GEEK SQUAD

TOOLSET REFERENCE MRI STARTUP MANAGER - STARTUP LIST

JUNE 2010

CREATED BY: AGENT IAN BANNERMAN





TABLE OF CONTENTS

MAIN TOPICS

	3
WHAT IS STARTUP LIST?	3
STANDARD VIEWS	4
SYSTEM STARTUP	4
CRITICAL FILES	5
DRIVERS AND SERVICES	6
USER LOGON	8
EXTENSIONS	10
BROWSER	11
CODECS	12
EXPLORER	13
SCHEDULED TASKS	14
ADVANCED	15
FILE EXECUTION	16
FILTER DRIVERS	10
NETWORK	18
PRINT	10
SECURITY	20
SYSTEM	20
STOTEM	21
IN-DEPTH VIEWS	22
EVERYTHING	22
BRUTE FORCE {CLSID}	23
DISABLE, DELETE, RESET	24
IINDA MANAGED	25
<u>ONDO MANAGEM</u>	<u> </u>
CONCLUSION	28
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 <u>MRI Toolset</u> <u>Authorized/Unauthorized List</u> 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 <u>MRI Toolset IP Listing</u> 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=261 240

MRI Toolset IP Listing http://infozone/depot/index/docDetail.asp?Doc_ID=280 633

If you have any additional questions, please contact <u>MRI@GeekSquad.com</u>.





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.

🖅 📖 📸 🛒 🔻 I			MRI Sta	rtup Manag	ger			_ = ×
Home Inspect	Tools Option	is Resource	s					()
Startup List Boot Profiler App Mode	o Filters Actions	able Entry ete Entry ete Entry + File	Search Online *	() File Pro	operties cate Propertie: to Clipboard マ tion	ger RegEdit s Composition F-MOD Jump To	View Log File Notes	
Startup List	Entry Name	Analysis Arch	Signed	Start 9	Status SN	A SM w Com	pany Name	Description ^
Standard Views	AxInstSV BEESVC BFE Benjour S Browser Bothserv CertPropSvc Cr_optimiz clr_optimiz clr_optimiz	1 x64 1 x66 1 x64 1 x64		ManualSManualSAutomRManualRManualSManualSDisabledSDisabledSAuto (S	Stopped Stopped Running Running Running Stopped Running Stopped Stopped Stopped	Micro Micro X Micro Apple X Micro Micro Micro Micro Micro Micro	soft Corporation soft Corporation soft Corporation enc. soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation soft Corporation	ActiveX Installe BDE Service Base Filtering I Background In Bonjour Servic Computer Brov Bluetooth Sup Microsoft Smai .NET Runtime (.NET Runtime (
Services	Cir optimiz	× X64	1	Auto (S	stopped	Micro	soft Corporation	NET RUNTIME C
The Services view details the configuration and current state of services on the system. Basic actions such as starting / stopping services or configuring their start types are supported.	Properties for "BITS Entry Location Key Path Entry Propertie User Entry Name Command	HKLM\Syste HKLM\Syste BITS %SystemRoo	em\Controls	Set001\Servi 132\qmgr.dll rtificate	ices\BITS	21		
©2004-2010 Geek Squad. For Inte	rnal Use Only. 🕴 To	otal: 178 Visibl	le: 178	lidden: 0	-		Re	cognized OS 🖃

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!!!

