GEEK SQUAD

TOOLSET REFERENCE
MRI STARTUP MANAGER – BOOT PROFILER

JUNE 2010

CREATED BY: AGENT IAN BANNERMAN

TABLE OF CONTENTS

MAIN TOPICS

MRI TOOLSET RESOURCES

MRI TOOLSET POLICY REMINDER

All agents must use only the Geek Squad-authorized tools. Previous versions of the MRI Toolset may contain unauthorized or deprecated versions of software, and should be disposed of immediately. Single-write media should be destroyed and re-writeable media should be erased. The store servers will keep the previous version of each toolset in case of emergency.

The use of unapproved tools or distributing the MRI disc outside of Best Buy is not only in violation of Company policy, but could result in legal risk to employees and the Company. Violations of this policy will be treated very seriously and will lead to disciplinary action up to and including termination.

For a list of authorized tools, see the MRI Toolset Authorized/Unauthorized List on Employee Toolkit's Geek Squad Job Aids, Guides & Manuals page under Technical>Tools.

NEED THE LATEST MRI?

You can obtain the latest version of the MRI Toolset from your Precinct's SY04 server. If you don't know your server's address, use the MRI Toolset IP Listing on the Job Aids, Guides & Manuals page under Technical >Tools. If your Precinct's link is down or not updated, contact the Help Desk.

LATEST MRI NEWS

Stay tuned to Employee News, the MRI Toolset ETK Widget, and Geek Squad Forums for the latest in MRI Toolset related news.

ADDITIONAL SUPPORT TOOLS

Geek Squad Forums
http://forums.geeksquadcental.com

Geek Squad Armory
http://www.geeksquad.com/armory

Best Buy Learning Lounge
http://www.bestbuylearninglounge.com

MRI TOOLSET LINKS

MRI Toolset Authorized/Unauthorized List
http://infozone/depot/index/docDetail.asp?Doc_ID=261240

MRI Toolset IP Listing
http://infozone/depot/index/docDetail.asp?Doc_ID=280633

If you have any additional questions, please contact MRI@GeekSquad.com.

INTRODUCTION

By now you should have already read the other Toolset Reference documents in this series on MRI Startup Manager. The other documents covered Startup List and an overview of the new MRI Startup Manager as a whole. In the event you are trying to start your training from this document, it is recommend you put this one away and go back and read the MRI Startup Manager Introduction and MRI Startup Manager Startup List. Both of these documents can be found on the Best Buy Learning Lounge.

Now if you are all up to date on the other Toolset Reference training, then you should be good to go. This is the last document on MRI Startup Manager and will cover the new Boot Profiler feature and assumes you have already read the other documents. So let's get started.

BOOT PROFILER

One area Startup List can't come through is showing what *actually* happened on boot. It does a phenomenal job setting you up for an accurate guess, but doesn't have the means to prove it. If malware were to find a new load point, or manage to chain-load via another component, Startup List alone might not be able to catch it. Furthermore, troubleshooting crashes or delays on boot has thus far always been a matter of guess and check, with no easy means to figure out what launched what when and what died (maybe a few lucky WinDbg cases here and there).

Giving line of sight to all of that and more is Boot Profiler. Boot Profiler can be configured from any mode of Windows (including MRI PE), and the second the computer reboots it's tracking everything. A log of the entire boot process is created and can be viewed and replayed later. Boot Profiler is both very powerful and complex; it does its best to simplify the data collected, but it still takes agent know-how to find and repair issues.

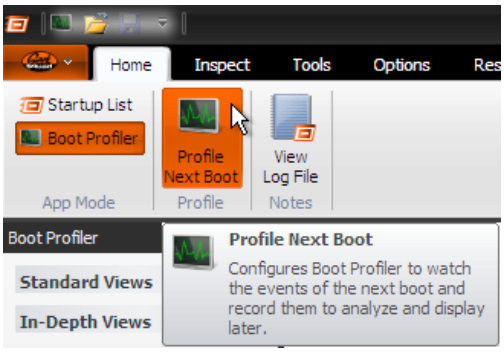
MECHANICS OF A BOOT PROFILE

Boot Profiler works by installing a custom-built driver and service into Windows, both of which are the first of their kind to start on boot. A GSBoot driver is the first driver to load, and a GSBootSvc is the first service. In this manner, every event that occurs during the boot is caught, traced, and logged to the disk for viewing later. As for malware or rootkits, a Windows boot basically goes ntoskrnl.exe -> drivers, and GSBoot is at the front of that. There isn't much of a chance for malware to get in before us, meaning we should always be up and running and logging *before* the malware can try to hide from us.

MRI Startup Manager is also hyper intelligent about how it handles the Boot Profiler setup – the driver and service installs are checked for integrity to ensure they weren't tampered with, and both automatically self-disable on boot so as to mitigate any chance of them causing a boot loop or running repeatedly. MRI Startup Manager automatically cleans up and alerts when a profile didn't start successfully. With the extent of the safeguards in place, you can rest assured that no permanent damage can be caused any piece of Boot Profiler.

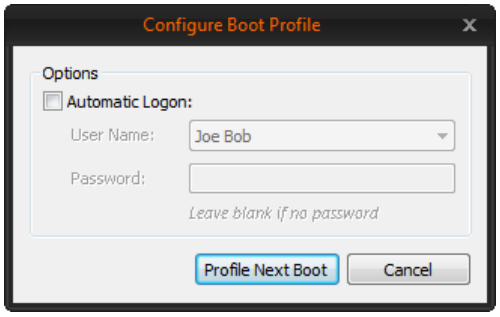
STARTING A BOOT PROFILE

When you first switch into the Boot Profiler App Mode in MRI Startup Manager, you only have two options – Profile Next Boot and View Log File. Profile Next Boot is the first step to starting a Boot Profile, launching the two step configuration wizard seen to your right.



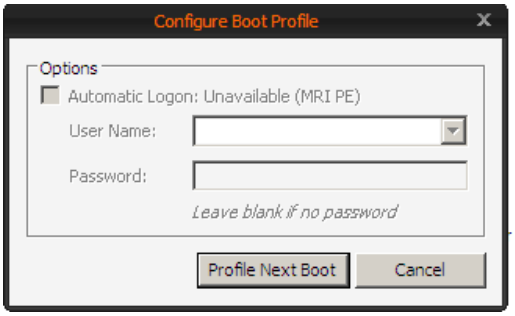
MRI Startup Manager – Boot Profiler – Starting a Boot Profile

The first window presented to you offers the option of Automatic Logon for any Administrator accounts on the system. Passwords are qualified before continuing, and the automatic logon is reverted when the profile completes. Your decision squared away here, clicking Profile Next Boot kicks off the installation of the Boot Profiler components.



