GEEK SQUAD

TOOLSET REFERENCE
MRI STARTUP MANAGER - STARTUP LIST

JUNE 2010

CREATED BY: AGENT IAN BANNERMAN

TABLE OF CONTENTS

MAIN TOPICS	

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 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.

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 MRI Startup Manager Introduction Toolset Reference document. 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 in order to help ensure you know the basics. This other document can be found on the Best Buy Learning Lounge in case you don't have it.

Now if you are all up to date, then you should be good to go. At this point, you should be familiar with the basics of MRI Startup Manager like the UI and how to perform basic actions. This document on MRI Startup Manager will cover the Startup List feature. So let's get started.

WHAT IS STARTUP LIST?

Renamed for clarity, Startup List is everything old MRI Startup Manager was and more. All of its functionality has been revisited and massively upgraded – more locations, more resets, better organization, display, and user account support, proper x64 support (no joke!!), the list goes on and on.
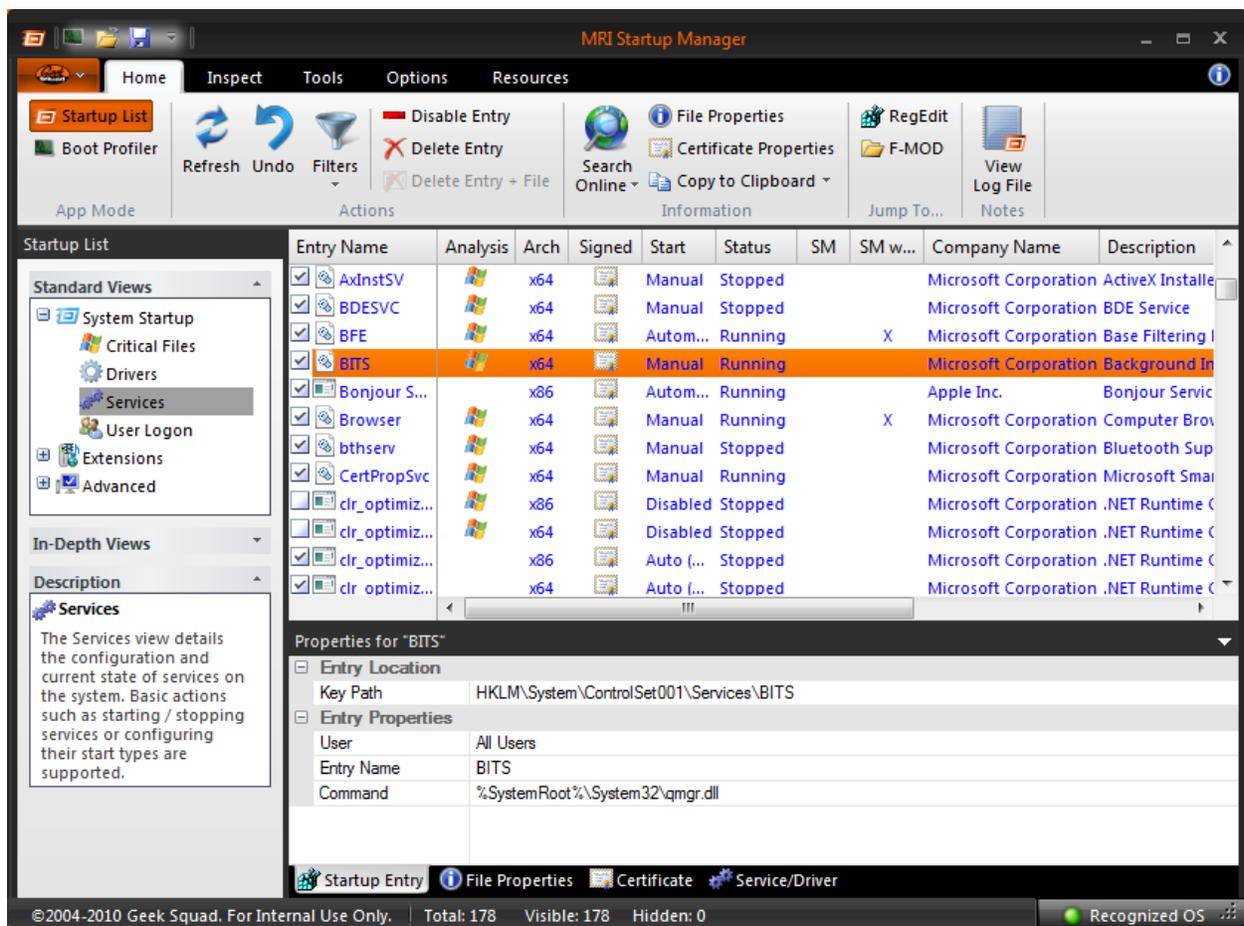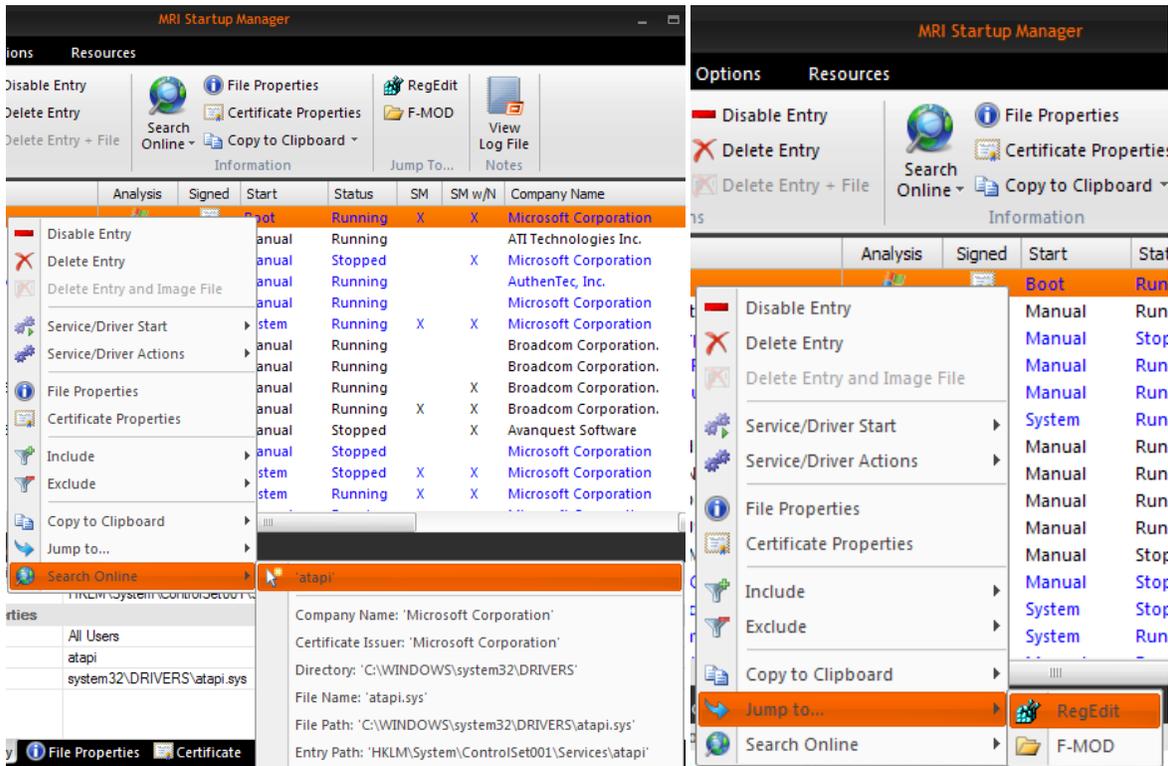

MRI Startup Manager – Startup List

Startup List takes advantage of the new task panes with a brand new layout and accompanying descriptions for each view. Standard Views offers targeted looks at specific parts of Windows, while In-Depth Views uses an Everything and Brute Force {CLSID} view to offer massive dumps of data best used with searching or filters.

Also, powerful columns mitigate the need for strict separation between user accounts or Normal and Safe modes, and all of the information displayed is able to be copied, searched, and filtered.

Beyond that, the Properties pane displays a veritable ton of information for each startup entry, covering just about all the information you can imagine. Startup List even supports jumping from an entry directly to RegEdit or F-MOD, and can even launch a Google search for any entry. Talk about AWESOME!!!
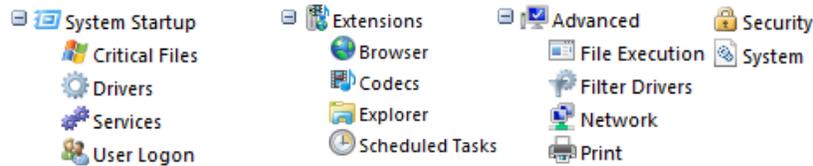

MRI Startup Manager – Startup List – Jump To Examples

 Each view in Startup List has a specific aim, a particular area of startup that it focuses on. Understanding the various categories is important for the successful repair of a computer, as many of the entries shown in Startup List can have the potential break, bust, BSOD, or explode a computer if approached haphazardly. We'll tour the different views to build an understanding of what is possible with Startup List and how to utilize them.

STANDARD VIEWS

The Standard Views group contains the core of Windows startup, sections specific to extensions, as well as lower-level advanced views covering system components. The Extensions and Advanced categories are minimized by default, and are usable as is with a basic filter in place.