		MR	l Startup	Manager								MR	l Startup	Manager	
ions	Resource	s													
Disab	le Entry	6	N 🛈 F	ile Prope	rties	📸 Reg	Edit			Opti	ons Resourc	es			
Delete	e Entry e Entry + File	Sear Onlin	ch ne → 🗈 C Info	Certificate Copy to C Dormation	Properties	Jump	10D V Lo To N	iew g File otes		D X D	isable Entry elete Entry	Sear	ch	ile Propertie Certificate Pr	es opertie:
	An	alysis	Signed	Start	Status	SM	SM w/N	Company Name		D 🟹	elete Entry + File	Onlin	ie - 🗐 🕻	opy to Clipi	board *
	Disable Entry	 /	1000	Pot	Runni	ng X	Х	Microsoft Corporatio	in 👘	15			Inf	ormation	
×	Delete Entry			anua	i Runnii I Stopp	ng ed	x	Microsoft Corporatio	'n		A	nalysis	Signed	Start	Stat
	Delete Entry	and Ima	age File	anua	l Runni	ng		AuthenTec, Inc.		_		10		Boot	Run
				anua	I Runni	ng		Microsoft Corporatio	n	t —	Disable Entry		[Manual	Run
47	Service/Drive	r Start		▶ stem anua	Runnii I Runnii	ng x na	x	Broadcom Corporatio	on on.	X	Delete Entry			Manual	Stop
100	Service/Drive	r Actior	15	anua	I Runni	ng		Broadcom Corporati	on.		Dalata Entry any	Imperal	File	Manual	Run
0	File Propertie	es		anua	l Runni	ng	х	Broadcom Corporati	on.			image	riie	Manual	Run
	Certificate Pr	opertie	s	anua	l Runnii I Stonni	ng X ed	x	Broadcom Corporation	on.	1	Service/Driver St	art	•	System	Run
-	Include			▶ anua	I Stopp	ed	~	Microsoft Corporatio	'n		Capitas (Driver A	tions		Manual	Run
-	Exclude			stem	Stopp	ed X	х	Microsoft Corporatio	n	1 ann	Service/Driver A	luons	· ·	Manual	Run
U				stem	Runni	ng X	x	Microsoft Corporatio	n	1	File Properties			Manual	Run
	Copy to Clip	board		•		_	_				Cartificata Dean			Manual	Run
>	Jump to			•						N STR	Certificate Prop	erties		Manual	Stop
۹	Search Onlin	ie sterin ver			'atapi'					جه ک	Include		•	Manual	Stop
rties					Company Na	ame: 'Mio	rosoft Cor	poration'		ت ا	Fuchada			System	Stop
	All Users				Certificate Is	suer: 'M	crosoft Co	rporation'		r T	Exclude			System	Run
	atapi		29\atani e	ue.	Directory: 'C	:\WINDO	WS\systen	32\DRIVERS'		Ba	Copy to Clipboa	rd			-
	ayatem 32 \	CHIVE	io latapită	,.	File Name: 'a	atapi.sys'					lump to			de an	
					File Path: 'C	WINDO	WS\system	32\DRIVERS\atapi.sys'			Jump to		· · · · ·	RegEd	n e
y 🚺	File Propertie	es 🦷	Certificat	e	Entry Path: 1	HKLM\Sy	stem\Cont	olSet001\Services\atap	i'	0	Search Online		Þ	F-MOI	0

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 lowerlevel 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.



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.

🖅 📖 📂 🚂 🗢 I			MRI Sta	rtup Manager		_ = ×
Home Inspect	Tools Option	s Resources				()
Boot Profiler App Mode	o Filters	able Entry ete Entry ete Entry + File	Search Online *	 File Properties Certificate Properties Copy to Clipboard ~ Information 	RegEdit F-MOD View Log File Jump To	2
Startup List	Entry Name	Analysis User	Arch	Signed Company Nam	ne Description	File Path
Standard Views * Standard Views * Startup Critical Files Drivers Services User Logon Extensions	winlogon Isass.exe services.exe wininit.exe winload.exe winresume	All Use All Use	ers x64 ers x64 ers x64 ers x64 ers x64 ers x64 ers x64 ers x64	Microsoft Corpe Microsoft Corpe Microsoft Corpe Microsoft Corpe Microsoft Corpe Microsoft Corpe Microsoft Corpe Microsoft Corpe	oration Windows Logon A oration Local Security Aut oration Services and Cont oration Host Process for V oration Windows Start-Up oration OS Loader oration Resume From Hib	Applicat C:\Windows\S hority P C:\Windows\S iroller a C:\Windows\S Mindow C:\Windows\S p Applic C:\Windows\S C:\Windows\S ernate C:\Windows\S
🖽 🔛 Advanced	Drivers					
In-Depth Views 🔻	✓ 🚳 1394ohci ✓ 🚳 ACPI	All Use	e <mark>rs x64</mark> ers x64	Microsoft Corpo	pration 1394 OpenHCI Dri pration ACPI Driver for NT	iver C:\Windows\s C:\Windows\s
Description	🗹 🚳 AcpiPmi	All Use	ers x64	Microsoft Corpo	oration ACPI Power Meter	ring Driv C:\Windows\s
System Startup contains the core segments of the Windows boot process. It is recommended to use this view with Hide Recognized OS Files on, leaving only non-standard and third party files visible.	Properties for "1394 Entry Location Key Path Entry Propertie User Entry Name Command Startup Entry	Al Users Al Users 1394ohci system32\DF	m\ControlS RIVERS\13 s Cer	Set001\Services\1394ohci 394ohci.sys tificate #*Service/Driver		
©2004-2010 Geek Squad. For Inte	rnal Use Only. To	ital: 493 Visibl	e: 492 F	lidden: 1		Recognized OS 44

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.