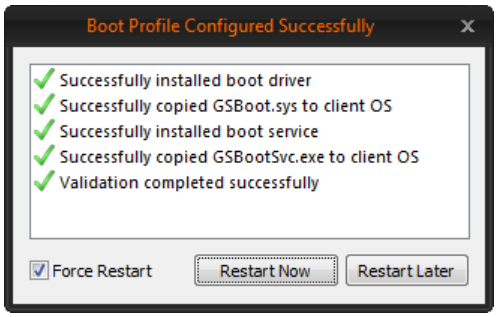
MRI Startup Manager – Configure Boot Profile

Just an FYI, this window is a little different in MRI PE Mode since Automatic Login cannot be selected in MRI PE Mode. That won't cause any issues because all you will need to do is select any User Account once Windows loads. If it's a single user PC, it will already auto login anyways.



MRI Startup Manager – MRI PE Mode – Configure Boot Profile

The mass majority of the time, Boot Profiler will install without issue and you'll be ready to reboot the computer to begin the profile. In the event you choose not to immediately reboot, Restart Later will drop you back into MRI Startup Manager and will highlight the Profile Next Boot button in orange. Toggling this button provides the means to disable / re-setup a boot profile.

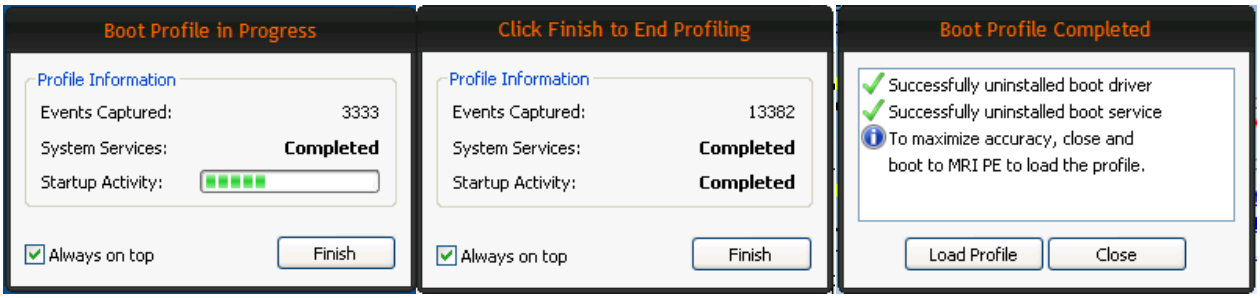


MRI Startup Manager – Boot Profile Configured Successfully

In the rare case that you encounter an error during the installation, the window will indicate as such and the Boot Profiler setup will be cleared from the system. At that point you should boot into MRI PE where the installation can proceed uninhibited by any locally installed software or malware.

ENDING A BOOT PROFILE

Once the reboot begins you're playing the waiting game. The profile takes place silently in the background, and there is no indication of progress until you arrive back at the user's desktop. Once there, MRI Startup Manager launches a window similar to the ones seen here. This Boot Profile in Progress window intelligently displays the status of the automatic start services and the user's startup items and reports when they've finished starting. The Events Captured number represents the number of individual events recorded, and will continue to rise as long as there is system activity. These three pieces of information are there to assist you in determining when you want to end the profile; Boot Profiler will continue until you tell it otherwise.

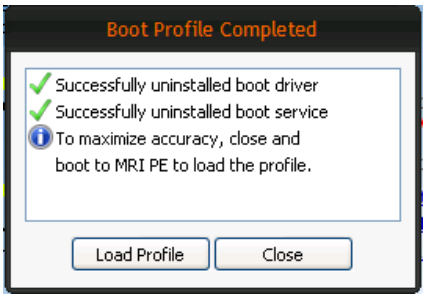


MRI Startup Manager – Boot Profiling Examples

Once you are satisfied that the computer has fully booted (or that the particular trouble you wanted to catch happen has, in fact, occurred), the End Profiling button is there to complete the profile. Ending the profile stops Boot Profiler's driver and service and uninstalls them from the system.

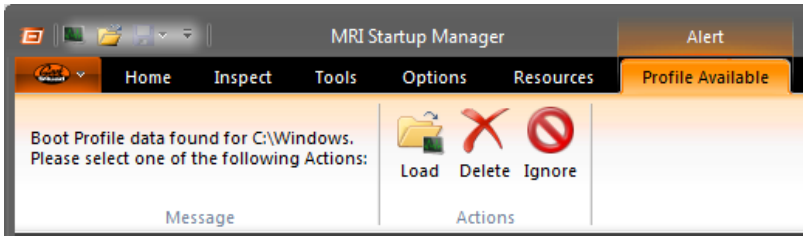
LOADING A BOOT PROFILE

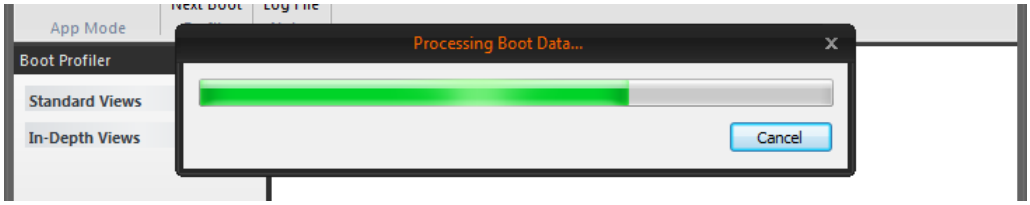
Loading a Boot Profile can take place at any time within MRI Startup Manager. When a Boot Profile completes, the final dialog shown here at the right is displayed and you are offered two choices. You can choose to close the window to open the profile later (possibly in MRI PE to maximize accuracy – MRI PE is completely immune to rootkits and liars) or you can choose to load the profile immediately and jump straight in to MRI Startup Manager.



MRI Startup Manager – Boot Profile Completed message that allows you to Load Profile

While in Windows, the possibility is very real that malware can attempt to trick or lie to MRI Startup Manager about its file's existence or identity; it will always be safer to view a profile in MRI PE. That said, choosing to load a profile directly from the Boot Profile Completed dialog affords you the one time opportunity for rootkit detection; rootkit detection is restricted to just this particular load in order to minimize the chance of false positives. Rootkit detection applies only to drivers, and should not be seen as a catch all. Regardless of your decision at this window, all future launches of MRI Startup Manager will display a notification in the ribbon. From it, you can choose to load the profile or delete the profile data.