*MRI Startup Manager – Startup List – Standard Views*

SYSTEM STARTUP

The first available category, System Startup, can most accurately be described as portraying a basic Windows boot. The Critical Files subcategory contains key Windows files that may not have a specific startup entry but that should absolutely be present and signed. Drivers follow next as the first true startup group that loads and executes on boot, tailed by Services and User Logon. Each of System Startup's subcategories uses a custom column set tailored to the specific information available.
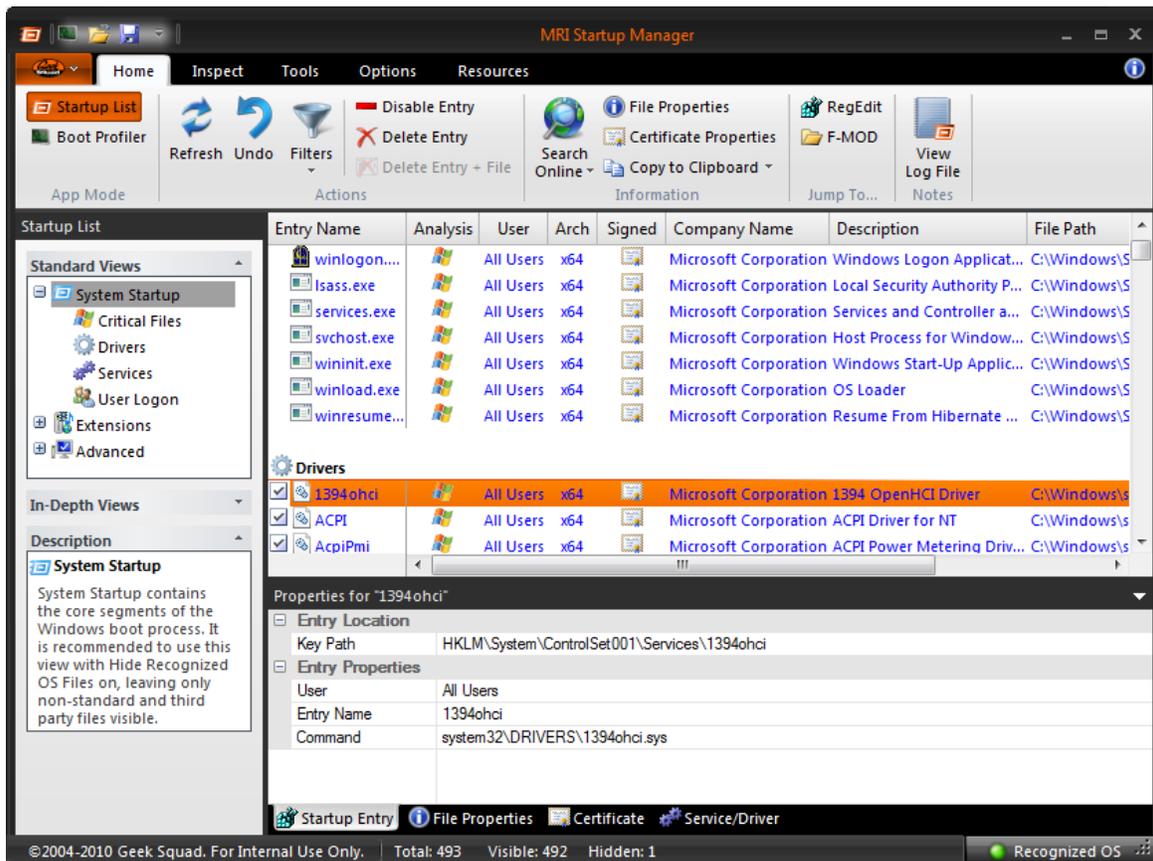
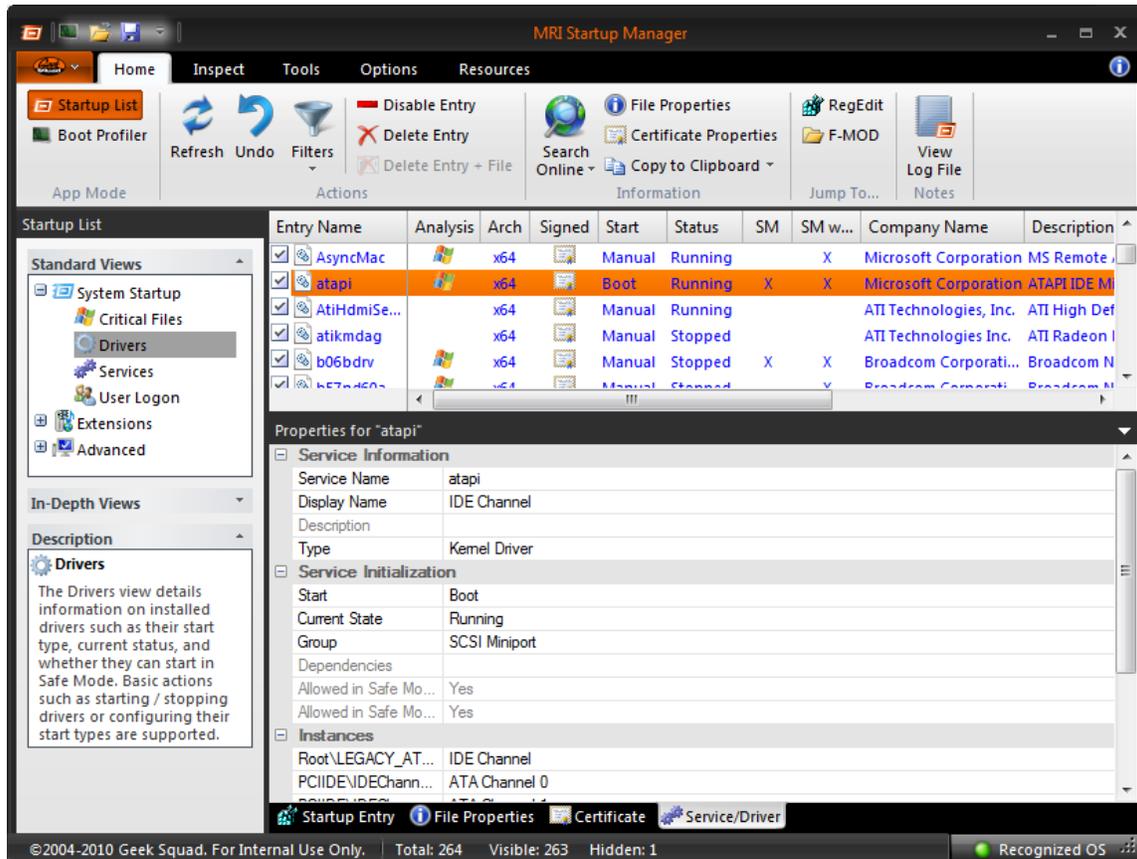*MRI Startup Manager – System Startup*

CRITICAL FILES

The Critical Files view exists to solve a problem seen with the previous Startup Manager. A virus could patch winlogon.exe, for example, proceed to get deleted by a scanner in FACE, and leave no obvious means of figuring out that the critical file winlogon.exe was suddenly missing. The patching or deletion of any of the files in Critical Files is liable to lead to BSODs or at the very least massive errors in Windows, and as such this view is seen as the first set of startup entries. Anytime a file in here is missing or unsigned the Analysis column will light up to let you know. At that point you should replace the problem file[s] with a known good copy from a similar service pack and architecture.
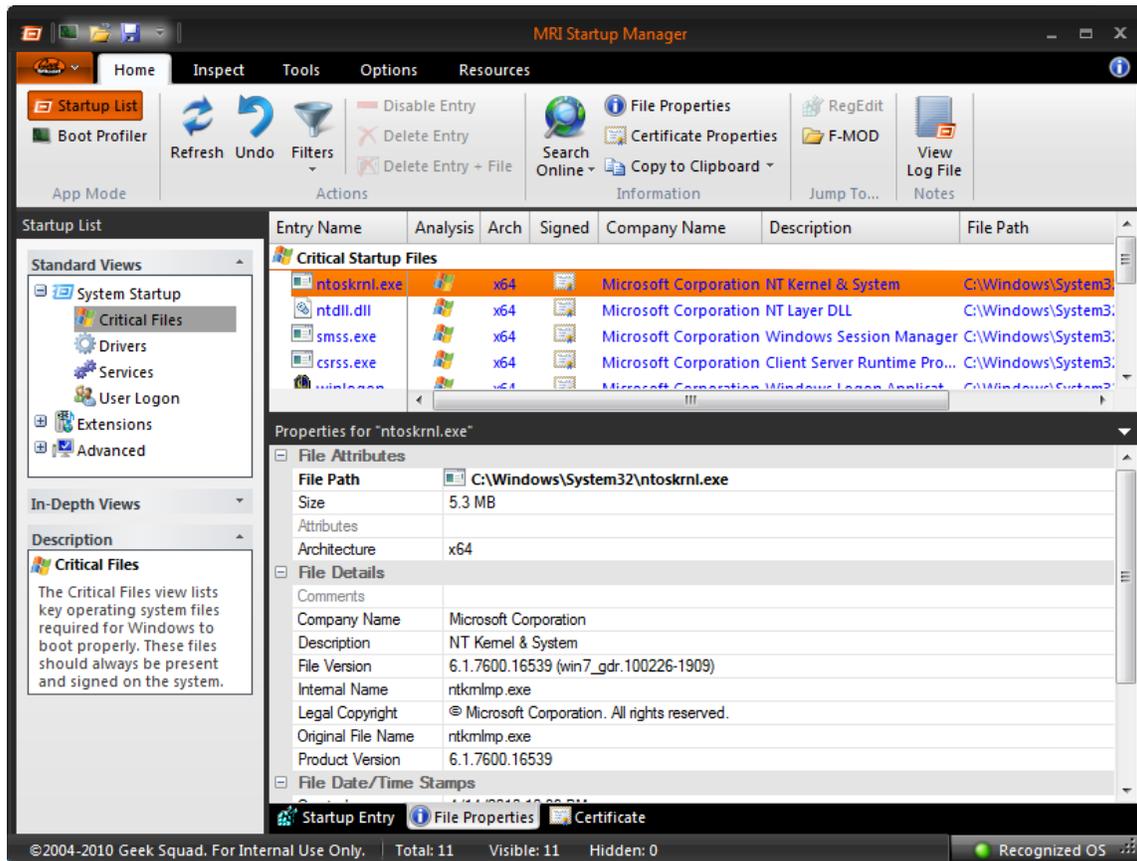
MRI Startup Manager – Critical Files

DRIVERS AND SERVICES

Drivers and Services are two powerful concepts in Windows, and they bring with them many possible configuration scenarios. To assist in managing these startup entries, the Drivers and Services views have a unique set of default and available columns. Four columns of Start, Status, Safe Mode (SM), and Safe Mode with Networking (SM w/N) are visible by default, and several others exist to be enabled as needed. The Properties pane also gains a tab to show extended information about each service / driver's configuration.