🖅 📖 📸 🔛 🔻 I			MRI Start	up Manager		- = ×
Home Inspect	Tools Options	Resources	s			()
E Startup List Boot Profiler App Mode	to Filters Actions	ble Entry te Entry te Entry + File	Search Online *	 File Properties Certificate Properti Copy to Clipboard Information 	ies CrepEdit	2 W File es
Startup List	Entry Name	Analysis Arch	Signed	Company Name	Description	File Path
Standard Views	A Critical Startup Fi	iles				E
T T Surtan Startun	💷 ntoskrni.exe	📲 x64		Microsoft Corporation	NT Kernel & System	C:\Windows\System3:
Critical Files	🚳 ntdll.dll	🦓 х64		Microsoft Corporation	NT Layer DLL	C:\Windows\System3:
Driver	smss.exe	鸄 хб4		Microsoft Corporation	Windows Session Manag	er C:\Windows\System3.
Convince	csrss.exe	鸄 хб4		Microsoft Corporation	Client Server Runtime Pro	C:\Windows\System3.
Services	🕼 wintegen	🧾 📈 📈		Microsoft Composition	Windows Logon Applicat	Civitin douur Curtom?
User Logon		•				
Extensions	Properties for "ntos	krnl.exe"				•
Advanced	File Attributes					*
	File Path	C:\Wind	lows\Syste	em32\ntoskrnl.exe		
In-Depth Views *	Size	5.3 MB				
Description *	Attributes					
Artical Files	Architecture	X64				
The Critical Files view lists	Comments					=
key operating system files	Company Name	Microsoft Co	prooration			
required for Windows to boot properly. These files	Description	NT Kernel &	System			
should always be present	File Version	6.1.7600.16	539 (win7_	gdr.100226-1909)		
and signed on the system.	Internal Name	ntkmlmp.exe	в			
	Legal Copyright	C Microsoft	Corporation	n. All rights reserved.		
	Original File Name	ntkmlmp.exe	е			
	Product Version	6.1.7600.16	539			
	File Date/Time	Stamps				-
	🚮 Startup Entry	🕕 File Propertie	s Cer	tificate		
©2004-2010 Geek Squad. For Inte	ernal Use Only. Tot	tal: 11 Visibl	le: 11 H	idden: 0		Recognized OS
		Charlens A	1	Critical Fi	1	

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.

🖅 🔍 📂 🔛 🔻 I			MRI Startup Ma	nager				_ = ×
Home Inspect	Tools Options	Resources						()
App Mode	to Filters Actions	e Entry e Entry e Entry + File	Search Online +	e Properties ertificate Prope opy to Clipboar rmation	rties 🖾 rd 👻	F-MOD F-MOD Log ump To No	ew File tes	
Startup List	Entry Name A	Analysis Arch	Signed Start	Status	SM SN	1 w Company	y Name	Description *
Standard Views	AsyncMac	A x64	Manu	al Running		X Microsoft	Corporation	MS Remote
🗏 🖅 System Startup	🕙 🕙 atapı	×64	Manu	Running al Running	X	ATI Techno	Corporation	ATAPI IDE MI
Critical Files	🗹 🚳 atikmdag	x64	Manu	al Stopped		ATI Techno	ologies Inc.	ATI Radeon I
Services	🗹 🚳 b06bdrv	灯 х64	Manu	al Stopped	x	X Broadcom	Corporati	Broadcom N
Scruces & User Logon		A	Manu III	ol Stoppod		V Propdcom	Corporati	Propdrom N
🗉 職 Extensions	Properties for "atapi"					_		•
🗄 🕎 Advanced	Service Informat	tion						*
	Service Name	atapi						
In-Depth Views *	Display Name	IDE Channe	l					
Description *	Description	Komol Drivo	-					
Drivers	Service Initializa	ation	1					E
The Drivers view details	Start	Boot						
information on installed	Current State	Running						
type, current status, and	Group	SCSI Minipo	rt					
whether they can start in	Dependencies							
such as starting / stopping	Allowed in Safe Mo	Yes						
drivers or configuring their	Allowed in Safe Mo	Yes						
start types are supported.	Instances	IDE CL						
	ROOT LEGACT_AT	IDE Channe	10					
			1		_			
	🟭 Startup Entry (File Propertie	s 🧾 Certificate	Service/D	river			
©2004-2010 Geek Squad. For Inte	ernal Use Only. Tota	al: 264 Visibl	e: 263 Hidden	1			Receiption	ognized OS 🚟

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.

× ×	Disable Entry Delete Entry Delete Entry and Image File	N	Incresoft Corporation DHG licrosoft Corporation DNS licrosoft Corporation Wire licrosoft Corporation WD	×	Disable Entry Delete Entry Delete Entry and Image File	orp	oration Micros	×	Disable Entry Delete Entry Delete Entry and Image File	ji ji	es, In es Inc	c. ATI High D c. ATI Radeor
\mathcal{C}_{k}^{0}	Service/Driver Start	۱	✓ Automatic	10 ¹⁰	Service/Driver Start	•		${\mathfrak A}_{{\mathfrak a}}^{{\mathfrak A}}$	Service/Driver Start	•	v	Boot
18 ⁴⁰	Service/Driver Actions	۲	Automatic (Delay)	43.03	Service/Driver Actions	•	Start	19 ¹⁰	Service/Driver Actions	F	2	System
0	File Properties Certificate Properties		Manual Disabled	0	File Properties Certificate Properties		Stop Pause	0	File Properties Certificate Properties		1	Automatic Manual
*	Include	► de	s for this computer. If this servi	7	Include	•	Resume Restart	7	Include	•	[Disabled
T	Exclude			T	Exclude			T	Exclude	Þ		
	Copy to Clipboard	► E			Copy to Clipboard	•			Copy to Clipboard	F.		
\$	Jump to	•		\$	Jump to	•		\$	Jump to	F		
٨	Search Online	Þ		٨	Search Online	F		ø	Search Online	F		