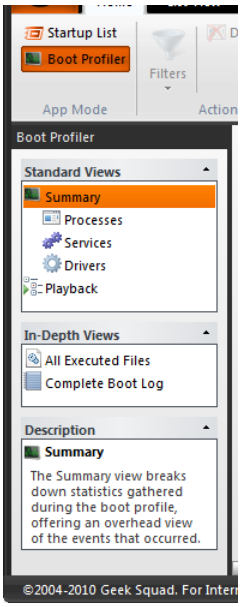




The actual loading of a profile is pretty straightforward. MRI Startup Manager moves you directly to the Boot Profiler App Mode and displays a progress bar as the log file is read. Once complete, analysis and verification of all of the files it saw on boot begins, and you're taken to the first of many views, the Summary view.

WORKING WITH BOOT PROFILE DATA

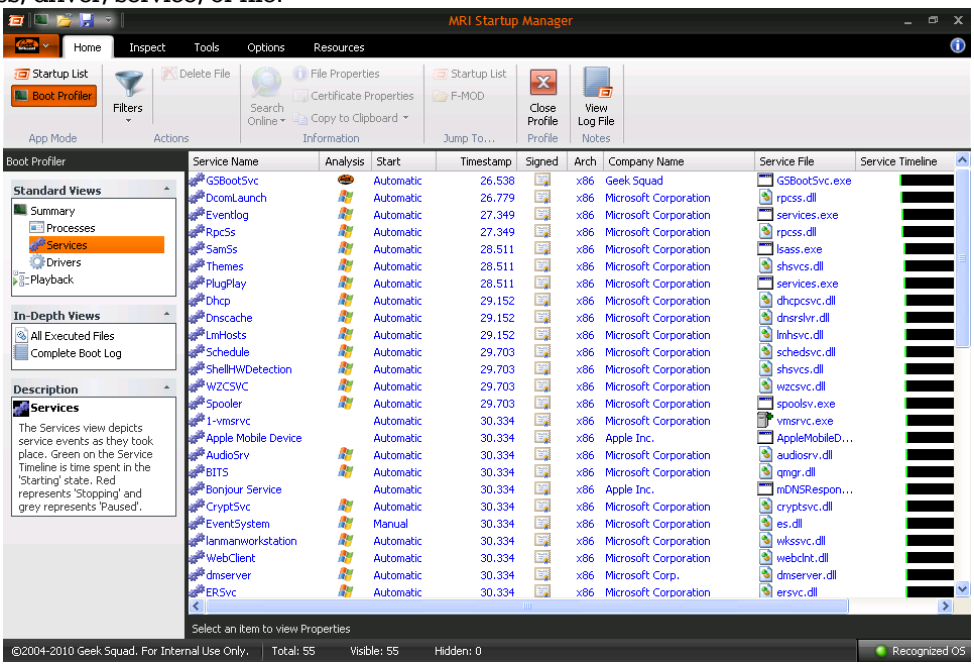
Throughout the profile, the GSBoot driver is logging away to a log file. The second the hard drive is available to write to (about 3 – 7 seconds into the boot), the events being captured are securely logged to the disk. In this manner, if the computer crashes 10 seconds in or reboots before you can end the profile, everything Boot Profiler gathered up until that point will have been logged safely to the drive. MRI Startup Manager will work with a log file in any state; it doesn't require a complete boot profile to function. You can also load a profile in any mode of Windows, including MRI PE. The moral here is that if Boot Profiler was able to start logging, you're in the clear. Ideally you get to the point when you can click End Profiling, but MRI Startup Manager has your back either way.



With a profile loaded, the Standard and In-Depth Views groups fill out with seven available views. As in Startup List, the Standard Views offer targeted looks at the data captured. A Summary page, views for Processes, Services, and Drivers, and finally a Playback view allow you to see the boot profile from familiar angles. Meanwhile, the In-Depth Views organize the profile data from a more global sense, listing events by file and timestamp respectively. All Executed Files has every file load recorded during boot, and Complete Boot Log is literally a step by step dump of every event captured in timestamp order.

On the note of timestamps, it is important to call out the different nature of the data being displayed in the Boot Profiler app mode. While Startup List sorts generically A – Z or via the entry order found in the registry, Boot Profiler focuses uniquely on timestamps. Every event captured during the profile is logged with the specific timestamp that it occurred at. A dedicated Timestamp column in every view is used to sort the events in the exact order they took occurred during boot. This will make more sense momentarily as we break down the views and their troubleshooting purposes.

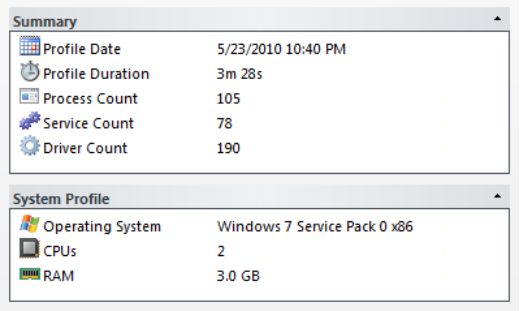
Boot Profiler maintains much of the same functionality introduced in Startup List. An Analysis column is always hard at work checking for potential issues or marking files as recognized, and verification takes place automatically. The Properties pane is back again and displays as much information as is available for items in each view. And as in Startup List, the available columns, search and filters are as flexible as possible to assist in spotting malware or a finding particular process, driver, service, or file.

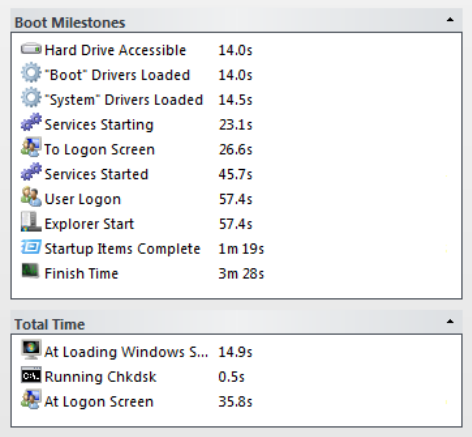


MRI STARTUP MANAGER – BOOT PROFILER

SUMMARY

Once a profile has been loaded, the Summary view (which is the default) will show a full set of statistics that were gathered throughout the boot process. The Profile Summary will detail the date the profile was performed, how long it ran for, as well as total number of processes, services, and drivers seen active during the profile. A System Information group immediately following has a small bit of system specifications mostly as a matter of convenience and line of sight.