MRI Startup Manager - Drivers

Drivers and Services share a similar concept of a 'start type'. Drivers, which can start much earlier, support five different start types – Boot, System, Automatic, Manual, and Disabled. Services support only the last three – Automatic, Manual and Disabled, with an additional type of Automatic (Delayed Start) on Vista+. The Start column displays a driver or service's start type while the Status column indicates whether it is currently Running, Stopped, or otherwise. Unchecking a driver or service will change the start type to disabled; you can also manage the start type manually via the context menu.
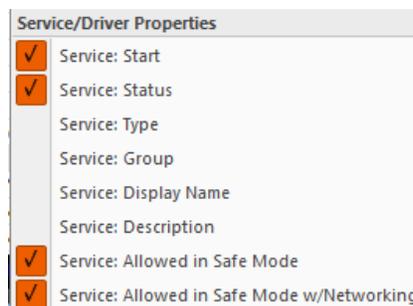

MRI Startup Manager – Service/Drivers Column Options

Startup List also allows you to try to start and stop drivers and services via the Actions item in the context menu. This can prove to be a quick way to try to resolve an issue you suspect a service is behind or uncover the error preventing something from starting. The Analysis column also updates automatically with alerts on any dependency issues that a change to a driver or service may have caused. All in all, you should be careful when modifying these entries as the wrong change can be very damaging to Windows.
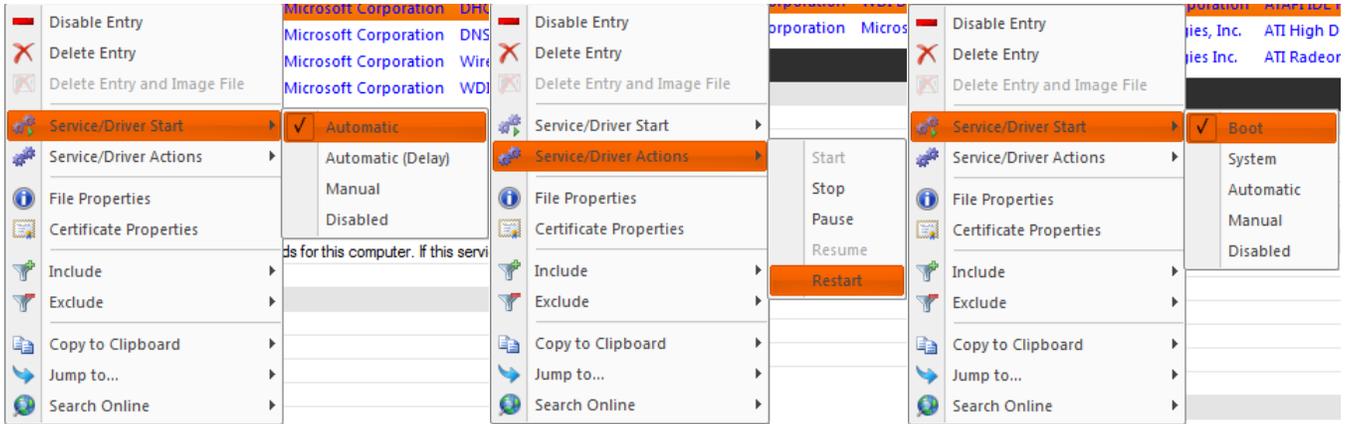
MRI Startup Manager – Service/Driver Context Menu
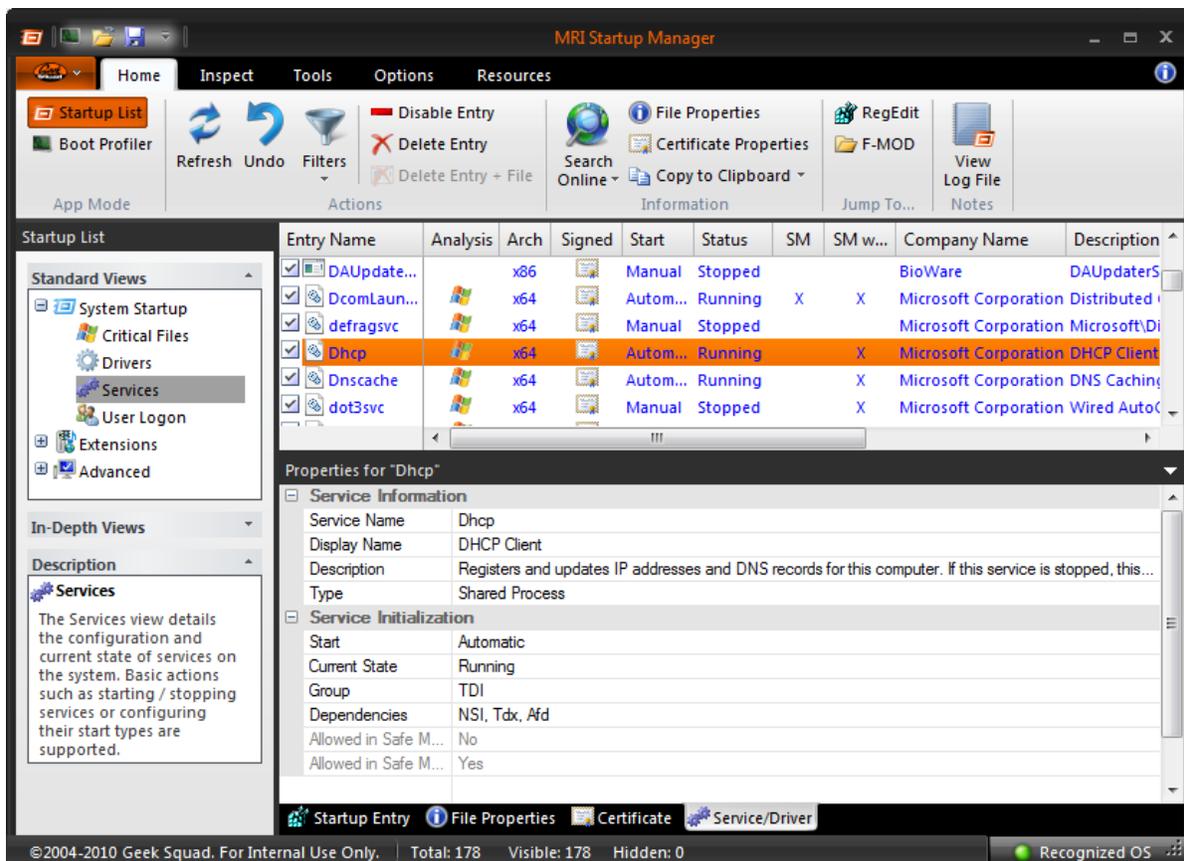
MRI Startup Manager - Services

USER LOGON

User Logon is the unified view that contains the startup entries for each user account on the system. Rather than split user accounts into separate views like in previous versions of Startup Manager, a User column specifies what account the startup entry applies to. Browser add-ons have been pulled out of User Logon and stashed more appropriately under Extensions; with that change, User Logon now appropriately represents only the startup items that run immediately upon a user logging in.
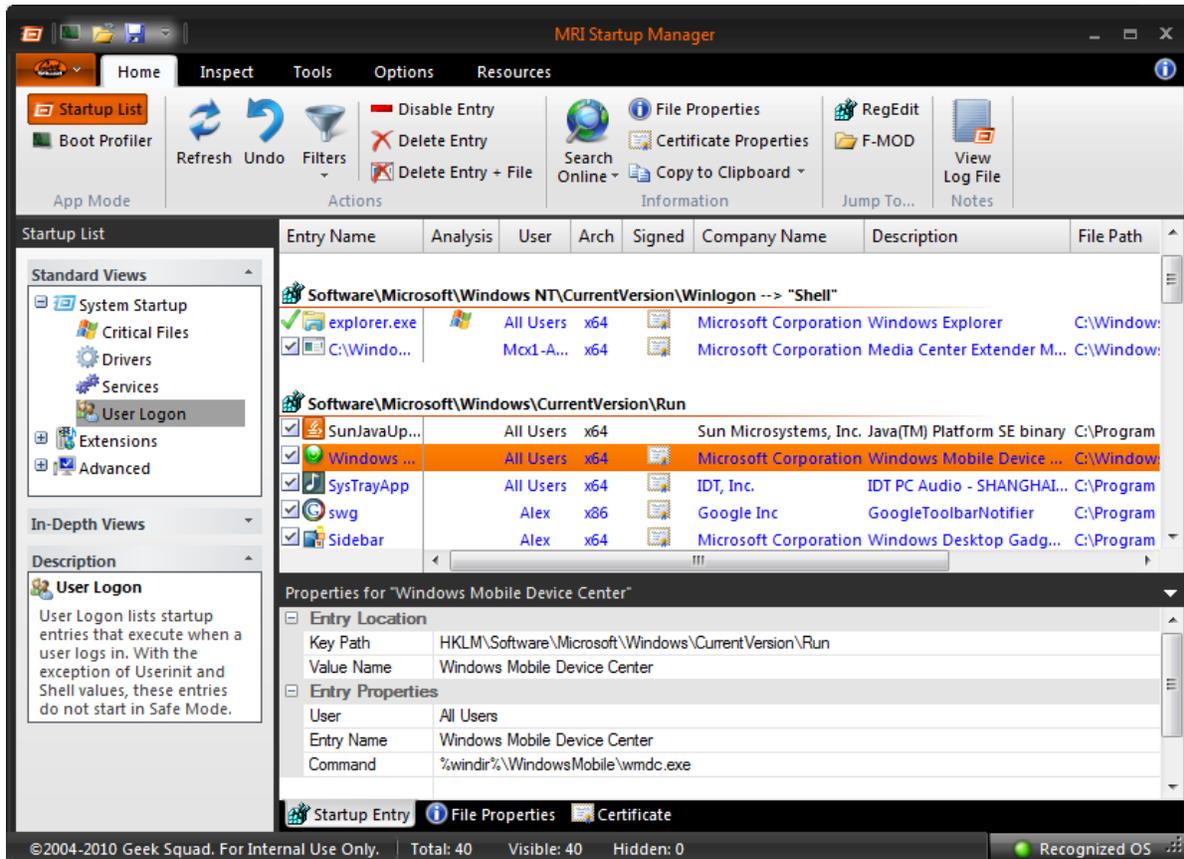
MRI Startup Manager – User Logon