MRI Startup Manager – Service/Driver Context Menu

🖅 📖 📸 🚂 🔻			MRI Startup Mana	iger			_ = x
Home Inspect	Tools Option	ns Resources	;				()
Startup List Soot Profiler App Mode	ndo Filters Actions	able Entry lete Entry lete Entry + File	Search Online + Cop	Properties ificate Properties y to Clipboard マ nation	📸 RegE 🍙 F-MC	dit View Log File Notes	
Startup List	Entry Name	Analysis Arch	Signed Start	Status SM	SM w	Company Name	Description *
Standard Views	DAUpdate ComLaun ComLaun	x86 🔊 x64 ಶ x64	Manual Autom Manual	Stopped Running X Stopped	x	BioWare Microsoft Corporation Microsoft Corporation	DAUpdaterS Distributed (Microsoft\Di
Drivers	✓ <mark>[®] Dhcp</mark> ✓ [®] Dhscache ✓ [®] dot3syc	<mark>∦∛ x64</mark> № x64 № x64	Autom Autom Manual	Running Running Stopped	X X X	Microsoft Corporation Microsoft Corporation Microsoft Corporation	DHCP Client DNS Caching Wired Auto(
User Logon B the Extensions							- F
🗄 🕎 Advanced	Properties for "Dho	:p"					•
In-Depth Views	Service Inform	Dhcp					
Description	Display Name Description	DHCP Client Registers and	updates IP address	es and DNS record	s for this con	nputer. If this service is s	opped, this
The Services view details	Service Initial	ization	:55				-
the configuration and current state of services on the system. Basic actions such as starting / stopping	Start Current State Group	Automatic Running TDI					
services or configuring their start types are supported.	Dependencies Allowed in Safe I Allowed in Safe	NSI, Tdx, Afd M No M Yes					
	Startup Entry	(i) File Propertie	s 📕 Certificate	Service/Driver			
©2004-2010 Geek Squad. For I	nternal Use Only.	otal: 178 Visibl	e: 178 Hidden: 0			Rec	ognized OS 🖽
		MRI Startup	o 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.

🖅 📖 📸 🛃 🔻						м	RI Start	up Mana	ger					_ =	x
Home	Inspe	ct	Tools Op	tions	Res	ources								(i
Startup List	🥏 Refresh	J Und	Filters Actions	Disab Delet Delet	ole Entry se Entry se Entry +	File O	iearch nline *	 File F Certif Copy Information 	Properties ficate Propert to Clipboard ation	ies ies i i ≠ Jun	RegEdit F-MOD np To	View Log File Notes			
Startup List			Entry Name	A	Analysis	User	Arch	Signed	Company N	lame	Descripti	on		File Path	•
Standard Views	ip 1 Tasks	4	Image: Second system Image: Second system	d t e te c c p er		All Users All Users All Users All Users All Users All Users All Users All Users All Users All Users	x64 x64 x64 x64 x64 x64 x64 x64 x64		Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca Microsoft Ca	orporation prporation prporation prporation prporation prporation prporation prporation	Windows SCA Volu Device Sta Systray sh Windows Network V Windows Action Ce Windows Windows	Shell Com me age Shell E ell service Media Ce Connectio Shell Com nter Provid Shell Alt T Portable I	imon object nter S ns Shell imon ders ab Device	C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window	
Description		*	Properties for *	llear /	Account (ontrol C	ack Sa	nvice"			_			,	_
Extensions Extensions represe startup locations W offers to enhance of software functiona category includes b add-ons, media and extensions as well a	nts the Vindows core user ality. This prowser d shell as tasks.		Entry Loca Key Path Entry Prop- User Entry Name Command Startup Ent	erties	HKLM\So All Users User Acc %System	oftware \M ount Contr Root %\Sys	ol Chec stem 32	Windows k Service hcprovide	Current Versior rs.dll	n\Explorer\:	ShellServic	eObjects\{	900c076	3-5cad-4a34	4
©2004-2010 Geek So	quad. For	r Inte	rnal Use Only.	Tota	al: 296	Visible: 2	96 H	lidden: 0					Reco	gnized OS	

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.