The next two groups, Boot Milestones and Total Time, try to explain when certain milestones were reached, or where chunks of time were invested. Their goal is to help you connect the dots between a timestamp and a specific stage in the boot process. With the Boot Milestones, for example, if you saw a major delay in the boot once a user logged in, you could focus on events from around the 60 second mark. Explorer didn't start until a minute nineteen, so your trouble is likely to fall between those two times.

Meanwhile, Total Time describes which stages of the boot process saw how much time. In our example to the left, 15 seconds of the boot was spent at the loading screen with the scrolling progress bar (or in Windows 7's case, the animated Windows logo). Autochk didn't need to run, so not much time was spent there, and following that we saw 36 seconds invested to the logon screen, possibly configuring updates or waiting for a user to authenticate. Finally, we see that the last two and half minutes of the boot were dedicated to waiting for an agent to end the profile. Whether Rootkit Detection was performed is also detailed in the Summary view, but we'll discuss that later.

The Summary view's main job is to help you understand where time was invested in the boot, and spot any major issues or gaps. The plaintext nature of these statistics should be somewhat simpler to place than watching processes fly by later.

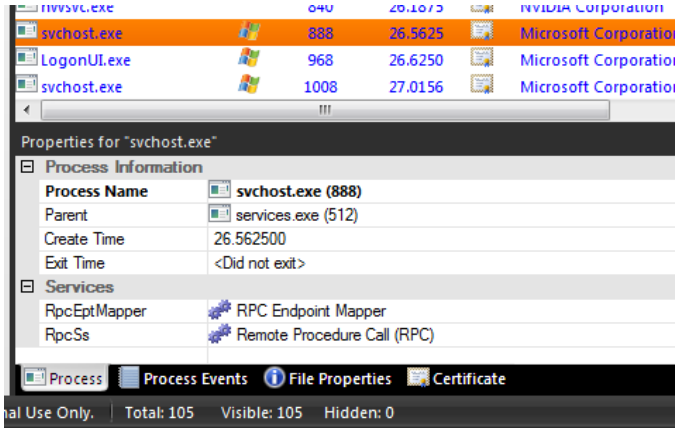
MRI STARTUP MANAGER – Boot Profiler Summary showing a detected rookit using heuristics

PROCESSES

The Processes View displays the boot profile data from the perspective of processes – rather than a left column of Entry Name, we have Process Name, and the view is ordered by timestamp from the first process create to the last. PID, or Process ID, details each process's PID to provide a means to distinguish between those of similar or the same name. A Special column tries to call out the various different components some processes represent. Many system processes have unique icons that tooltip describing their purpose, and all processes containing services picks up the service gears. Finally, a Process Timeline column on the far right completes the view by showing the start and end time of each process. The black bars you can see below will slowly slide to the right as you get further into the boot process; the green graphs inside each of them represents a process's unique CPU activity.

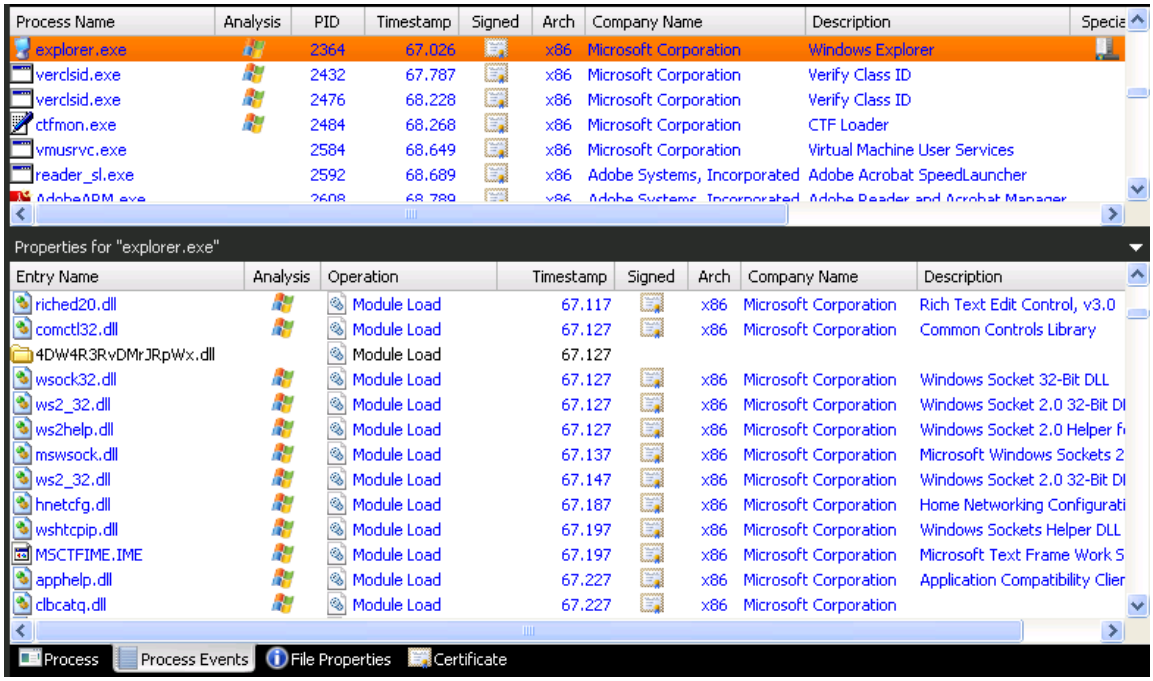
MRI Startup Manager – Boot Profiler - Processes

Not content with stopping there, the Processes view picks up two unique tabs in the Properties pane to offer even more information. A Process tab details the process name, its parent process, any child processes, and when it started and exited. If the process contains any services, that information is present as well.



MRI Startup Manager – Boot Profiler – Process tab

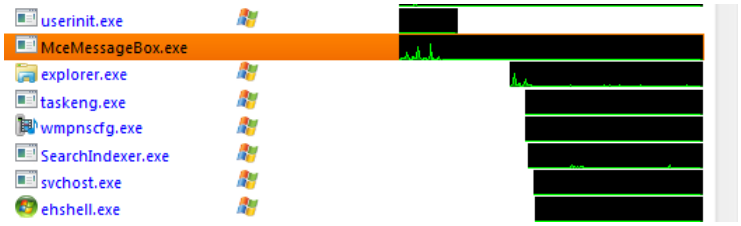
The existence of the second tab, Process Events, stems from the fact that just showing information about the processes themselves wouldn't cover the bases. A malicious file could load into a completely legitimate process, for example, and nothing thus far would let you see that that happened. To shed light on what a process did while it was running, Process Events gathers every operation performed by a process and lists it in timestamp order. Nine such operations are tracked during the boot profile: Process Create, Module Load, Service Starting, Started, Pausing, Paused, Stopping, and Stopped, and Process Exit.