Outside of the User column, the other major change in this view is that the Userinit and Explorer entries are now resets. Whenever these entries have been modified or deleted, Startup List will toss an Analysis warning and the Disable Entry button in the ribbon changes to Reset. This should prove able to solve any issues with Userinit breaking on logon or malware trying to steal explorer.
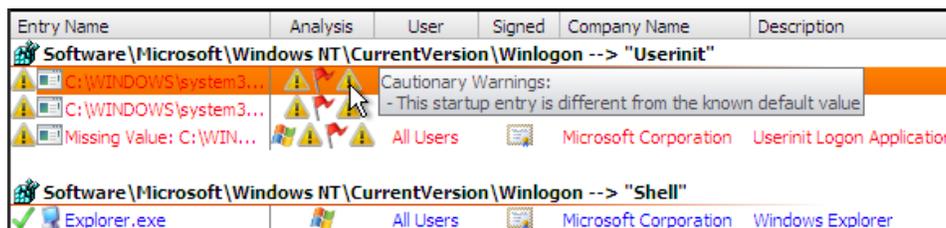
MRI Startup Manager – User Logon – Analysis showing Userinit is compromised by malware
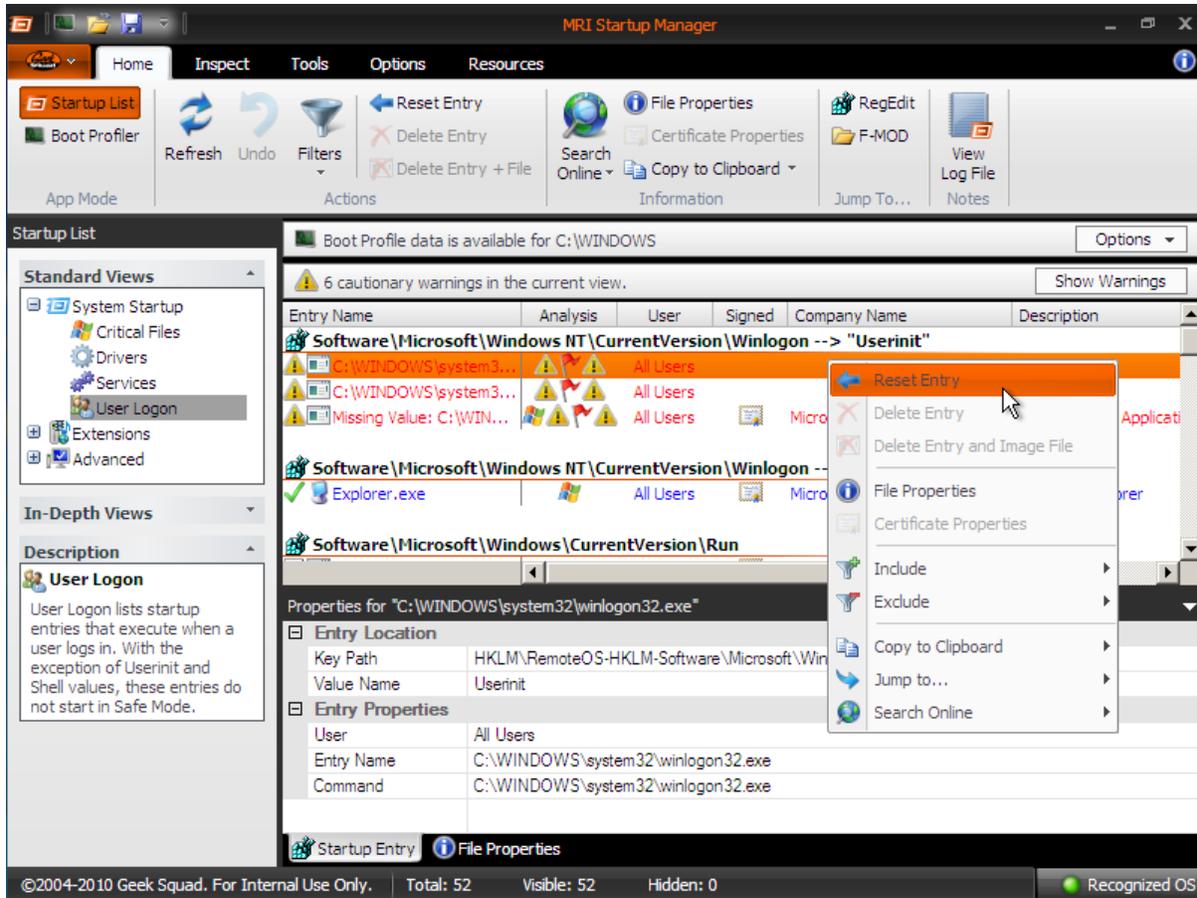
MRI Startup Manager – User Logon – Reset Entry of Userinit compromised by malware

The rest of User Logon is familiar territory with the various basic startup locations. User Logon remains one of the easiest ways to optimize a computer and remove a bulk of a malware infection, as it is the most common startup location to find third party items, malware, and extraneous startup entries in.
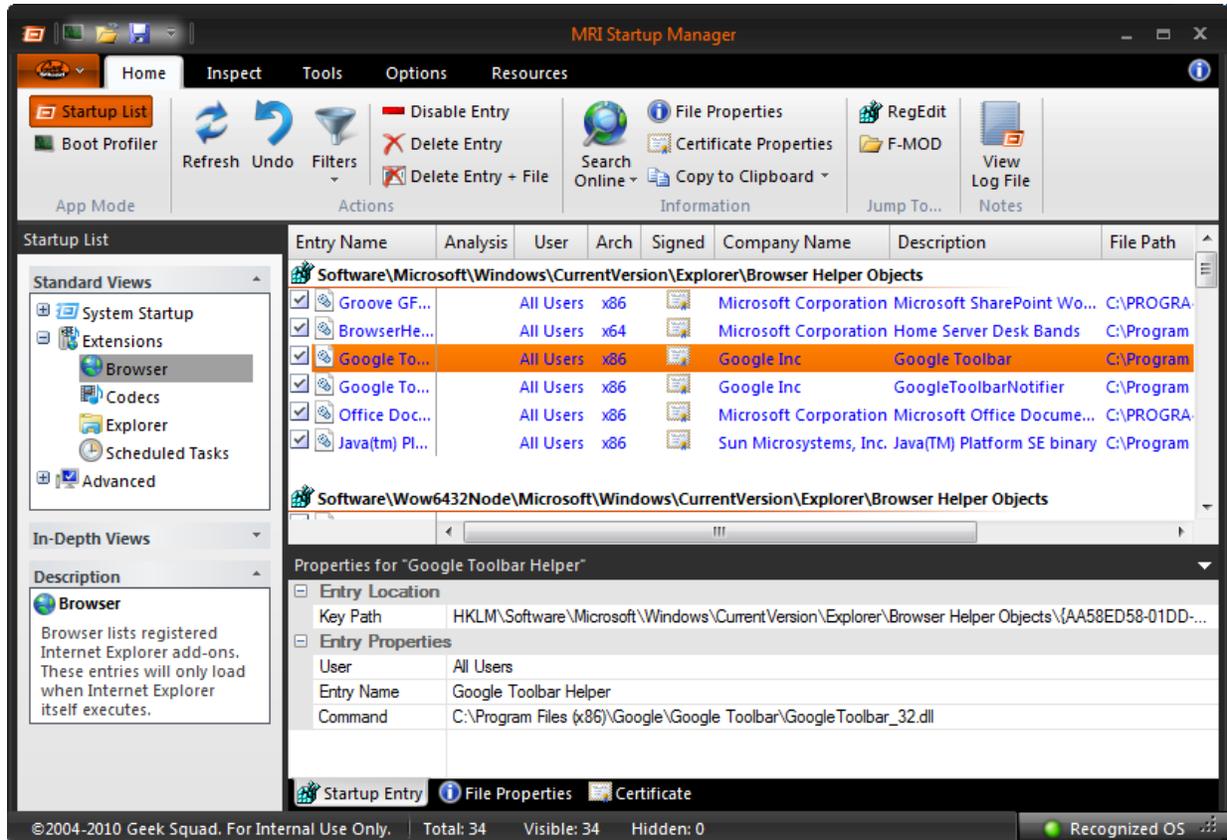
EXTENSIONS

The Extensions category pulls browser add-ons, multimedia codecs, Explorer additions, and scheduled tasks under one simple group. The bulk of the startup entries visible under this header exist by default in Windows, making it wise to take advantage of the Hide Recognized Operating System Files filter. The Codecs category, for example, sees third party codecs interspersed with the many built in ones, and modifications to the built in ones can quickly break audio functionality.
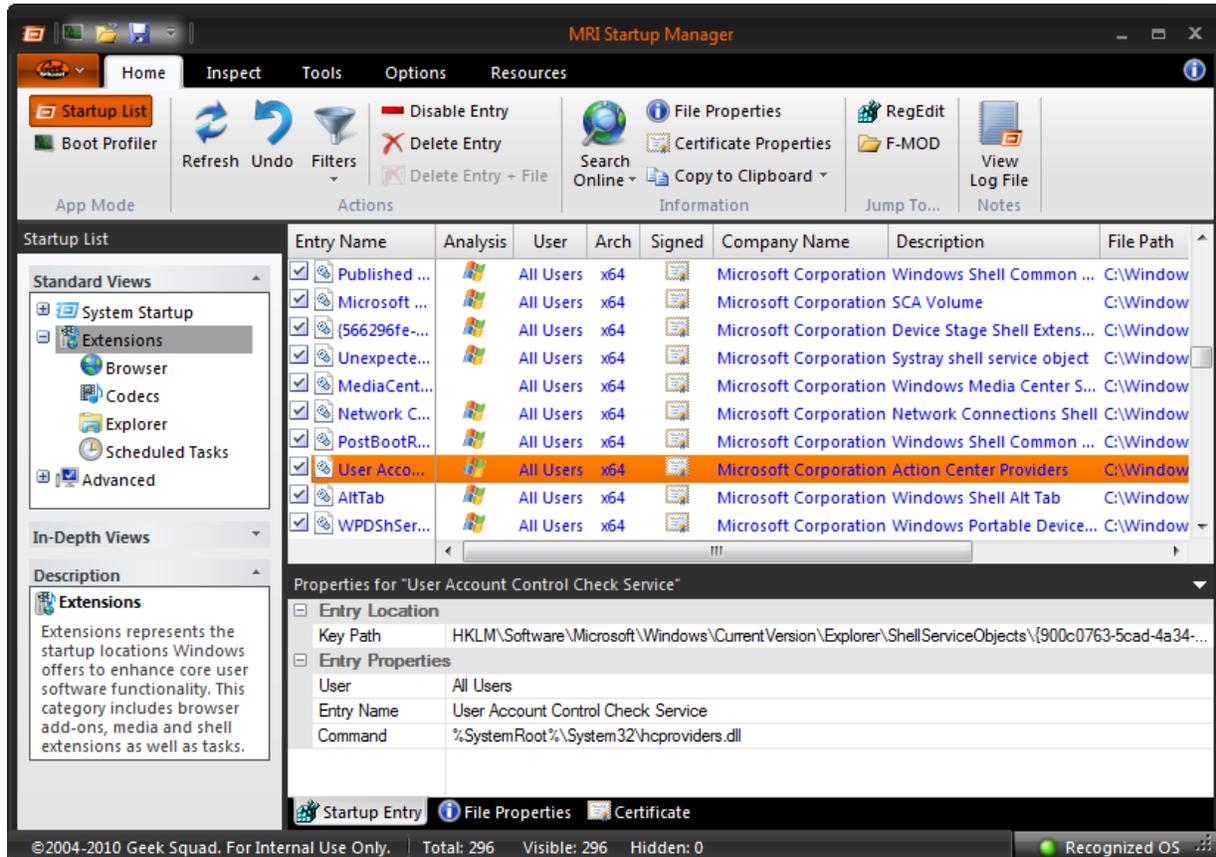
MRI Startup Manager – Extensions

BROWSER

The Browser category currently supports Internet Explorer only; as every entry here is an add-on, supplemental to Internet Explorer itself. So things like toolbars or even security software browser protection add-ons. Also, this is a common area that malware loves to hang out. So feel free to remove the malware but be careful removing other items since it might prevent an add-on from running properly.

