

Cratering: Survive and Prevent Virus Outbreaks

Rev 2, June 1, 2006

Lieberman Software Corporation
www.liebssoft.com

Abstract

An explanation and step by step instructions describing how to protect and disinfect your environment from virtually any virus using a new process called "Cratering."

Contents

1. Introduction	3
2. Background	3
3. Another Solution to the Problem: ACLs (Access Control Lists)	3
4. Interesting Side Effect of Virus Disabling Rather than Removal	3
5. Processes and Virus Files	4
6. Registry Keys/Values	4
7. Cratering for Other Purposes	5
8. Example Run to Prevent Infection by Three Different Potential Viruses	5
9. Conclusion	7

1. Introduction

The recent outbreak of the MSBlaster virus created a nightmare scenario for IT administrators responsible for Windows workstations and servers. Their machines were so busy doing processing work for the virus that they were unable to receive the hot fix(es) required to stop the virus.

This white paper presents tactics an administrator could use to cripple a virus and thereby regain access to infected machines so that critical hot fixes and service packs can be applied.

2. Background

Recent virus outbreaks such as the MSBLAST worm allow a machine to be infected by being connected to a network that contains infected machines. This type of infection is particularly difficult to remediate because the infection spreads so rapidly and becomes so invasive.

The steps taken to correct an infected machine involve applying the proper Microsoft supplied patch, followed by disabling and deleting the virus. If a machine is so overloaded by a virus' activities that the patch cannot be applied, many administrators find that they must pull the network cable from the machine, and then manually terminate the virus process using the Window Task Manager. Only then will the machine activity subside enough to accept the patch.

In some cases a physical visit to the machine may be required and it may take an hour or more to repair and update each machine. As you know, IT administrators are looking for any alternative to going out and visiting infected machines.

3. Another Solution to the Problem: ACLs (Access Control Lists)

Most Windows NT and newer systems use the NTFS file system on the system disk (most viruses live in operating system directories). NTFS allows administrators and users to set complex permissions on file and directory objects to control how those objects can be used. Modifying the permissions on virus file(s) themselves allows you to leave a virus in place, yet disable it.

Disabling the virus via ACL modification is pretty simple: remove the existing default permissions on the virus file(s) and replace them with a single ACL "Deny" entry set to "Everyone:Full". This will lock out all access to everyone, including the operating system.

This change can be done using the built-in program CACLS.EXE or the Microsoft Resource Kit utility [XCALCS](#).

There are also free third party ACL management tools available such as [SetACL.EXE](#).

4. Interesting Side Effect of Virus Disabling Rather than Removal

If the ACLs on a virus file are set so that no one can access it or run it, the virus will be unable to start. And as a bonus, unless the virus is very smart about handling ACLs (not a trivial task), a new infection will be unable to take hold since the disabled virus file cannot be overwritten. In essence, the disabled virus gums up the works of re-infection.

A proactive step that an administrator could take would be the insertion of a series of files with known virus names and locations that are ACL locked-out, but placed on all machines. If a known virus attempts to infect the system, it will find that it has no place to go due to the fact that an inert locked file has already taken its place.

While developing functionality[1] to automate this disablement and blocking of viruses, Lieberman Software coined the word “Cratering,” to describe how we modify the execution/file permissions of virus programs to disable them.

We also added persistent automatic retry to seek out the “window of opportunity” for disabling the virus. In essence, if a machine is not available due to constant reboots and network problems, User Manager Pro keeps on trying until it succeeds. In a constant reboot scenario, there is usually a small window of opportunity at boot up time when an infected machine is on line, yet not completely crippled by the virus. The auto retry feature attempts to use that small time window to fix the machine.

5. Processes and Virus Files

Locking the ACLs on a virus file will not stop a virus process that is already running. The running virus process can be killed with the Task Manager, which requires manual intervention at the machine, or by rebooting the machine, which can be done remotely and en-masse. After the reboot[2], the operating system will try to launch the virus process, but will be prevented from doing so by the new ACL on the virus file(s). Furthermore, if a remote machine attempts to re-infect, it too will be inhibited from both copying and running the virus.

6. Registry Keys/Values

Many viruses start up automatically with every reboot because they have inserted entries into the Registry of the machine that contains details of what to run, and where.

User Manager Pro provides an easy way to determine which of your systems have been infected. Do an enterprise-wide report[3] of the “Run” keys on all of your systems and by sorting and locating the known values for common viruses (most anti-virus vendors publish the keys used by viruses), you can see which machines are already infected. You can then do an enterprise wide edit of your machine registries to remove the entries that are causing the virus to start up.

