

microsoft.public.security.virus: Re: Over-writing virus damage severe. How can I recover?

## Re: Over-writing virus damage severe. How can I recover?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-03/0513.html>

---

**From:** David H. Lipman (*DLipman~nospam~\_at\_Verizon.Net*)

**Date:** 03/07/04

Date: Sun, 7 Mar 2004 07:22:22 -0500

Please read the following URL:

<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>

The objective:

-----

- Turn off the System Restore function
- Reboot the PC
- Using your AV package, perform a full scan of all files on the platform and clean/delete infectors found
- Turn on the System Restore function, and re-apply any System Restore preferences, e.g. HD space to use
- Reboot the PC
- Create a new System Restore point.

If you have problems, it can be done manually....

Use the WinME floppy boot disk and boot from drive "A:"

When you get to a DOS prompt enter the following command

```
attrib -r -s -h c:\_RESTORE
rename c:\_RESTORE c:\RESTORE.old
```

Reboot the PC.

In Windows delete the folder; c:\RESTORE.old

Please report back your results.

I see why you go so many problems with viruses. You don't practice Safe Hex.

Now you want to trade one set of problems with another by posting your true email address to UseNet !

Here's why that is bad...

If you post to UseNet with your TRUE, not a munged, email address then you have invited the swen Internet worm [aka; W32/Gibe-F] to visit you.

Re: Over-writing virus damage severe. How can I recover?

microsoft.public.security.virus: Re: Over-writing virus damage severe. How can I recover?

The Swen is news spelled backwards. The reason it is called this is because the Swen worm harvests email addresses from UseNet News Groups. It has an engine that allows it to post itself to UseNet News Groups and well as it has its own email engine. From the list of email addresses that it has harvested, it will then email itself to those addresses.

Dave

"Ryan Nyquist" <ryan\_nyquist12@hotmail.com> wrote in message  
news:853c01c4040a\$e7176270\$a501280a@phx.gbl...

| To Whom This May Concern,

| I had somehow became infected with a W32.Mydoom.A and

| VBS.Stages.A and another over-writing VBS virus along with

| SubSeven, Back Orifice 2000, OptixPro, and a couple others

| that were detected as Backdoor.Trojan. A total of 91

| infected files had to be deleted. All files were in the

| C:\\_RESTORE\TEMP directory so Windows ME protected them

| and they could not be deleted by regular virus scanner so

| I had to use F-Prot Virus Scanner for DOS and scan in DOS

| mode to delete these viruses. But they did some hefty

| damage. My main drive only has less than 1 GB f