MRI Startup Manager – Extensions - Browser

CODECS
This category lists all the multimedia Codecs used by the computer. Codecs are like drivers used by Windows to playback certain types of multimedia content like videos, music, and photos. This could be items that allow playback of DVD video (MPEG2) or even MP3 audio. Malware has been known to chill here too but the more common use is to help identify potential codec conflicts or issues related to not having proper codecs for playback.
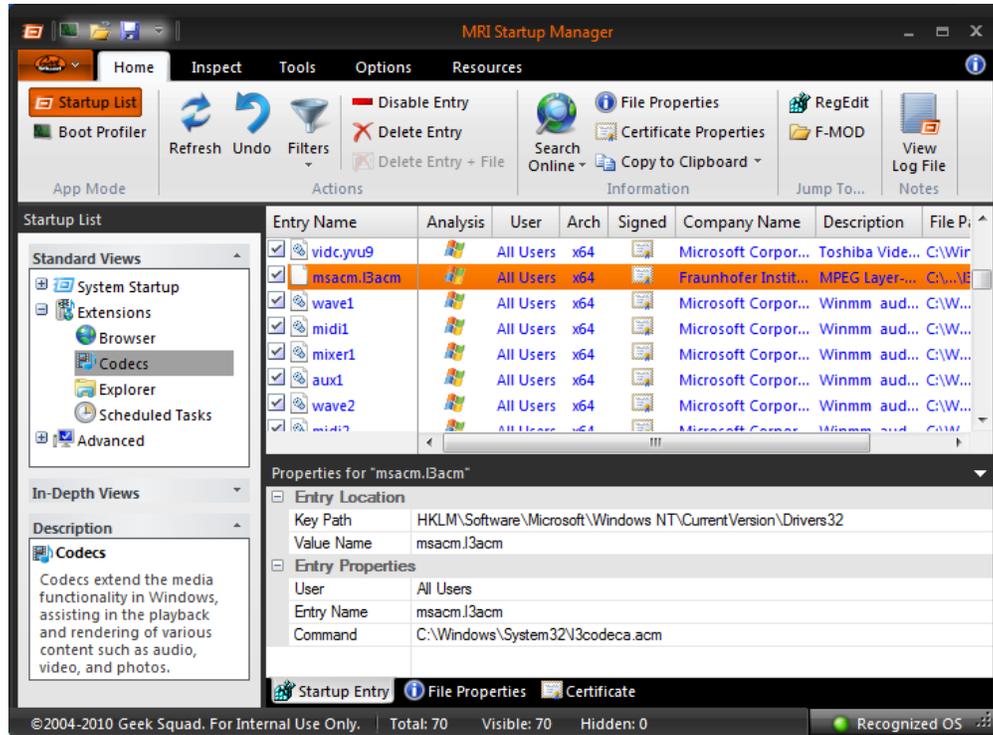
MRI Startup Manager – Extensions - Codecs

EXPLORER

This category organizes Shell Extensions, which add additional functionality to the Windows Shell (Explorer.exe). An example of this could be adding a context menu for 7Zip or integrating Dropbox functionality in to Explorer.
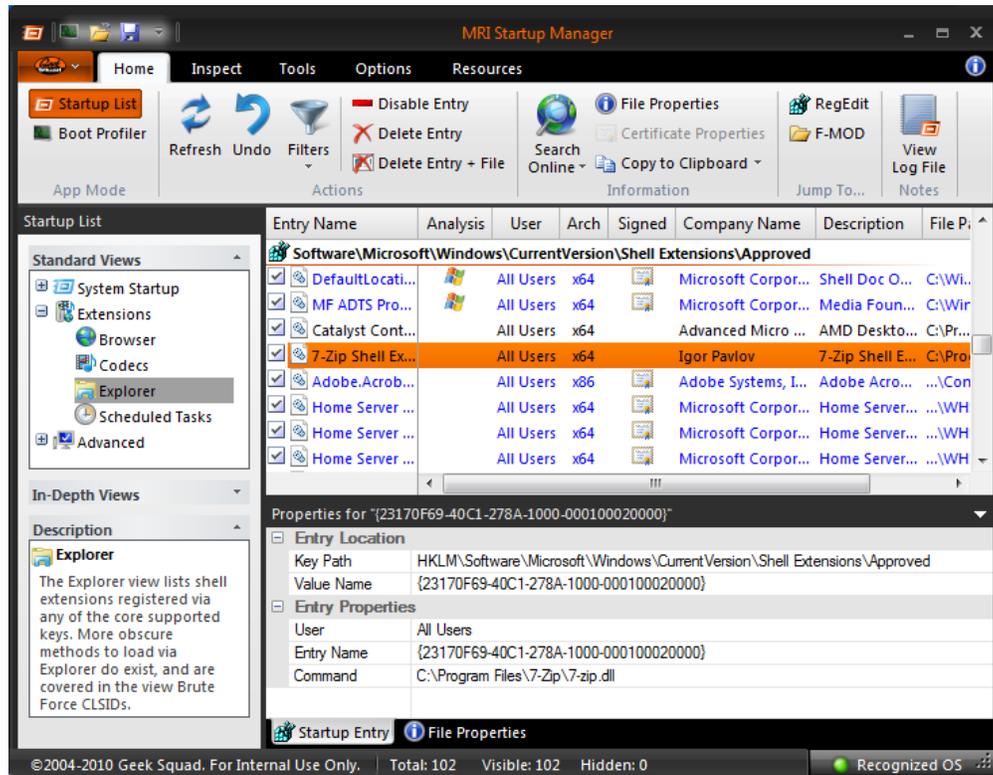
MRI Startup Manager – Extensions - Explorer

Since Explorer is a primary component of the OS (it's the GUI of Windows for crying out loud), this area can be misappropriated by malware to load with Explorer. While you can safely delete malware from this category, you should only modify third party entries from within the respective application to avoid troublesome issues later.

SCHEDULED TASKS

Scheduled Tasks is the last of the Extensions category. With Windows XP, Tasks are used fairly infrequently, and at that mostly by third parties or the off malware here and there. In this case, the entries should be safe to modify as necessary. On the other hand, Vista/7 suspects have seen a strong increase in Scheduled Tasks usage, and tasks are now used to manage events such as Windows Update running at 3 AM, automatic defragmenting, etc.

This massive upgrade to Tasks requires the native Windows viewer for some of the more complex functionality (such viewing and changing times, triggers, etc.), but Startup List can properly disable or delete them without trouble. It is worth noting that the Hide Recognized Operating System Files filter appropriately hides Vista's/7's built in tasks, leaving behind a much more manageable set of items to deal with.
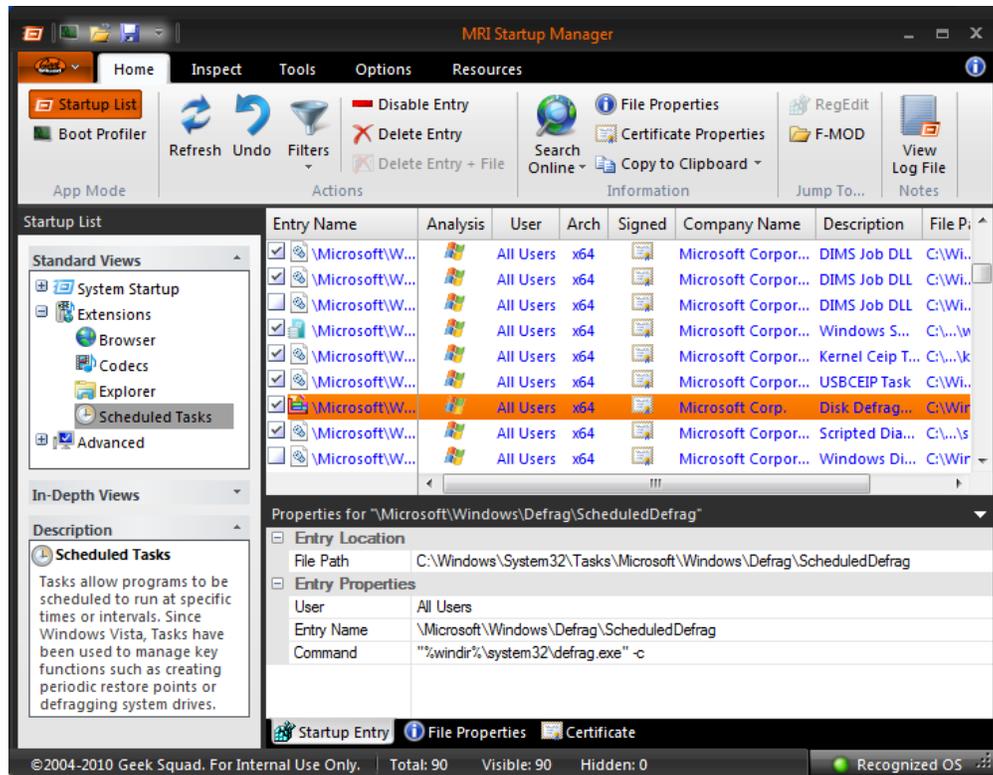
MRI Startup Manager – Extensions – Scheduled Tasks

ADVANCED

The Advanced category combines six views that directly affect various Windows components. Modifications to third party additions in these views should be approached with caution; uninstalling any questionable software properly is liable to be a better approach than directly modifying these entries. That said, the relative obscurity of some of these locations has made it a target for malware authors – to cope with that, resets have been employed where blatant deletion of malware isn't safe.