MRI Startup Manager – Boot Profiler – Process Events with a malware Module Load event

Now a big point of clarification needs to be made in regard to items under Process Events and items in the main list view above it, specifically in relation to how signing and filtering work. In the main list view, processes are highlighted in blue indicating being signed based solely on their main executable – no regard is paid to potential existence of unsigned files loading into the process later. This holds true when the Processes view is filtered – a 'Hide Entries Signed by Microsoft' filter will hide every process whose main exe signed by Microsoft, regardless of any unsigned or signed-by-other-parties files that may be loaded in the exe. There is no way to filter based on Process Events or to receive line of sight to the existence of such files without manually looking; that said, the view All Executed Files that we'll cover shortly can help mitigates the need to do so.

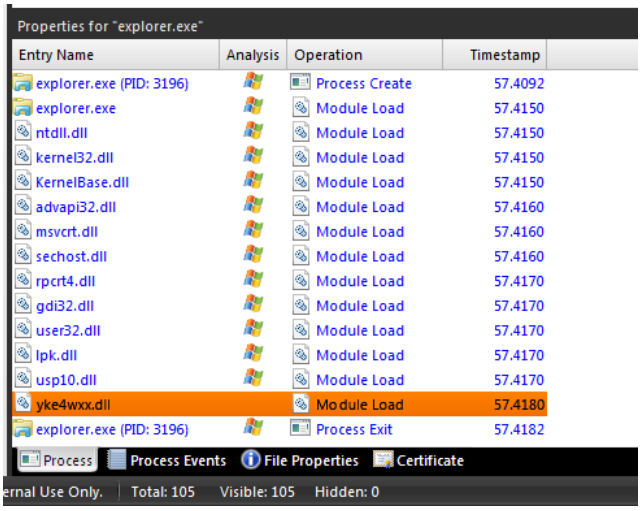
With an understanding of how the different arms of the Processes view work, it's time to delve into some troubleshooting scenarios where the view comes into play. The Process Timeline graphs can be simple clues as to where there may have been trouble on boot. As the boot progresses and you're moving down the list of processes, the Process Timeline graphs will be sliding to the right. A significant delay that appears to be holding up the start of subsequent processes is likely to be problem.



MRI Startup Manager – Boot Profiler – Process Timle example of MceMessageBox.exe

In the example above, userinit.exe launched MceMessageBox.exe immediately on login, which seems to have held explorer.exe up for quite some time. You should investigate what MceMessageBox is, and possibly disable it from startup. Boot Profiler has a Startup List jump to button available in the ribbon that will jump you back to the Startup List App Mode, switch to the "Everything" view, and create a filter to show just startup entries matching the MceMessageBox.exe file path.

The Process Timeline graphs are great for spotting such unexpected delays. Another way to use the graphs is in combination with the Process Events tab in the Properties Pane. If you were seeing a situation where explorer.exe was crashing shortly after launching, you could select the explorer.exe process, switch to the Process Events tab in the Properties Pane, and scroll down to the bottom of the list. While not always the case, the last few operations can often be a great help in diagnosing the trouble. Below it seems that explorer.exe died in the moments after it loaded the unsigned file yke4wxx.dll. It is very likely that this file attributed to the crash, and should probably be removed from the computer.



MRI Startup Manager – Boot Profiler – Process Events example of yke4wxx.dll loading before explorer.exe exits

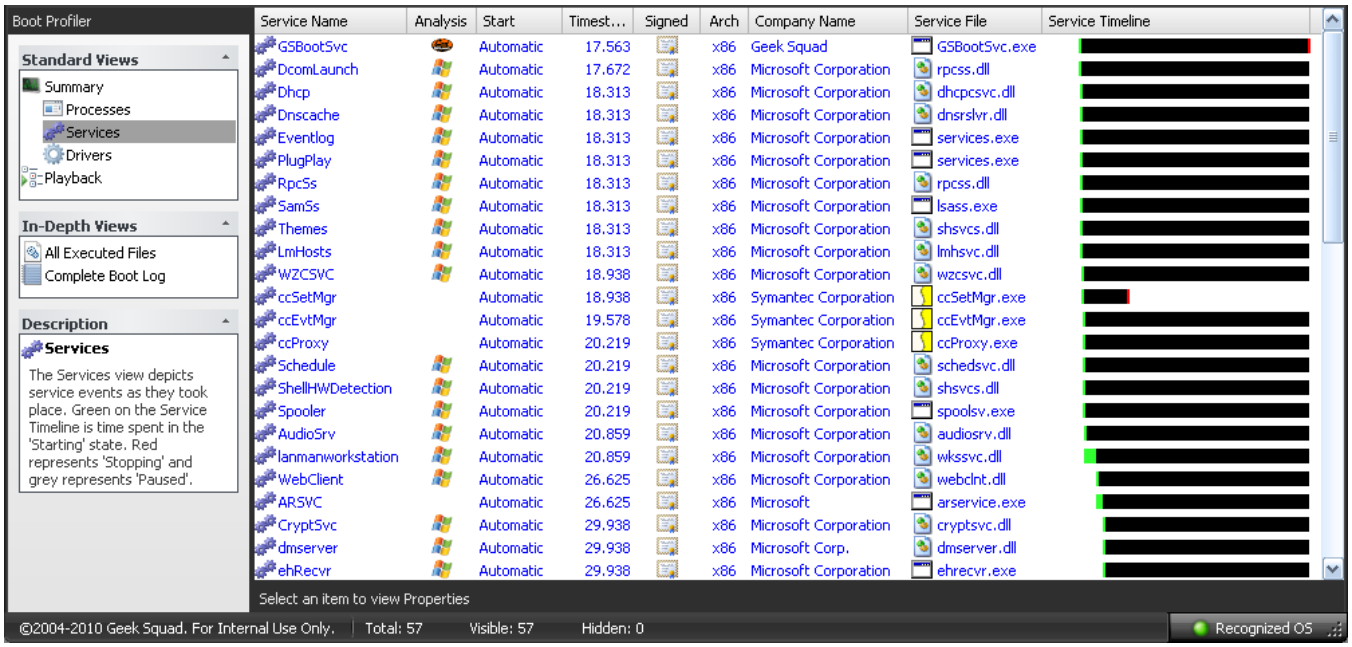
Every boot profile will be different than the last, and not every issue will be immediately obvious and solvable from just the perspective of processes. Stepping beyond Processes in the Standard Views takes us to Services.

