ShitWare and You

Spyware/Adware has become one of the biggest problems on the internet. Complacent users download and install freeware/shareware applications at will without regard to possible ill side-effects. As this 'shitware' becomes more common-place, so do the applications meant for removing said named 'shitware'. Some of the available applications for 'shitware' removal are decent, quality products whereas some might not work as well or may even install some type of 'shitware' themselves. Some removal tools find 'shitware' that the others do not, some only scan certain portions of a hard disk, and some run extremely fast (probable side effect of scanning only certain portions of the disk) whereas others might take up to an hour on not-so-recent equipment. Best case scenario, what users end up with is; a quick scan, over *most* of the hard disk that finds *most* of the 'shitware'. Some might consider this acceptable, and considering what these scanners are up against, these type of results are better than nothing. But what happens in the time between the user installing his shiny new freeware app to the time of his next scan? You guessed it, his information is being streamed back to 'shitware HQ'. Now I know what you're thinking, "but some of these scanners provide real-time protection...". This is true, some do provide real-time protection, and others do not. And do we know how good this protection really is? Unless the user is running some type of network traffic analyzer and continuously sifting through any and all packets sent, then the user is just relying solely on what the marketing department for his scanner "says" it can do. The users personal information is still totally at the will of a small group of programmers.

Up til now I've only talked about fighting 'shitware' *after* the infection. This has become the norm for fighting 'shitware'. This kind of stance in *any* type of conflict almost certainly leads to some sort of initial loss. The eventual outcome may 'usually' come out in favor of the user (if the problem is caught in time), but again, a defensive posture as such will let some of a users information be stolen. I deem this as unacceptable.

So how can users drop this entirely defensive posture and be more proactive in the fight against 'shitware'? One idea, from Whitedust Security's Projects Director was, "firebombing of shitware producers real world headquarters is a step in the right direction." Although I like his approach, it doesn't seem very feasible for 'every-day' users as most don't have access to explosive ordinance. Another idea might be to never install any freeware/shareware applications. Anything to be put on the users PC would be bought and paid for, having the EULA's parsed by a highly paid lawyer. Again, doesn't seem very feasible for 'every-day' users because most would like to see how the application performs prior to paying for it and can't afford to bring Johnny Cochrain back from the dead to peruse all of the EULA's.

Now comes my proposal.

Users should be able to stop 'shitware' before it even reaches their PC. I'm thinking of a type of 'indexing' service. A website that users could go to to check to see if the application they are going to download contains 'shitware'. Upon the results, they might see that application X contains shitware Z and opt to search for a similar application that does not contain any unwanted extras. Another possibility is a 'mirror' of the popular download sites (download.com, tucows.com, etc..) containing the same information as these sites along with an entry detailing if any 'shitware' is going to be installed with the app.

How do we accomplish this?

Focus would have to start on just the major download locations. There is no way to index *every* freeware/shareware application on the internet, it's just not feasible. As of now (sept 24, 2005) i haven't figured out a fully-automated way of going about testing all of these (thousands, tens of thousands) of applications. So each and every application will have to be tested on it's own, on a clean system. This will require a lot of help from the community. I'm not talking about installing freeware application X and then running Spybot S&D. Testing will have to be much more thurough. Monitoring for Registry changes, running processes, analyzing network traffic and then possibly scanning with one or more of the 'shitware' scanners themselves. If you have any ideas on automating this process, then please feel free to use the contact portion of this document.

The Indexing site.

The indexing site would contain the index of applications (of course), a section for users to submit new applications for testing and a message board for discussing the applications. The index would list the name of the application, where the application was found at, if the application contains 'shitware' , and possibly might list alternate applications to use instead of the 'shitware' infested application.

The Whole Idea.

The whole idea would revolve around an active and supportive userbase and some hardworking staff. This could possibly help narrow the workload of the anti-'shitware' scanner coders resulting in better prodcuts on thier part as well.

Contact.

If you have any ideas, or think you would like to help, then either email me at shitwaresucks@badfoo.net or drop by irc.cad-net.org #badfoo or #mentor

Thank you for reading this and any support you will give!