If you are ever unsure of an entry in these groups, your best bet will be to compare it to the similar entry (or lack thereof) on a known good machine. All in all, a solid filter in place and the highlight on the Advanced category, most of the startup entries present here will be appropriately hidden.
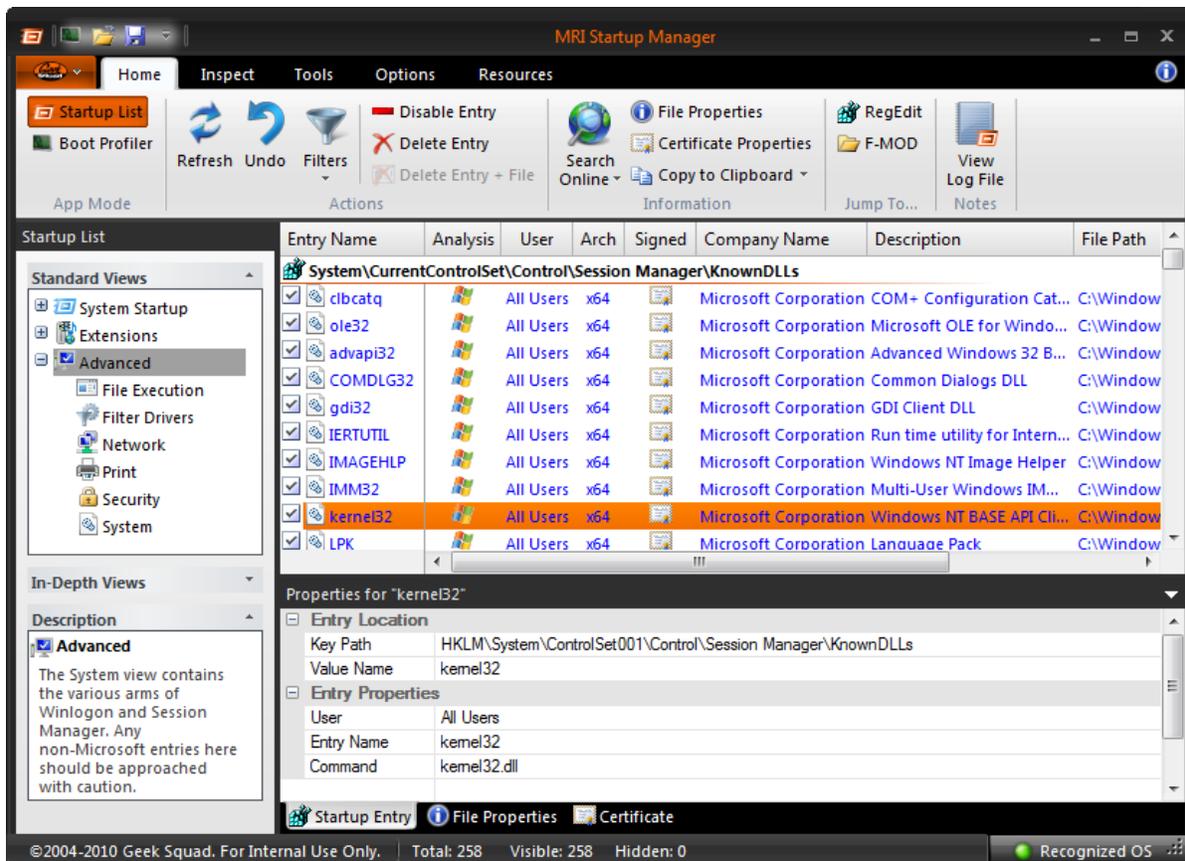
MRI Startup Manager – Advanced

FILE EXECUTION

File Execution serves to pull entries that can directly affect the successful launch of an executable file. From various Debugger keys, to the .exe / exefile Class keys to KnownDlls and elsewhere, if exe files aren't launching, this view should pull the information and offer the resets to get you back up and running.
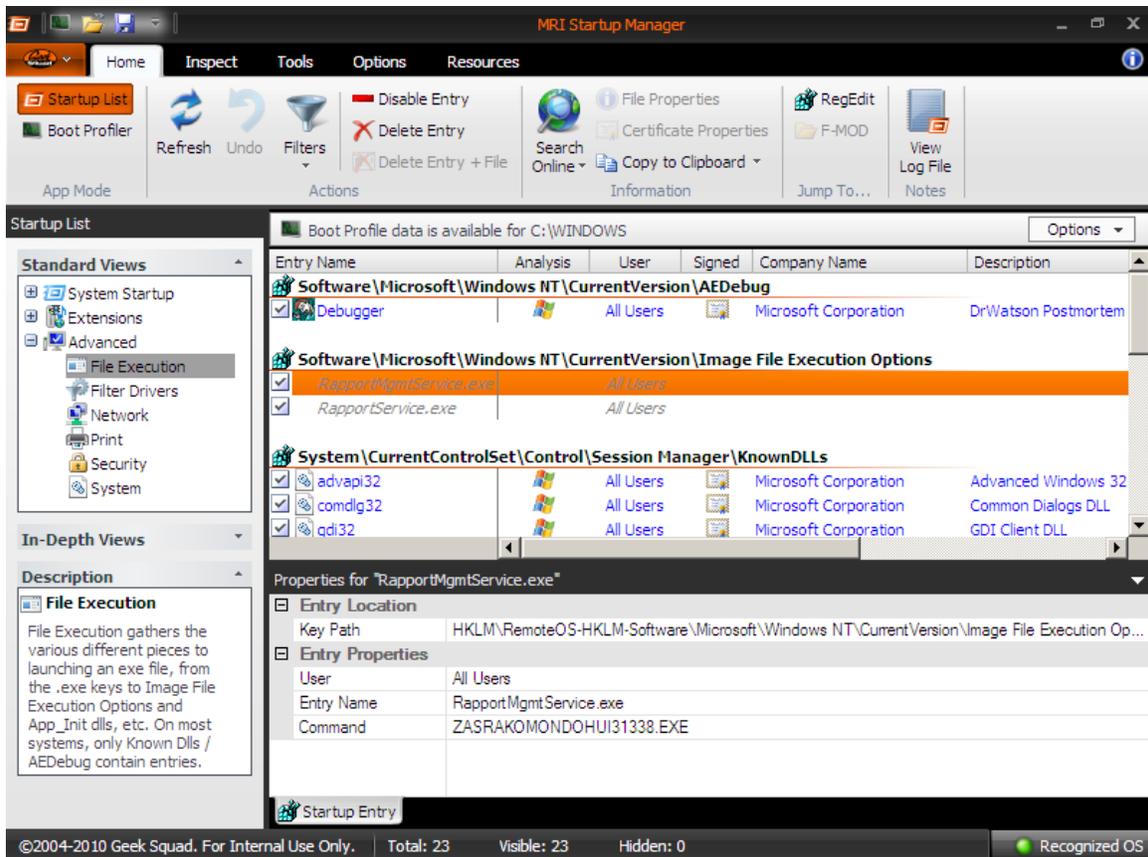
MRI Startup Manager – Advanced – File Execution – Malware leftover attached to Image File Execution Options

FILTER DRIVERS

Filters aren't inherently bad; it's just that when they break, they have a tendency to blow up all of the devices in question. Lots of filters exist by default to aid in the functionality of device; and it's important to call out that merely deleting a filter isn't usually the right fix. Deleting a filter will often remove critical functionality (aka burning CDs in iTunes) or can otherwise break the device, and doesn't target the underlying issue of why the filter was 'broken'. Startup List simplifies working with filters via strong Analysis conditions specific to these entries.

If a filter driver is disabled or broken, the device[s] depending on it will fail to start properly. However, a missing filter can be equally damaging if the device in question is expecting it to be there. The Filter Driver view pulls every filter on the system and lists its start state and current status. A corresponding Loads With column shows with what device[s] specifically the filter will load with. Devices that aren't currently connected to the system will have filter drivers with a status of Stopped; once the device is present though, the status should refresh to Running, and a Running filter is a functioning filter.

MRI Startup Manager – Advanced – Filter Drivers

What this boils to is this: if you think you have a filter issue, Startup List can help you solve it. Every filter on the system is pulled and ran by the Analysis conditions, which will tooltip the exact cause of the problem. If a filter isn't running, try to start it via the context menu and work through the error that returns. Only once you've exhausted your options or determined that the filter is safe to remove should you disable or delete it.