🖅 📖 📸 🛒 = I		MRI St	artup N	lanage					⊨ x
Home Inspect	Tools Options	Resourc	es						1
Startup List Boot Profiler App Mode	o Filters Actions	o le Entry e Entry e Entry + File	Sea Onlin) (rch ne + () File Pro Certific Copy to Informati	perties ate Properties) Clipboard ~ on	📸 RegEdit 🍙 F-MOD Jump To	Viev Log F Note	v N ile
Startup List	Entry Name	Analysis	User	Arch	Signed	Company Na	ame Descrip	tion	File Pi 🔦
Standard Views	🗹 🚳 vidc.yvu9	🦧 A	II Users	x64		Microsoft Cor	por Toshiba	Vide	C:\Wir
 ⊕ System Startup Extensions 	msacm.l3acm wave1 wave1 with mixer1 water1 water1 water1 water2 water2 water2 water2 Properties for "msacm.l3acm	- 20 A - 20	II Users II Users II Users II Users II Users II Users	x64 x64 x64 x64 x64 x64 x64		Fraunhofer In Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	stit MPEG L por Winmm por Winmm por Winmm por Winmm por Winmm	ayer (aud (aud (aud (aud (aud (C:\W C:\W C:\W C:\W C:\W C:\W
In-Depth Views	 Entry Location Key Path 		m Miem	ooft\\M/	indowo NT		Drivor 22		
Description ^	Value Name	msacm.l3acm	ire vivlicro	SOIL \VVI		i vourrent Version	Univers32		
Codecs extend the media functionality in Windows, assisting in the playback and rendering of various content such as audio, video, and photos.	User Entry Name Command	All Users msacm.l3acm C:\Windows\\$	System 32	2V3cod	eca.acm				
©2004-2010 Geek Squad. For Inte	rnal Use Only.	File Propert	ies 🔜	Certifi Hide	cate den: 0		Re	cognize	d OS 🔐

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.

🧰 📖 💋 🔛 s				MRI	Startup M	lanage						x
Home	Inspect	Tools	Options	Resou	urces							1
Startup List	🥏 📕 Refresh Ur	odo Filters Actio	Disab Delet M Delet	le Entry e Entry e Entry + Fi	ile Onlin) 0 rch ne ▼ 1	File Pro Certifica Copy to	perties ate Properties • Clipboard on	اللہ اسر	RegEdit F-MOD Lo mp To	/iew g File lotes	
Startup List		Entry Nam	e	Analysis	User	Arch	Signed	Company Na	me	Description	File	Pi 🕋
Standard Views	*	💣 Softwar	e\Microso	ft\Window	vs\Current	Versior	n\Shell Ex	tensions\Appro	oved			
	tup ed Tasks	Y Image: Constraint of the second s	ultLocati DTS Pro yst Cont Shell Ex be.Acrob e Server e Server e Server		All Users All Users All Users All Users All Users All Users All Users All Users	x64 x64 x64 x64 x64 x64 x64 x64		Microsoft Corp Microsoft Corp Advanced Micr Igor Pavlov Adobe System Microsoft Corp Microsoft Corp Microsoft Corp	oor oor 5, I oor oor	Shell Doc O. Media Foun, AMD Deskto 7-Zip Shell E Adobe Acro. Home Server Home Server	. C:\M C:\M C:\Pi C:\Pi \C \W	Vi Vir r on /H /H →
In-Depth Views	Ψ.			•			111		_			F
Description Explorer The Explorer view extensions regist any of the core sı keys. More obscu methods to load Explorer do exist, covered in the vie Force CLSIDs.	I lists shell ered via upported ire via and are w Brute	Properties Entry L Key Patl Value N Entry F User Entry Na Commar Startup	for *{23170 ocation n ame Properties ame nd b Entry	DF69-40C1- HKLM\Soft {23170F69- All Users {23170F69- C:\Program File Propo	278A-1000 ware \Micro 40C1-278A 40C1-278A Files \7-Zip erties	-000100 soft\Wi -1000-0 -1000-0 \-1000-0	ndows\Cu 00100020 00100020	urrent Version \She 1000} 1000}	ell Exte	ensions\Appro	ved	•
©2004-2010 Geek	Squad. For In	ternal Use On	ly. Tota	al: 102 V	isible: 102	Hide	den: 0			Recogn	ized O	si

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.

