The way most internet-based hacks work is by exploiting a security hole in Windows, or the browser, or another running program to run a bit of hacker-generated code. Typically what this bit of code does is to 'infect' the computer so the hacker can deliver a more sophisticated 'Trojan' virus later. After the computer is infected, the 'Trojan' typically runs silently, stealing data, infecting other computers, all the while running under the infected user's security context.

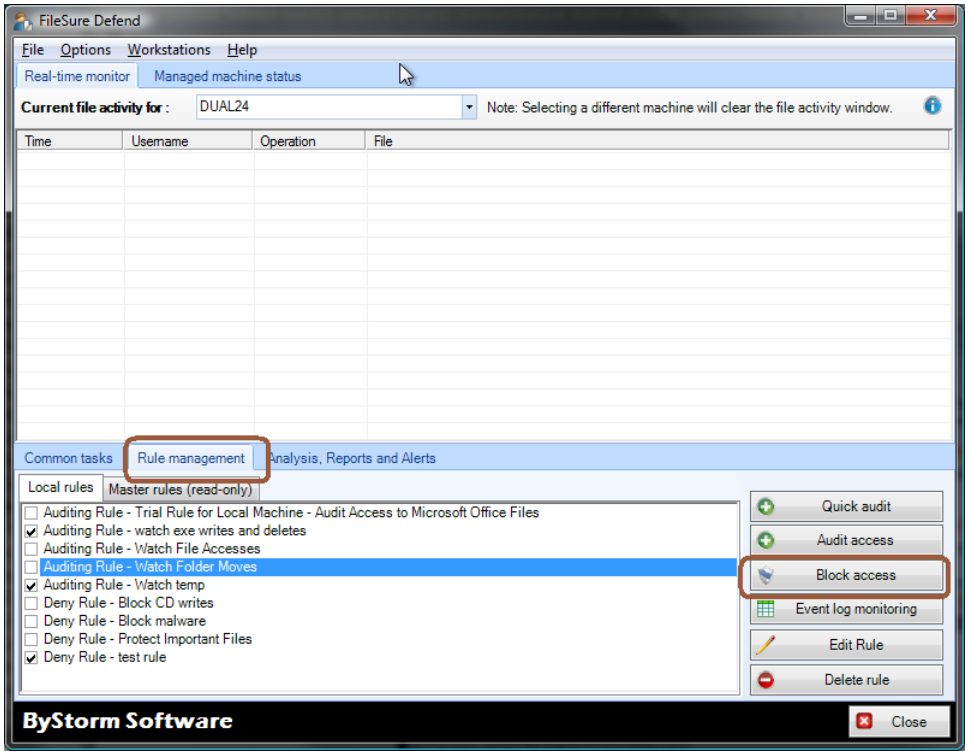
What doesn't (always) work: Protecting against viruses that are already known. If you happen to get a new malware infection that isn't one of the files your virus protection is scanning for . . . you're out of luck.

How we do it:

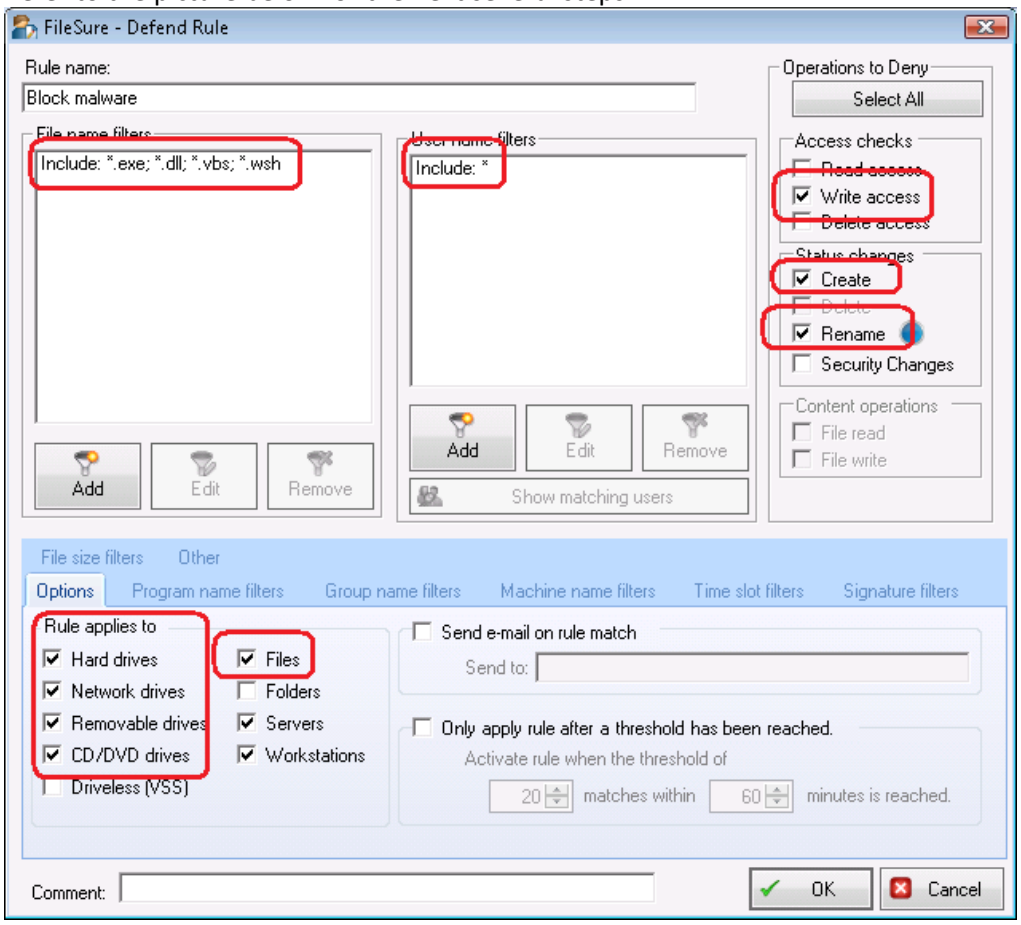
1. Block any program from writing code to the hard drive. Period. Most people never need to write an a executable format or even a VBS file so setting up FileSure to block ALL code from being written to the drive, you stop hackers cold.
2. Use a Data Loss Prevention-styled rule and block access to protected files with a 'White-List' of applications. Since any hacker that gets on your system (you obviously missed step one, but nonetheless) will be using a non-authorized program, FileSure will block it from reading the file.

