Detecting Spyware Autostart Methods in MS Windows-based Machines

Removing the autostart method is one of the most important steps in disinfection. If a system admin can remove the malware entry from autostart method used, the malware will fail to execute on reboot (even if the executable files have not been removed).

Following is a list of commonly used autostart methods for malware:

Autostart Folder

All items in the autostart folder will autostart.

Win.ini

[windows]
load=malware.exe
run=malware.exeSystem.ini

[boot]
Shell=Explorer.exe malware.exeAutoexec.bat

c:\malware.exe

Registry Shell Open

[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]A key with the value "%1 %*", will be executed each time you execute an .exe file. "malware.exe %1 %*" .

Alternate Registry Keys

[HKEY_CLASSES_ROOT\.exe] @="myexefile"]
[HKEY_LOCAL_MACHINE\Software\CLASSES\myexefile\shell\open\command\ @="malwaree.exe %1 %*"]
winstart.batA batch file that autostarts with Windows.

Main Registry

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]wininit.ini

This file is called upon when windows loads, it is then deleted.

CAUTION

When editing system.ini, pay careful attention to the Shell=Explorer.exe malware.exe line. Delete only the malware entry. Do not delete Explorer.exe; if you do, the system will not boot into windows.