🖅 📖 对 🚽 🔻				MRI	Startup N	lanagei					⊨ x
- 😂 🕶 Home	Inspect	Tools	Options	Resou	rces						(
Startup List	Refresh U	ndo Filters	Disable Delete	e Entry Entry Entry + Fil	sea Onli	rch ne +	File Pro Certifica Copy to	perties ate Properties Clipboard 👻	💣 R 🍃 F	egEdit -MOD Log p To	ew File tes
Startup List		Entry Nar	ne	Analysis	User	Arch	Signed	Company Na	me	Description	File Pi ^
Standard Views	up d Tasks		rrosoft\W rrosoft\W rrosoft\W rrosoft\W rrosoft\W rrosoft\W rrosoft\W rrosoft\W		All Users All Users All Users All Users All Users All Users All Users All Users All Users	x64 x64 x64 x64 x64 x64 x64 x64 x64		Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	oor E oor E oor V oor V oor V oor U oor S oor V	DIMS Job DLL DIMS Job DLL DIMS Job DLL Windows S Kernel Ceip T JSBCEIP Task Disk Defrag. Scripted Dia Windows Di	C:\Wi C:\Wi C:\Wi C:\\w C:\\w C:\\s C:\Wir C:\\s
Description	*	Properties	for "\Micro	soft\Windo	ows\Defra	g\Sche	duledDef	rag"			_
Cheduled Task Tasks allow progr scheduled to run times or intervals. Windows Vista, Ta been used to mar functions such as periodic restore p defragging system	ams to be at specific Since asks have hage key creating oints or n drives.	File Pat File Pat Entry User Entry N Comma	h (Properties	C:\Windows All Users \Microsoft\V "%windir%\s File Prope	\System3 Vindows\I ystem32\c	2\Tasks Defrag\S lefrag.ex	Microsoff Scheduled (e'' -c	\Windows\Defra	ag\Sch	eduledDefrag	
©2004-2010 Geek S	Squad. For I	nternal Use Or	nly. Tota	l: 90 Vi	sible: 90	Hida	ien: 0			Recogniz	ed OS 🖽

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.

-						м	RI Start	up Mana	ger				_ =	x
- Home	Inspe	ct	Tools	Option	ns Re	sources								1
Startup List Boot Profiler R App Mode	🥏 lefresh	5 Undo	Filters Actio	Disa Del M Del	able Entry ete Entry ete Entry +	File O	Search Inline *	 File File File File File Certi Copy Inform 	Properties ficate Prope y to Clipboar ation	rties 🗁 rd 🔹	RegEdit F-MOD mp To	View Log File Notes		
Startup List			Entry Nan	ne	Analysis	User	Arch	Signed	Company	Name	Descript	ion	File Pat	:h 📩
Standard Views			谢 System	\Current	ControlSe	t\Control	Sessio	n Manage	er\KnownDL	.Ls				
System Startup System Startup System Startup System Startup System Startup System	on rs		Image: Constraint of the constr	atq 2 api32 4DLG32 2 UTIL GEHLP 32 wel32		All Users All Users All Users All Users All Users All Users All Users All Users All Users	x64 x64 x64 x64 x64 x64 x64 x64 x64 x64		Microsoft (Microsoft (Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation Corporation	COM+ Co Microsoft Advancec Common GDI Clien Run time Windows Multi-Use Windows Language	onfiguration Cai t OLE for Windo I Windows 32 B Dialogs DLL t DLL utility for Interr NT Image Help er Windows IM NT BASE API Cl e Pack	t C:\Winc C:\Winc	low low low low low low low
n bepar views			Properties	for "kerr	nel32"									•
Pescription	itains ion es here ied		 Entry Key Pal Value N Entry User Entry N Comma 	Location th lame Propertie ame nd p Entry	HKLM\S kemel32 es All Users kemel32 kemel32	iystem \Cor ! ! !.dll operties	ntrol Set ()	101\Contro	ol\Session Ma	anager\Know	mDLLs			
©2004-2010 Geek Squ	uad. For	r Inter	nal Use Or	nly. 🕴 To	otal: 258	Visible:	258 H	lidden: 0				Re	ecognized (os "ii