NETWORK

This area covers objects that directly affect network functionality. Things like Winsock objects, Terminal Server objects, and basic networking protocols (i.e. TCP/IP). This is a common place that malicious redirectors may hide and even helpful network security software may lie (i.e. firewall).
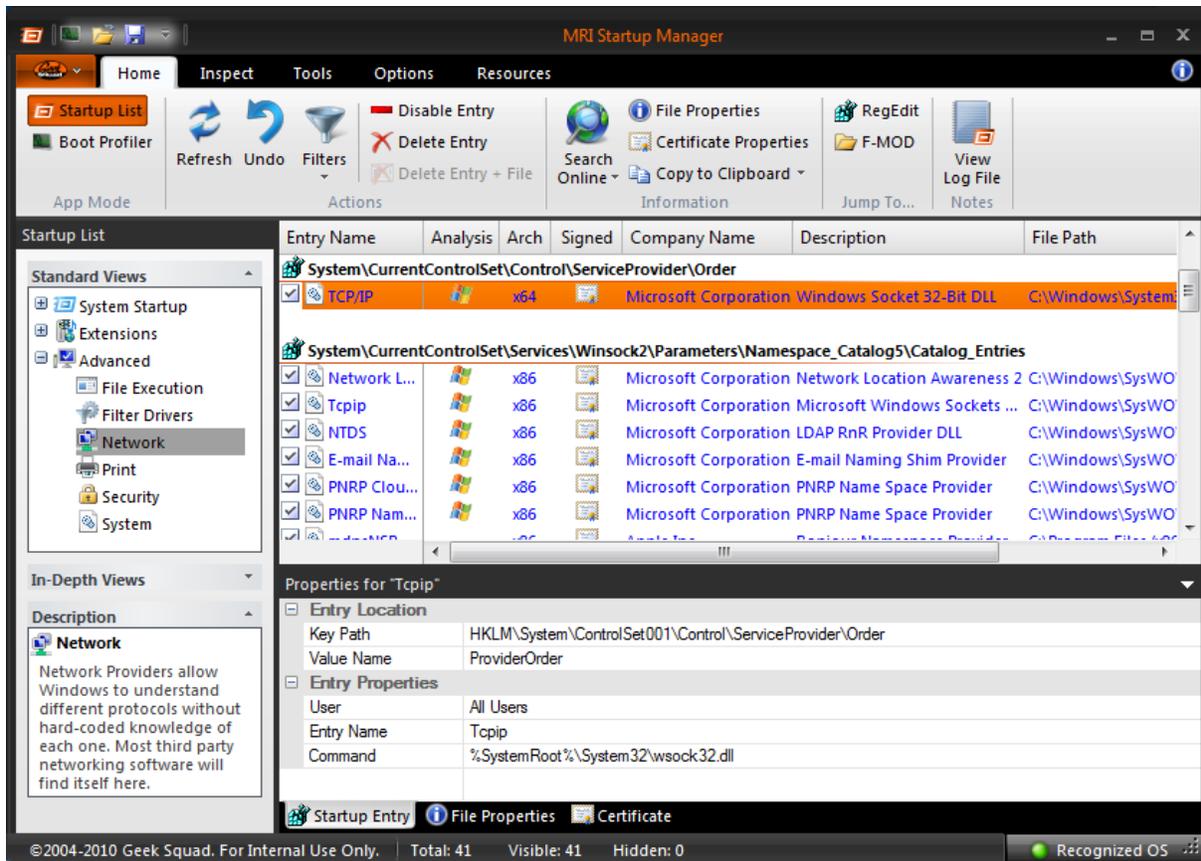
MRI Startup Manager – Advanced – Network

PRINT
This section includes items related to the functionality of the printing subsystem of Windows. That means things that will load with the Print Spooler or directly interact with it to provide basic or enhanced printing functionality. So things like print drivers, monitors, providers, and processors. These items are generally best left untouched but malware could hide here. Also, you may need to check out this area to help manually remove print drivers or resolve Print Spooler conflicts/errors.

MRI Startup Manager – Advanced – Print

SECURITY

This section deals with objects that help in the enforcement of OS security. This includes items that perform actual user account authentication (Authentication Packages) or help enforce system security. Malware has been known to attach here in order to compromise a system but lots of corporate networks also add additional security objects to enhance the security of their user base.
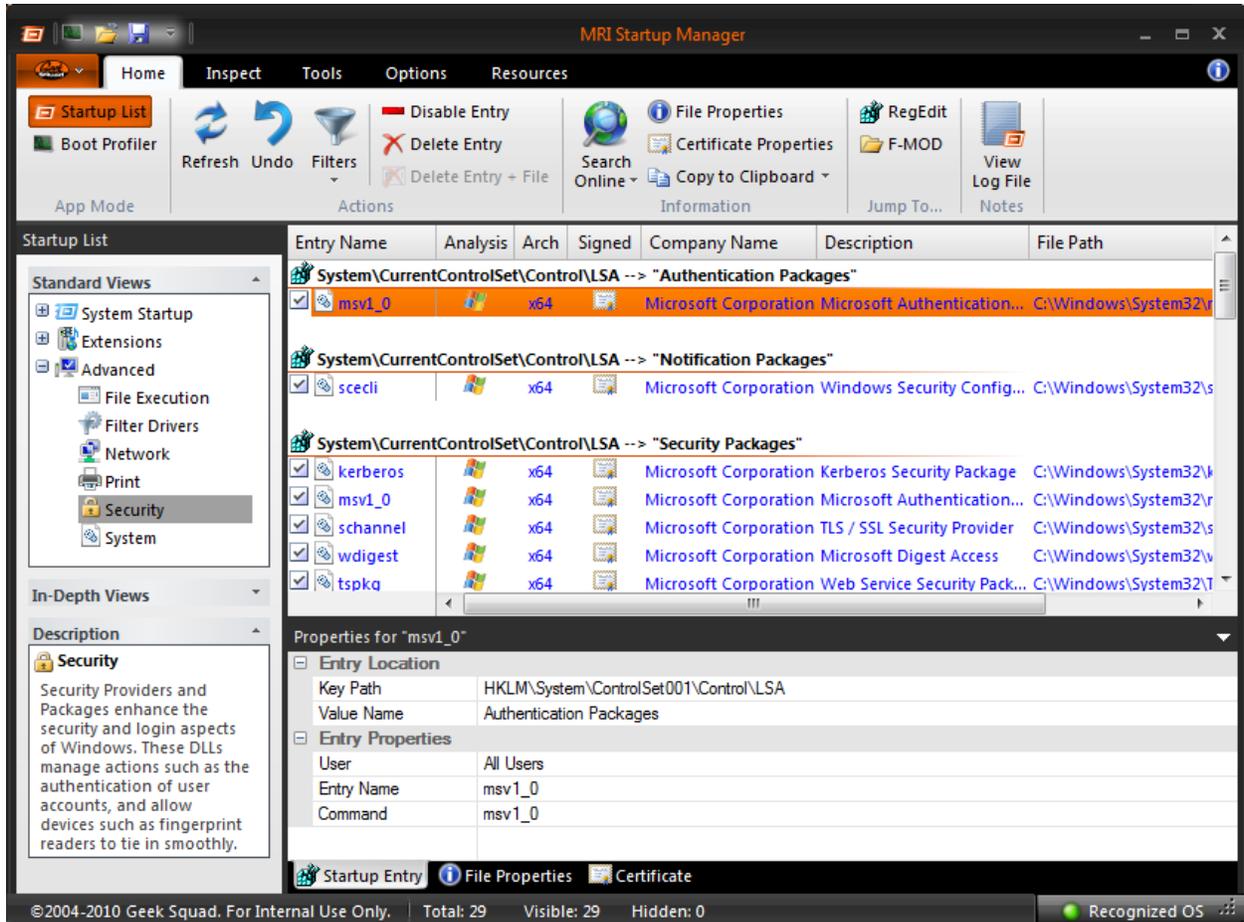
MRI Startup Manager – Advanced – Security

SYSTEM

System is a potpourri of various base startup entries not covered elsewhere, and is mostly powered by resets. Keep in mind that lots of the items in here cover some very important core OS functionality like the actual subsystem and things related to Session Manager. Again, malware likes to get deep in to the OS so this is an area that can be compromised.

MRI Startup Manager – Advanced – System

IN-DEPTH VIEWS

The two In-Depth views exist to make it easier on searching and filtering. The first of the two, the Everything View, works just like it sounds – it takes all of the Standard Views categories and merges their startup entries into one single view. While you lose the columns unique to specific views, you gain a one stop shop for searching or filtering. On many systems, kicking in a full 'Hide Files Signed by Microsoft or Verisign' filter will drop the view's contents down to under one hundred entries.
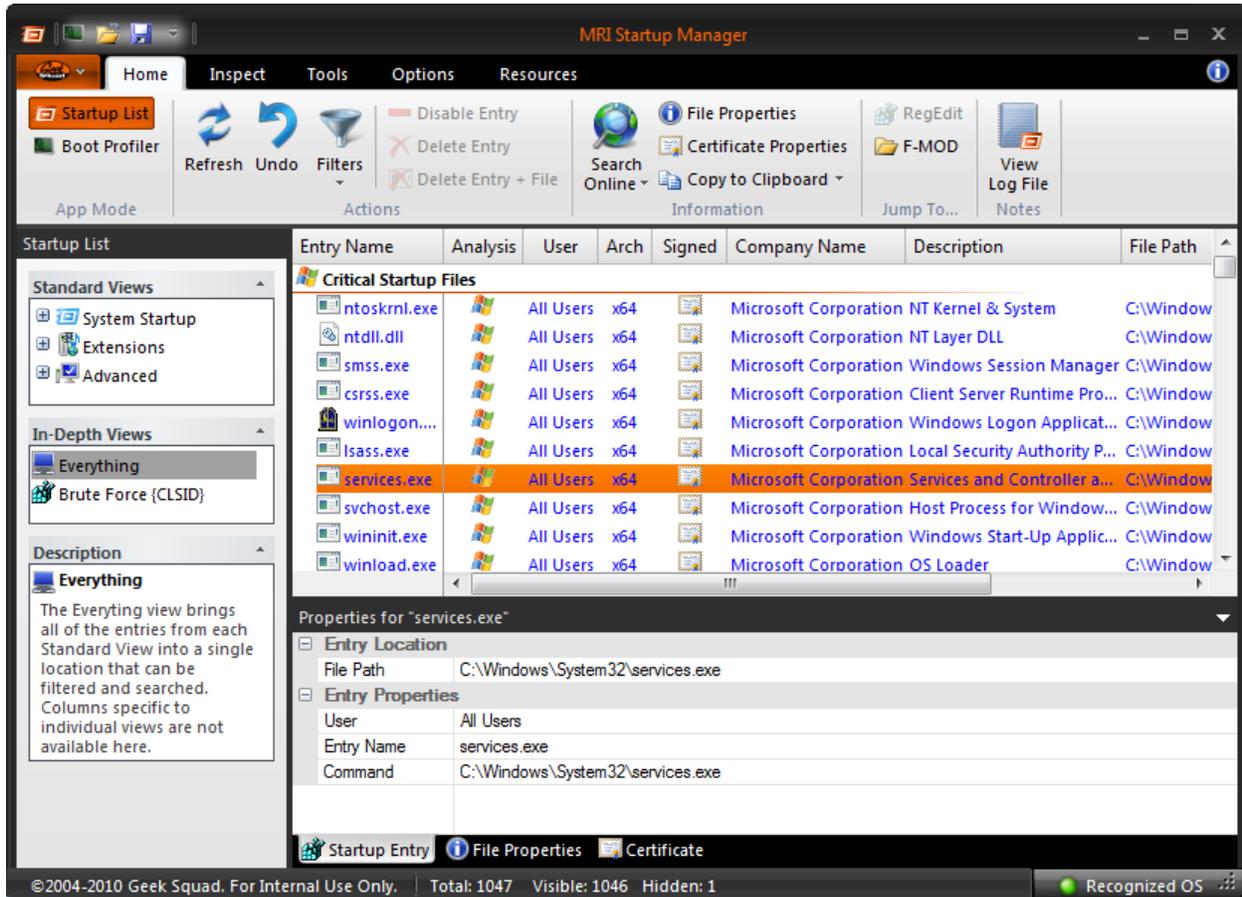
MRI Startup Manager – In-Depth Views - Everything

BRUTE FORCE {CLSID}

Brute Force {CLSID} is perhaps the most complex view in Startup List. If not just due to the sheer number of entries, then due to how obscure what they represent can sometimes feel. A CLSID is a Class ID; it's a unique identifier used by Windows to represent shared components, a piece of something that anyone can reference, use. Browser Helper Objects are registered via CLSIDs, as are Shell extensions. CLSIDs enable everything from versioning to preventing human readable name from overlapping (aka two SuperToolbar programs), to otherwise providing a consistent means for developers to find and use the component they're looking for. Because there is so much going on in Windows behind the scenes with CLSIDs, this view can be quite intimidating.