SERVICES

Services are often seen as magical creatures hidden in the background of Windows. Boot Profiler takes service information gathered during the profile and displays it in a clean, intuitive view. As with Processes, the view is ordered by timestamp and bookended by a Service Name column on the left and a Service Timeline column on the right. Outside of a service changing states (starting, stopping, etc), it's not really possible to track what it does – services run inside of a process, but you can't separate the actions of the process from the actions of any number of potential services inside it. As such, there is not specific information around what files were loaded or how much CPU a service used. The Services view is constrained to the main service file, when the service started, and the different states the service was in.

That said, the view serves its purpose well. Any delays in the boot brought on by a service are very obvious in the Service Timeline graphs. The graphs use four colors to represent the state of the service at that moment in time – green on the graph indicates time the service spent in the 'Starting' state. Black indicates time spent 'Started', with Grey representing 'Paused' and Red 'Stopping'. As a general rule, colored portions of the graphs should be very small, and the service timeline should slide to right smoothly. Lengthy amounts of time in Green / Red may indicate trouble with the service, and bear investigation.

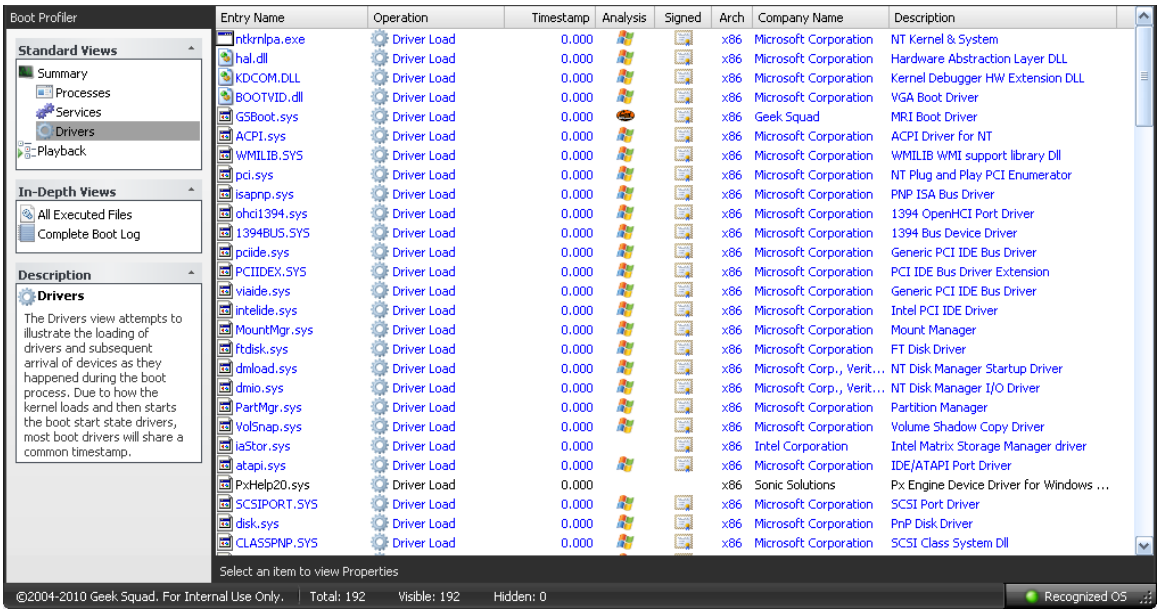
If you find a service is significantly delaying others from starting, or appears to have stopped prematurely, you have a few options. You can search online for any known issues that can cause the delay, or attempt to start the service in Startup Manager and research the error returned. If you determine the service isn't critical, simply disabling it may be a solution.



MRI Startup Manager Boot Profiler - Services

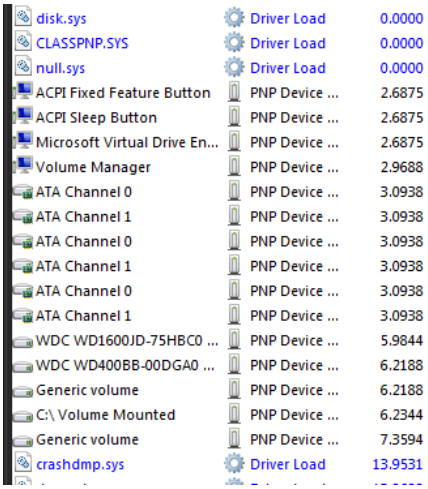
DRIVERS

Drivers are about as low-level and powerful as things get in Windows. Once a driver loads, it has essentially assumed God Mode and, with the right code, can affect just about anything. Due to their low-level nature, Windows heavily optimizes how they run, and file loads, CPU usage, or a timeline aren't really relevant. Drivers function with just the code in their driver file or in tandem with other drivers. Any CPU usage that would be reported is seen via the System process, visible generically in Processes. With this minimal yet powerful nature in mind, the Drivers view comes together as a list of the various driver files that loaded on boot and the device arrivals that followed.



MRI Startup Manager Boot Profiler - Drivers

The Drivers view has a few idiosyncrasies. Every Boot start driver reports a timestamp of 0.000. While the order is accurate, these drivers load so early no actual timestamp is available. Next, PNP Device Arrivals are notifications from the Windows kernel that a device is now 'connected' and ready for use. These are not able to be directly tied to a driver, but some basic logic can help you associate the various events. For example, disk.sys loaded before the hard drives arrived.