The most common key used for virus infection is:

```
\\KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

By inserting an arbitrary value and the path to an executable (virus in this case), the operating system will run the program at system start up. Here are the names and values for two common viruses:

Virus Name: W32/Sobig.f@MM

```
"TrayX" = %Windir%\WINPPR32.EXE /sinc"
```

Virus Name: MSBlaster

```
"windows auto update" = msblast.exe"
```

An alternate strategy is to launch the virus when a specific user logs in by locating a virus start at:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

7. Cratering for Other Purposes

One of our clients needed some way to prevent their administrators from running the remote hash extractor program PWDUMP3E. We found that PWDUMP3E operates by creating a service in each remote machine with an executable named “pwservice.exe”. By cratering that file on all of the domain controllers, we easily disabled the use of this hacker tool.

Of course administrators can reverse the effect of the file lockout via ACLs, but this is more than a trivial exercise, given that most administrators will not know the file names that are being used.

8. Example Run to Prevent Infection by Three Different Potential Viruses

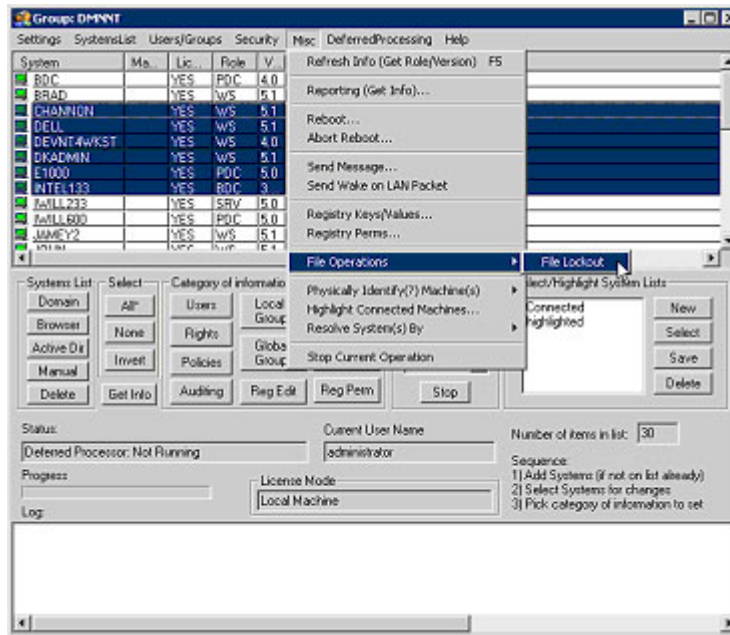
The following steps detail how to use User Manager Pro to crater a series of known virus files on a set of machines.

Save the following names and locations of the known variations of W32/Sobig.f@MM, MSBlaster, W32/Nachi.worm and Win32.Dumaru in a text file:

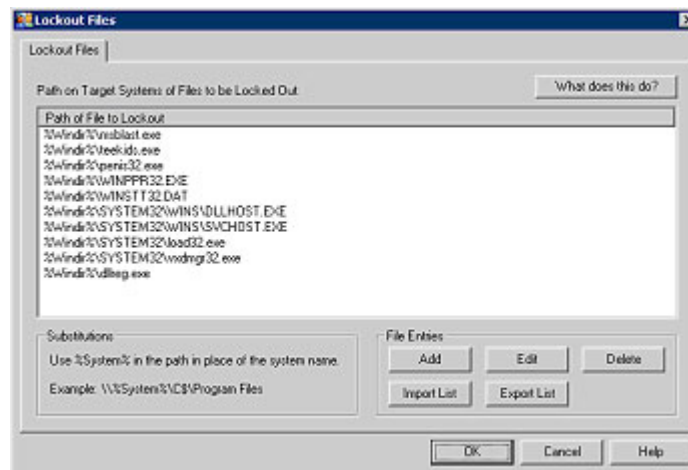
```
%Windir%\msblast.exe  
%Windir%\teekids.exe  
%Windir%\penis32.exe  
%Windir%\WINPPR32.EXE  
%Windir%\WINSTT32.DAT  
%Windir%\SYSTEM32\WINS\DLLHOST.EXE  
%Windir%\SYSTEM32\WINS\SVCHOST.EXE  
%Windir%\SYSTEM32\load32.exe  
%Windir%\SYSTEM32\vxdmgr32.exe  
%Windir%\dllreg.exe
```

