needed, an "automatic **upload**" can be initiated (with user consent) to obtain a copy of any mysterious file.
- The operator updates the "**blacklist**" or "**whitelist**" of items in the database via the web back end.
- The process **restarts** from number 3.

**Important notes**

- If an item is already known by the server, **zero operator action** is needed
- The operator only needs to examine each item once, so time can be spend processing new baddies, instead of looking at "coolwebsearch infection number 96.523"
- Results of the operator operation are available in (near) real-time



**Free!!!**

**X-RayPc Spyware Analyzer** is an interactive tool used to examine a users Windows environment and investigate and correct system malfunctions. This tool is designed for advanced users, spyware researchers and system administrators.