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 Sta	rtup Manager			_ = ×
Home Inspect	Tools Options	Resources					()
Startup List Boot Profiler App Mode	do Filters Actions	Entry ntry ntry + File	Search Online *	 File Properties Certificate Properti Copy to Clipboard Information 	es Composition for the second	View Log File Notes	
Startup List	Entry Name Ana	lysis Arch	Signed	Company Name	Description		File Path
Standard Views ^ ⊕ ☐ System Startup ⊕ ⊕ ⊕	✓ 🚳 HTTP Print 🧍 ✓ 🚳 LanMan Pr	7 x64 7 x64		Microsoft Corporation Microsoft Corporation	Internet Print Provi Client Side Render	der DLL ing Print P	C:\Windows\System: . C:\Windows\System:
🗏 🕎 Advanced	System\CurrentCont	rolSet\Contr	ol\Print\E	Environments\Windows	x64\Drivers\Versio	on-3	
File Execution	Adobe PD	x64		Microsoft Corporation	PostScript Printer D	Driver	C:\Windows\System:
🖗 Filter Drivers	M 🕲 Brother HL	х64		Microsoft Corporation	Unidrv Printer Driv	er	C:\Windows\System:
Network	M 🔊 hp deskjet	x64		Microsoft Corporation	Unidry Printer Driv	er	C:\Windows\System:
Print	M 🔊 HP Officej	х64		Microsoft Corporation	Unidry Printer Driv	er	C:\Windows\System:
🔒 Security	M NP Photos	x64		Microsoft Corporation	Unidry Printer Driv	er	C:\Windows\System:
🚳 System	Microsoft	x64		Microsoft Corporation	Microsoft Fax Prin	ter Driver	C:\Windows\System:
	A 1001 K #		3,0003	III	Minister Voc. D		Parada di Lindo Parada di F
In-Depth Views *	Properties for "HP Photo	smart Plus B	209a-m"				-
Description *	Entry Location						
Print	Key Path	HKLM\Syste	em\Control	Set001\Control\Print\Env	rironments\Windows	x64\Drivers	Version-3\HP Photosm
Print Providers work with	Entry Properties						
Windows to ensure things	User	All Users					
go smoothly, be it printing	Entry Name	HP Photosm	art Plus Bi	209a-m			
or to a unique file format.	Command	UNIDRV.DL	L				
· · · · · · · · · · · · · · · · · · ·							
	👹 Startup Entry 🕕 Fi	ile Properties	Cer	tificate			
©2004-2010 Geek Squad. For Inte	ernal Use Only. 🕴 Total: 2	2 Visible	e: 22 H	lidden: 0			🔹 Recognized OS 🖽

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.

🖅 📖 📸 🛒 🔹 🛛		М	IRI Startup Mana	ger		_ = x
Home Inspect	Tools Option	s Resources				(
Startup List Boot Profiler App Mode	lo Filters Actions	able Entry ete Entry ete Entry + File	Search Search Online + 🔁 Copy	Properties i 🎲 ficate Properties 📴 y to Clipboard 👻 ation Jun	RegEdit F-MOD View Log File mp To Notes	
Startup List	Entry Name	Analysis User	Arch Signed	Company Name	Description	File Path 🔺
Standard Views *	💐 Critical Startup F	iles		•	•	
	 ntoskrni.exe ntdil.dil smss.exe csrss.exe winlogon Isass.exe services.exe svchost.exe wininit.exe winioad.exe 	All Users All Users	x64 (************************************	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	 NT Kernel & System NT Layer DLL Windows Session Manager Client Server Runtime Pro Windows Logon Applicat Local Security Authority P Services and Controller a Host Process for Window Windows Start-Up Applic OS Loader 	C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window C:\Window
all of the entries from each Standard View into a single location that can be filtered and searched. Columns specific to individual views are not available here.	Properties for "serv Entry Location File Path Entry Propertie User Entry Name Command Startup Entry Trapil Lice Only	C:\Windows\Syste C:\Windows\Syste S All Users services.exe C:\Windows\Syste File Properties	m32\services.exe m32\services.exe Certificate		Par	

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.

🖅 📖 📂 🔛 🔻 I		MRI Star	tup Manag	ger			_ = ×	
Home Inspect	Tools Option	s Resources						()
Startup List Boot Profiler App Mode	Io Filters Actions	able Entry ete Entry ete Entry + File	Search Online *	 File P Certif Copy Information 	Properties ficate Properties to Clipboard ~ ation	RegE آهن اکن F-MC Jump To	dit Uiew Log File Notes	
Startup List	Entry Name	Analysis Use	Arch	Signed	Class Name		Company Name	Description ^
Standard Views ^ ⊕ ⊕ System Startup ⊕ ⊕ ⊕ Extensions ⊕ ↓ ∰ Advanced	✓ ⊗ (00020000) ✓ ⊗ (00020001) ✓ ⊗ (000200003) ✓ ⊗ (00020000) ✓ ⊗ (00020000) ✓ ⊗ (00020000)	All Us All All Us	ers x64 ers x64 ers x64 ers x64 ers x64 ers x64		Microsoft AVI Files AVI Compressed St Microsoft Wave Fil IAVIStream & IAVIF ACM Compressed	tream l le l file Pr l Audio l	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	Microsoft A Microsoft A Microsoft A Microsoft A Microsoft A
In-Depth Views ^ Everything Brute Force {CLSID}	✓ ⊗ (00020420) ✓ ⊗ (00020421) ✓ ⊗ (00020422) ✓ ⊗ (00020422)	All Use All Use All Use All Use All Use All Use	ers x64 ers x64 ers x64 ers x64		PSDispatch PSEnumVariant PSTypeInfo PSTypeLib		Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
Description *	✓ [™] {00020424 ✓ [™] {00020425	All Us	ers x64		PSOAInterface		Microsoft Corporation	
Brute Force (CLSID) Human readable names are	[00020425 [00021400 [00021 [00021 [0002 [0002 [0002 [0002 [0002 [0002 [0002 [0002 [0002 [0002 [0002 [000 [00 [00 [00 [00 [00	All Us	ers x04		Deckton		Microsoft Corporation	Mindour Ch
avoid this, Windows uses unique CLSIDs to represent shared components. These CLSIDs (Class IDs) can be	Properties for "(000) Entry Location Key Path	20000-0000-0000 HKLM\Software	-C000-000	000000046 CLSID\{000	5)" 020000-0000-0000-C	:000-0000	00000046}	×
referenced by any program to use the component; BHOs and Shell Extensions are registered via CLSIDs.	Entry Propertie	s All Users {00020000-0000-0000-0000-00000000046}						=
Brute Force {CLSID} pulls all registered CLSIDs and displays their dlls.	Class Name	Microsoft AVI Fil	es					Ŧ
©2004-2010 Geek Squad. For Inte	ernal Use Only.	tal: 5355 Visibl	e: 5355 H	lidden: 0			Rec	ognized OS 🚟