Startup List shows an additional column of Class Name to offer more information, but it's really only with a filter knocking several thousand entries from view that you can start to get somewhere. That said, you should approach this view with caution. If the goal is to track down a difficult piece of malware, by all means poke around in here. However, given the complex nature of these entries, any modifications to MS or third party entries are liable to break things in ways you hadn't quite imagined. If you're ever unsure if you can just delete an entry, first search online for the {CLSID}. They're unique, of course, so you should be able to track down whether it's an important component or a junk / malicious entry you can kill.

MRI Startup Manager – In-Depth Views - Brute Force {CLSID}

DISABLE, DELETE, RESET

Disable, delete, and resets have been concepts we've touched on briefly so far, but haven't paused to fully explain. In the old Startup Manager, items were disabled largely via MRI_Disabled subkeys scattered about the registry, and delete operations were always permanent. This method didn't offer any easy means to keep track of what was disabled, and led to situations where the client could stumble upon a MRI_Disabled key or an agent would want to undo something but couldn't. Looking to properly bring the three concepts of disabling, deleting, and resetting startup items together, and to enable the reversion of changes, Startup List incorporates a fully functional Undo Manager.
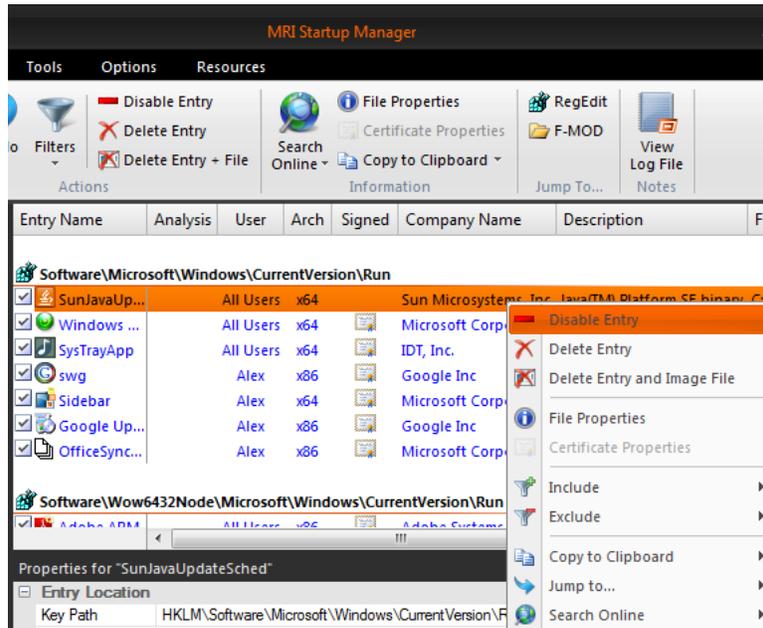
MRI Startup Manager – Delete/Disable example
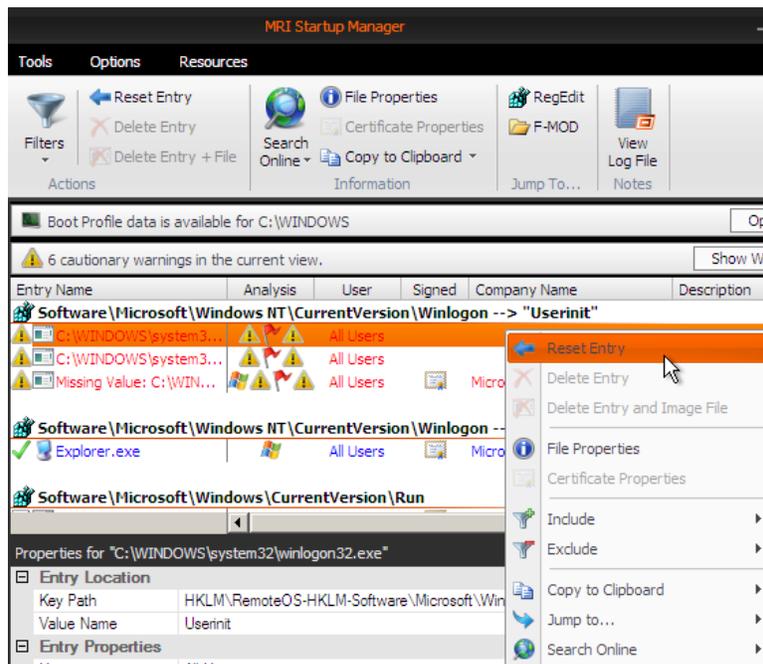
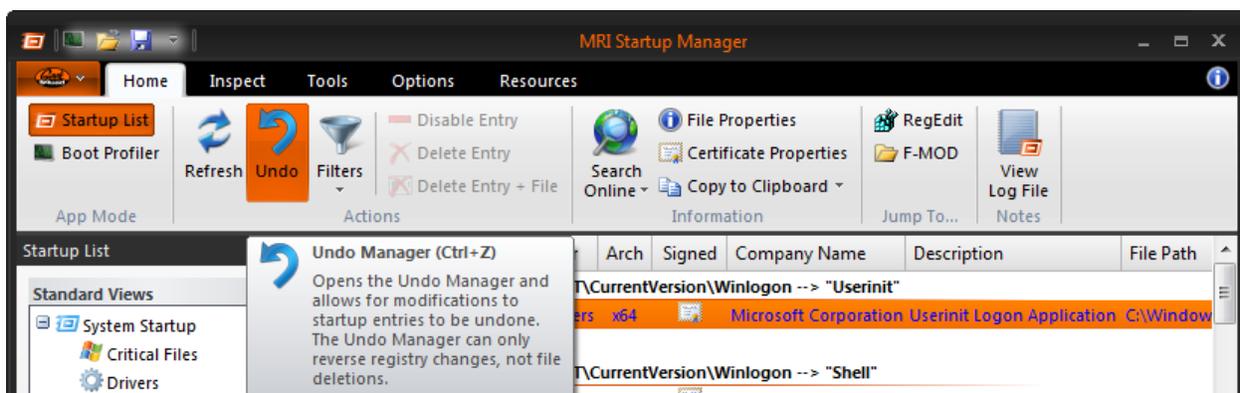*MRI Startup Manager – Reset example*

UNDO MANAGER

Accessed via the Undo button on the Home tab of the ribbon or via Ctrl-Z, the Undo Manager holds the power to revert any action taken on a startup entry. Whether you disabled, deleted, or reset an entry, the Undo Manager was snobbishly following behind you with a clipboard prepared for the moment you realized just how wrong you were. Every registry operation and non-permanent file ones are supported, playing out like so –

- Every disable operation is fully undoable
- Every reset operation is fully undoable
- Every registry deletion is fully undoable
- File deletions are permanent, and will prompt before taking place. Examples may be
    o Delete Entry + File / Shift Delete
    o Deleting Startup folder entries or Tasks (as they are actual files on the hard drive)

With the Undo Manager, you can more easily revert changes to startup items. Bear in mind however that it's only actions taken within Startup List that are tracked; changes made via the Regedit jump to, for example, cannot be tracked.

MRI Startup Manager – Launching Undo Manager
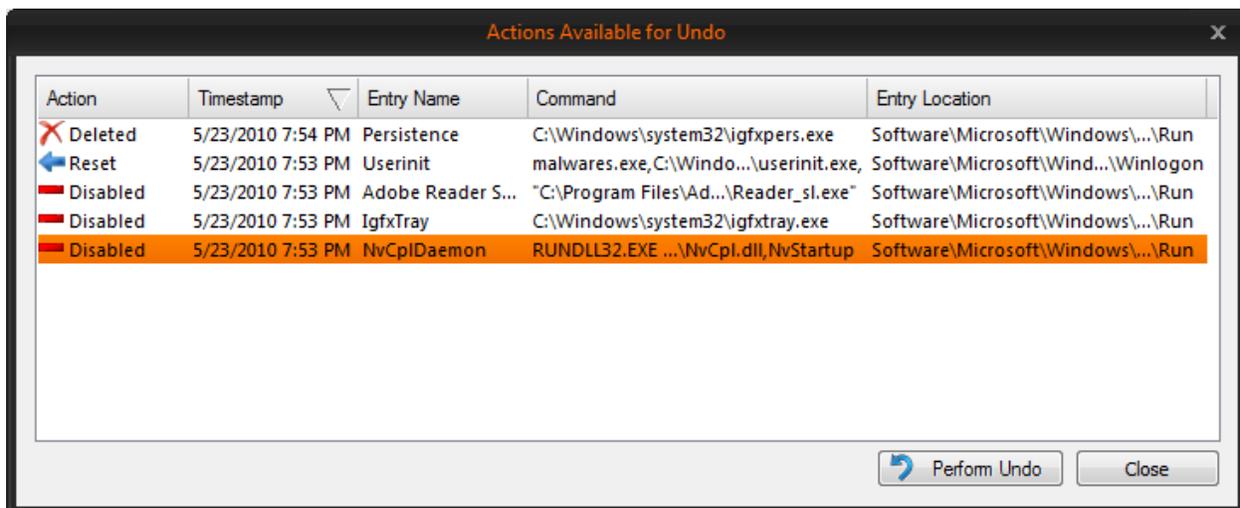
MRI Startup Manager – Undo Manager example

CONCLUSION

Well Agent, you have just finished reading about Startup List. There only one more Toolset Reference document to go, MRI Startup Manager – Boot Profiler. With the basics and Startup List knowledge under your belt and/or badge, you should be able to pick up on Boot Profiler quickly. So get start on the next Toolset Reference document so you can finish this trilogy of awesomeness.

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.