

## RE: sasser worm

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-05/0393.html>

---

**From:** TJ Campana [MSFT] ([tcampana\\_at\\_online.microsoft.com](mailto:tcampana_at_online.microsoft.com))

**Date:** 05/03/04

Date: Mon, 03 May 2004 19:41:08 GMT

>After installing the windows updates and rebooting, my computer continues to  
>exhibit the lsass.exe errors tied to sasser. The removal tools for sasser  
>from symantec and mcafee have not detected sasser at all. Are there any  
>other problems that could cause the aforementioned lsass.exe errors?

>  
>  
>

Patching the system is step 1. Now to clean the system. You can use the cleaner tools at the following Microsoft site to accomplish the clean of the worm.

<http://www.microsoft.com/security/incident/sasser.asp>

This tool is to be updates ASAP to deal with all variants of the sasser worms (A-D) sometime today. If the system(s) in question are patched then you can scan with this tool. if this tools does not come up with naything than you can implement the workaround until the scan tools can be updated. To work around this issue follow the instructions below:

Create a read only copy of the following file "dcpromo.log" in the >%systemroot%\debug directory. You can do this with the following two commands at the DOS prompt:

```
echo dcpromo >%systemroot%\debug\dcpromo.log
```

&

```
attrib +R %systemroot%\debug\dcpromo.log
```

This will stop the system from rebooting long enough for you to download the MS04-011 patch and the cleaner tool. Please patch then clean!

T.J. Campana [MSFT]  
Microsoft EPS Security

--

This posting is provided "AS IS" with no warranties, and confers no rights. Use of included scrip  
<http://www.microsoft.com/info/copyright.htm>

Note: For the benefit of the community-at-large, all responses to this message are best directed