

## Re: cOOL

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-12/0142.html>

---

**From:** Malke ([malke\\_at\\_nospoonnotreally.com](mailto:malke_at_nospoonnotreally.com))

**Date:** 12/05/04

Date: Sun, 05 Dec 2004 13:38:08 -0800

cquirke (MVP Win9x) wrote:

> *On Sun, 05 Dec 2004 05:05:54 -0800, Malke*  
>> *paintpearl wrote:*  
>  
>> *All scans should be done in Safe Mode.*  
>  
> *Hi Malke!*  
Hi Chris!  
>  
>> *1) Scan in Safe Mode with current version (not earlier than 2003)*  
>> *antivirus using updated definitions.*  
>  
> *I've wondered what "not earlier than 2003" refers to – specifically,*  
> *Norton? I'd have thought if an engine was new enough to still get*  
> *updates, it would be new enough to use.*

Hahahaha. Since we're at NAV 2005, we're reaching the end of NAV 2003's usefulness, including all Symantec support. Basically, this little blurb is in my general instructions because you wouldn't believe how many home users (many of whom are still using Win98/ME) still have the av that originally came preinstalled with their machines. You might also be amazed at how many people have NAV2003/4 or McAfee with expired virus definition subscriptions. Both those programs come preinstalled on OEM machines and even though that is usually a 90-day trial, I guess people are able to ignore the big red warning sign they get from the av every day. If they have av installed at all.

>  
> *I wonder what % of infected PCs have malware < 1 week old at time of*  
> *infection? After all, there's a lot of selection pressure exerted by*  
> *ISPs that scan for currently-known malware, etc.*

Hahahaha again. My admittedly unscientific answer – based on doing this for a living – is if the PC is infected, it has other non-viral malware. Survey says – 100%!

>  
> *If, as I suspect, a large % of ITW attacks will be < 1 week old, then*

Re: cOOL

> *the av simply has to be freshly updated to be relevant.*

Yes.

>

> *Not to say old attacks are gone, e.g. there are still plenty of old*

> *Lovesan/Blaster direct attacks etc. out there.*

Yes.

>

>>2) *Remove spyware ... a good idea to do in Safe Mode.*

>

> *You may need to repeat these scans on a per-account basis, given that*

> *they often patch in within account-specific settings that may be*

> *missed when scanning from the admin account in Safe Mode.*

Without a doubt, although not the virus scans. When I clean a PC, I go through the system manually and run all non-viral malware scans in each user account.

>

>>3) *With XP, you can delete all but the most recent (presumably*

>>*clean) System Restore point*

>

> *You can only presume the most recent restore point to be clean if you*

> *know it was done after the PC was cleaned. The best way to know that,*

> *is by manually creating a restore point straight after cleaning up.*

Yes. Exactly. That is SOP. Sometimes I'll even disable System Restore before the cleanup, but I don't really like to do that because then you have no way to back out. Of course, if the system is very hosed, it doesn't matter because the damage is too great anyway.

>

> *So my advice would be to purge all restore points straight after*

> *cleaning the PC, and then immediately make a new baseline restore*

> *point (as well as other fall-backs, e.g. in Spyware Blaster, HOSTS*

> *etc.). That approach can apply to both WinME and XP.*

>

>>4) *Make sure you've visited Windows Update and applied all security*

>>*patches. Do not install driver updates from Windows Update.*

>

> *Amen*

>

>>5) *Run a firewall.*

>

> *Yep. Also, verify that your av and firewall are working, and that*

> *they can update themselves – given how many malware attack and disable*

> *these defences, and how such damage can persist after malware's gone.*

>

>

Cheers,

Re: cOOL

Malke

--  
MS-MVP Windows User/Shell  
Elephant Boy Computers  
[www.elephantboycomputers.com](http://www.elephantboycomputers.com)  
"Don't Panic"