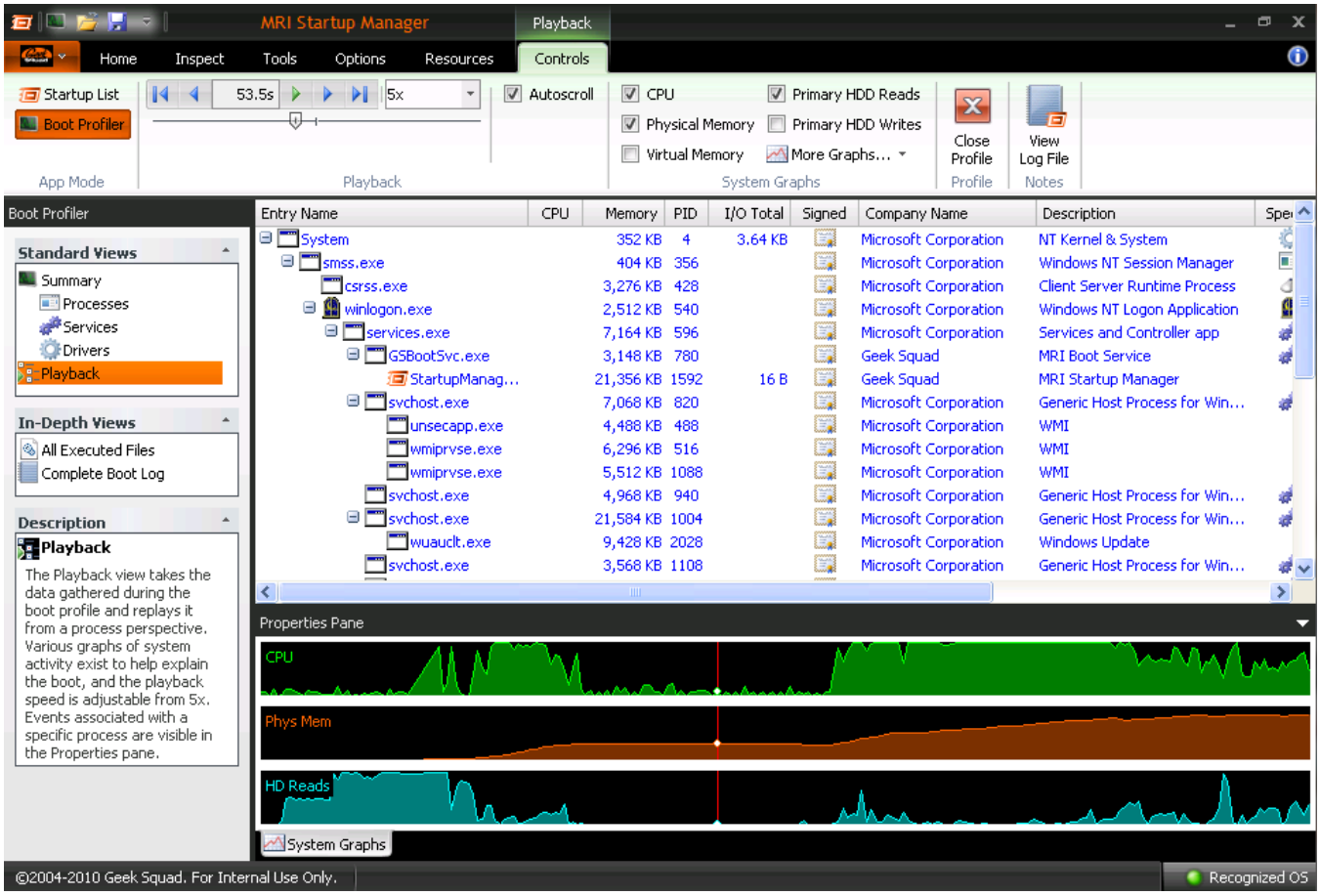


Regardless, the true value of the Drivers view is found in the following two situations – a BSOD on boot, and detecting malware hiding itself with a driver. A BSOD on boot will have the boot profile log suddenly come to a screeching halt. As in, you'll reach a certain point scrolling down and things will just stop – in all likelihood, a driver or device near the bottom will be behind the BSOD. If you caught the stop code, a quick bit of searching online can often reveal the answer.

As for finding malware, GSBoot is the first driver that loads on boot, hopefully trumping any malicious drivers. In this manner, they shouldn't have started yet to hide themselves, and as such will be caught and listed in the Drivers view on load. Furthermore, when a profile is loaded from the Load Profile immediately upon its completion, Rootkit Detection kicks in and can catch a virus trying to point Boot Profiler away from the driver file that actually loaded on boot. In such situations, Boot Profiler will alert that it may have detected a rootkit, and the driver will be colored red and called out via Analysis. Work in this view requires agent smarts, but should hopefully assist in solving some complex issues on boot.

PLAYBACK

The Playback view takes the data gathered during the boot profile and replays it as you could expect to see it via a program like MRI's Process Analyzer. At a default speed of 5x normal, you can watch processes being created and exiting, using CPU and hard disk I/O, even follow along with corresponding system graphs in the Properties pane. Playback is essentially the Processes view DVR'd.



MRI Startup Manager - Boot Profiler - Playback

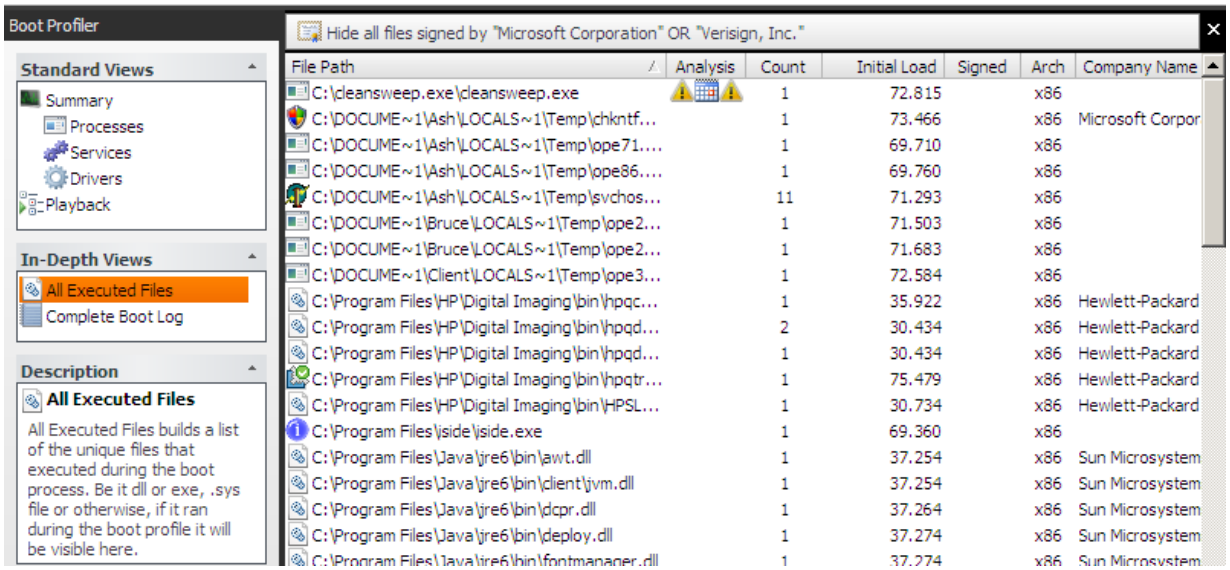
Full controls in the ribbon allow you to slide to any point the boot, speed up or slow the playback, even add a whole host of different graphs to track where resources were being spent. Playback is best used to isolate trouble at specific points in boot, diagnosing errors or wasted resources, or to otherwise spot when and via what a particular exe launched. Out of all of the views, Playback gives the best sense of how the boot proceeded, and should prove a valuable troubleshooting tool.