Specifically, how to do it: First, block creating, writing or the more clever hack of renaming to program files (.exe, .dll, .vbs, .wsh) and apply the rule to all drive types. Easy peasy . . . but note-- self-updating programs don't like this rule so you might want to 'Exclude' them from the rule.

Step 1: On the main FileSure console, click the "Rule management" tab and then click the "Block Access" button:



Refer to the picture below for the next several steps:

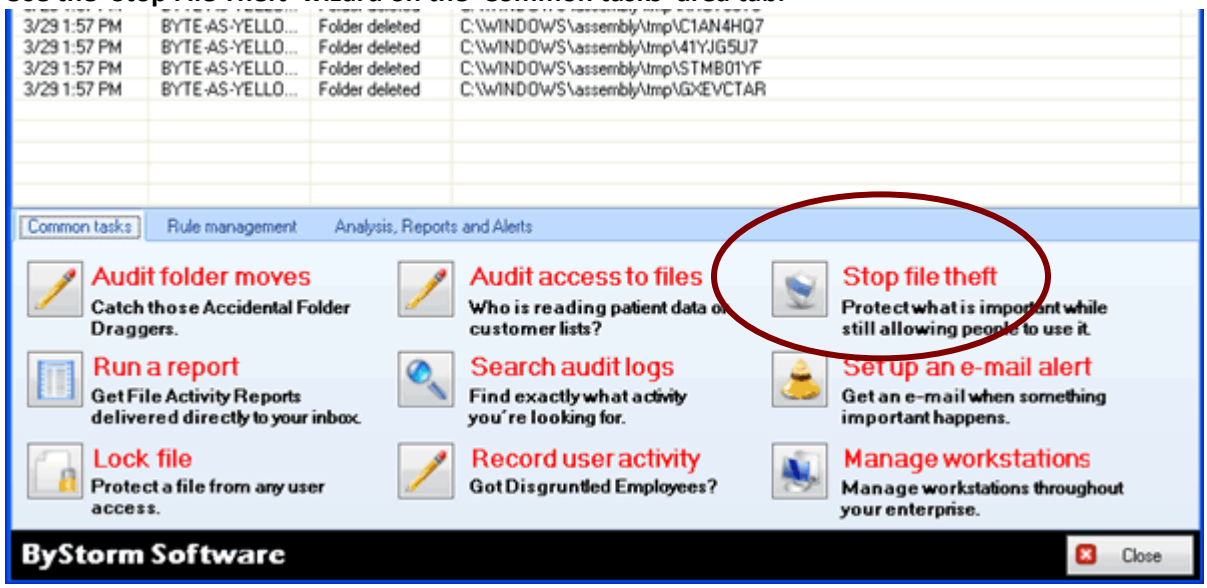


Step 2: Name the Rule “Block Malware”
Step 3: Click “Add” under file name filters and “include” .exe, .dll, .vbs, .wsh, Click “Add” under user name filters and designate all (“*”)
Step 4: Under Operations to Deny, check Write access, Create, and Rename
Step 5: On the “Options” tab choose everything but Folders and VSS under “Rule applies to . . . “
Step 6: Click OK
Step 7: Find the “Block Malware” rule on the rules list and enable it.

For the second half, we created an easy to use, one-page wizard to help you protect your files by limiting program access:

To protect all files of chosen types from theft while allowing authorized access:

Use the ‘Stop File Theft’ wizard on the ‘Common tasks’ area tab.



This wizard will build 2 rules:

1. To block all access to the named file type with the exception of the program listed as its default program, and

2. To prevent said type being written to a removable drive. You simply designate the file type (such as .doc, .xls, etc) and the wizard does the rest. Among other things, this will stop someone from simply doing a “save as” to a removable drive.

You will see the new rule listed on the rules list and already turned on and running. Select the rule and click **Edit Rule** if you need to add more programs to the list of “exceptions,” or other adjustments.

NOTE: For added security, a rule blocking file type changes for your protected file types is recommended. Example: if you have protected .xls files, create a new “block access” rule for files *.xls, all users, and click “renames” under file operations. If you then go to “other” at the bottom tabs, you can choose to allow renames within the same file type (so budget.xls can become budget1.xls, but NOT budget.123).