Because these names and paths are stored in a file, they can be modified and imported as virus names and paths change.

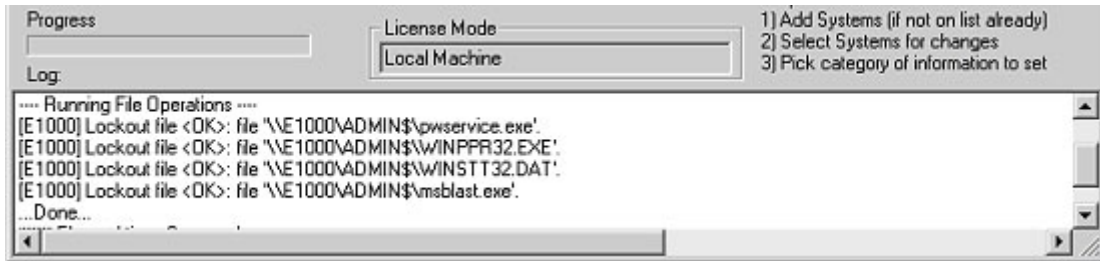
Next, start up User Manager Pro, select a group of machines, highlight the ones to be cratered. Then select the menu option: “Misc” | “File Operations” | “File Lockout”:



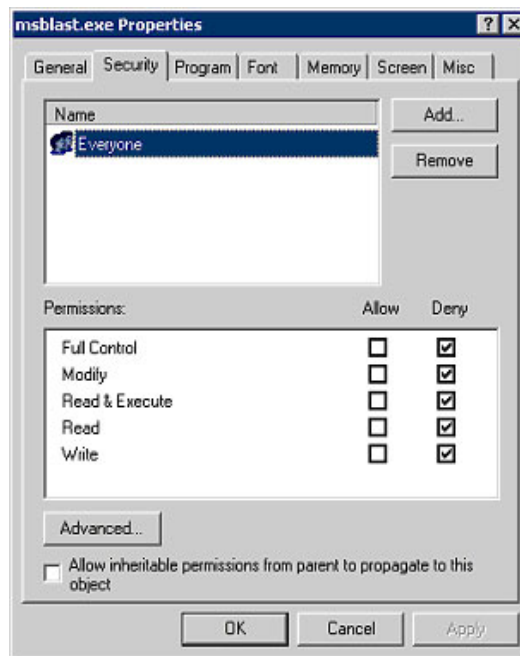
Decide which files to crater:



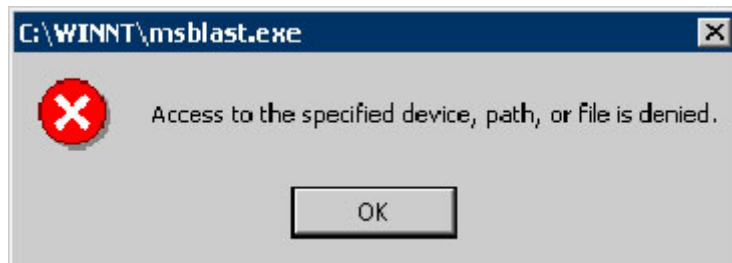
Within just a few moments all of the files are locked as seen in the log:



Here are the properties of a cratered file:



To finish, reboot all of your machines to kill any virus processes that were running. Now, executing the virus produces the desired results. Life is now good.



9. Conclusion

Obviously the best tactic for managing viruses is to keep all of your systems up to date with the latest service packs and hot fixes. But, as we all know, this is not always possible, and in some cases hot fixes are not available until after systems have come under attack.

In this white paper we have tried to provide you with some tactics to help identify and quench a virus outbreak. Of course, virus developers will no doubt come up with more sophisticated and devious methods of ruining your day (and nights). But as you can see, Lieberman Software's tools can give you the power to fight back against this and other challenges.

Our support staff is available to answer your technical questions whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)
Web: www.liebssoft.com Email: support@liebssoft.com



[1] The ability to create inert dummy files and lock down ACLs on lists of potential virus files was added to User Manager Pro in version 4.66 and later (this feature is just a tiny subset of what the product does). See <http://www.liebssoft.com> for download instructions.

[2] Mass reboot is a feature of User Manager Pro.

[3] User Manager Pro version 4.66 and later has enterprise-wide reporting of Registry values for both the HKLM and HKCU hives.