IN-DEPTH VIEWS

The two In-Depth views act as blatant dumps of data. All Executed Files lists every file that loaded on boot, sorted by unique file paths. The Properties Pane in this view picks up a unique File Events tab that lists the different process the selected file loaded into, making it easy associate a random file to a recognizable process.

ALL EXECUTED FILES

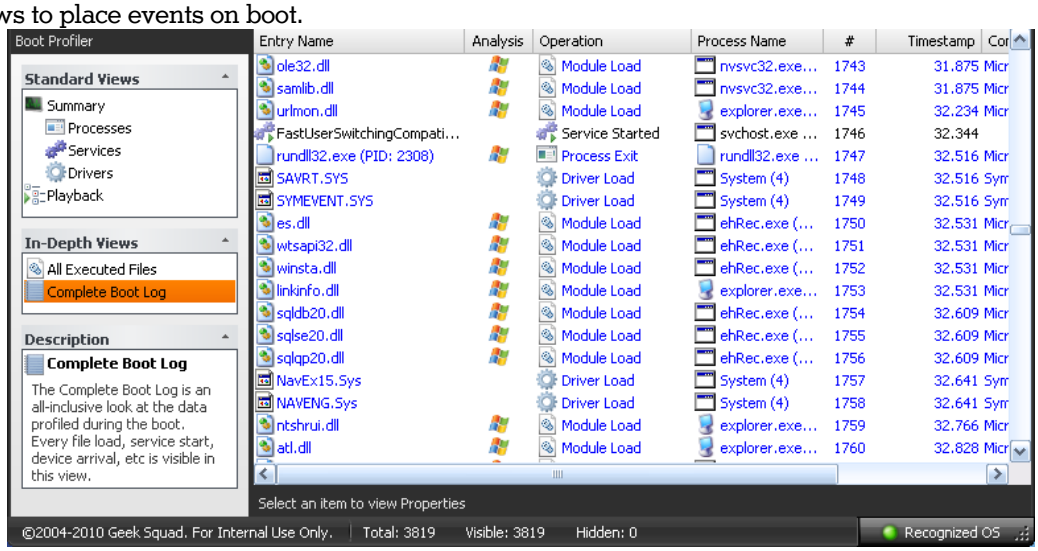
All Executed Files is possibly the best malware tool in our arsenal to date. With a filter in place, this view essentially becomes a list of unrecognized files that ran on boot; malware will sit visible in the open for easy pickings. Combined with some quick Delete Files in MRI PE and entire infections can be terminated in a matter of minutes.



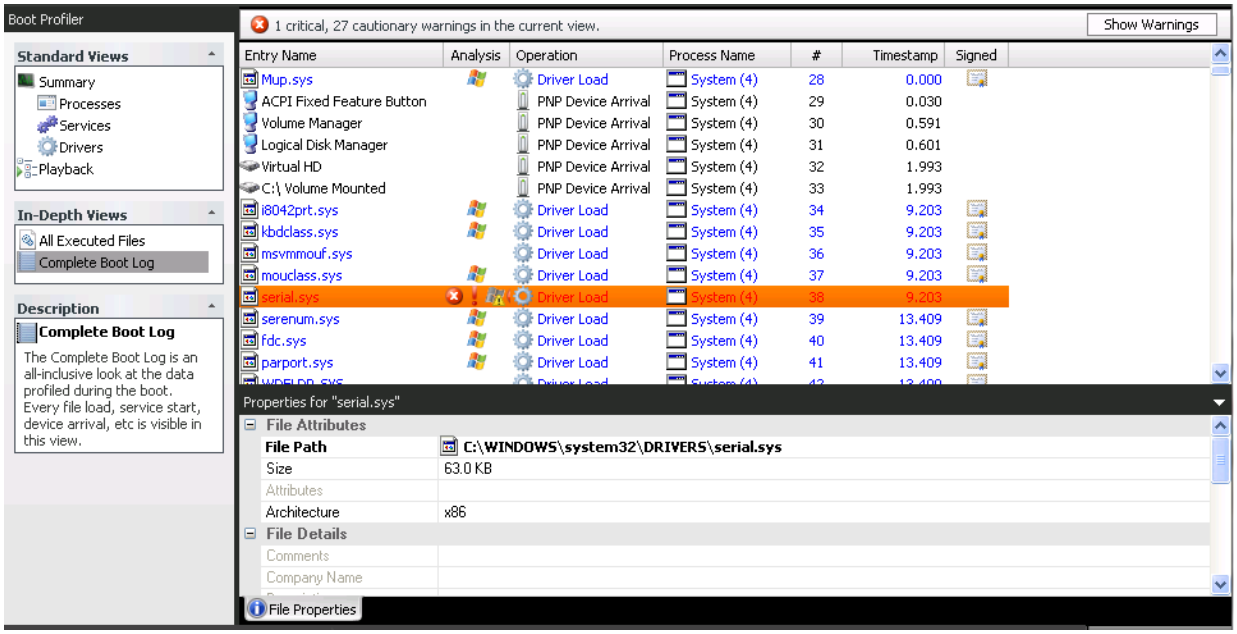
MRI Startup Manager - Boot Profiler – All Executed Files with a Filter turned on

COMPLETED BOOT LOG

The Complete Boot Log, on the other hand, functions just like it sounds – every event recorded by Boot Profiler, in the order it was recorded in, is displayed. If you were searching for a particular event but weren't sure where to find it, this is the view to use. Aside from that, the data here is usually too complex to decipher directly. It's best to use the other views to place events on boot.



MRI Startup Manager - Boot Profiler – Complete Boot Log



MRI Startup Manager - Boot Profiler – Complete Boot Log showing a rootkit that compromised a boot driver

CONCLUSION

This concludes the entire trilogy of MRI Startup Manager Toolset Reference documents! You are totally stoaked by now and are itching to start using MRI Startup Manager, Startup List, and Boot Profiler. So go ahead Agent, start saving the world from computer uprisings!!

If you have any MRI Toolset questions, feel free to reach out to the Technical Tools team at MRI@geeksquad.com. If you have any technical training questions, feel free to reach out to InternalAffairs@geeksquad.com. Don't forget you can also hit up the Geek Squad Forums.

For more on the new MRI Startup Manager, you can visit the Learning Lounge or hit up the Resources tab in MRI Startup Manager. There you can access other Toolset Reference documents and videos on MRI Startup Manager and more.