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.

Tools Options Resources Image: Solution of the properties of			1RI Startı	up Mana				
Image: Software \Microsoft \Windows \ All Users x64 Sun Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Sun Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Sun Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Sun Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Sun Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Microsoft Corp Disable Entry Image: Software \Microsoft \Windows \ All Users x64 Microsoft Corp Disable Entry Image: Sidebar Alex x64 Microsoft Corp Disable Entry Delete Entry and Image File	Tools Option	is Resources						
Entry Name Analysis User Arch Signed Company Name Description I Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\Run SunJavaUp All Users x64 Sun Microsoft Corp SysTrayApp All Users x64 Saftware Microsoft Corp Stolebar Allex x64 Saftware Microsoft Corp Saftware Microsoft Microsoft Corp Saftware Microsoft Microsoft Corp Saftware Microsoft Microsoft Corp Saftware Microsoft Microsoft Microsoft Corp Saftware Microsoft Mi	Filters Actions	able Entry ete Entry ete Entry + File C	Search Dnline *	 File F Certine Copy Inform 	Properties ficate Properties r to Clipboard ~ ation	ju	RegEdit F-MOD View Log File Notes	
	Entry Name	Analysis User	Arch	Signed	Company Nam	ne	Description	Fil
SunJavaUp All Users x64 Sun Microsystem Inc. Windows All Users x64 Microsoft Corp Disable Entry SysTrayApp All Users x64 Microsoft Corp Disable Entry SysTrayApp All Users x64 Microsoft Corp Disable Entry SysTrayApp All Users x64 Microsoft Corp Delete Entry Sidebar Alex x86 Google Inc Microsoft Corp	💣 Software\Micro	soft\Windows\Cur	rentVers	ion\Run				
Windows All Users x64 Microsoft Corp Disable Entry J SysTrayApp All Users x64 IDT, Inc. IDT, Inc. Inc. C Swg Alex x86 Google Inc Inc. Inc. Inc. Sidebar Alex x64 Microsoft Corp Inc. Inc. Inc. Inc. Image: Sidebar Alex x64 Microsoft Corp Inc. Inc. Inc. Inc.	🗹 🛃 SunJavaUp	All Users	s x64		Sun Microsyster	ns Ind	- Iava/TMI Diatform S	Ebinany Ci
Image: SysTrayApp All Users x64 Image: DT, Inc. Image: Dt, Inc. Image: Dt, Inc. Image: SysTrayApp Alex x86 Image: Dt, Inc. Image: Dt, Inc. Image: Dt, Inc. Image: SysTrayApp Alex x86 Image: Dt, Inc. Image: Dt, Inc. Image: Dt, Inc. Image: SysTrayApp Alex x86 Image: Dt, Inc. Image: Dt, Inc. Image: Dt, Inc. Image: SysTrayApp Alex x86 Image: Dt, Inc. Image: Dt, Inc. Image: Dt, Inc.	🗹 🥹 Windows	All Users	s x64		Microsoft Corp		Disable Entry	
Image: Sidebar Alex x86 Image: Sidebar Delete Entry and Image File Image: Sidebar Alex x64 Image: Sidebar Delete Entry and Image File	SysTrayApp 🖉	All Users	s x64		IDT, Inc.	×	Delete Entry	
Sidebar Alex x64 🦾 Microsoft Corp	∠ © swg	Alex	x86		Google Inc	\mathbf{X}	Delete Entry and Ima	ge File
	🗹 📑 Sidebar	Alex	х64		Microsoft Corp		File Deen entire	
Google Up Alex x86 🗰 Google Inc 🖤 File Properties	🗹 🚺 Google Up	Alex	x86		Google Inc	U	File Properties	
☐ ☐ OfficeSync Alex x86 🖾 Microsoft Corp 🖾 Certificate Properties	에너 OfficeSync	Alex	x86		Microsoft Corp		Certificate Properties	
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run	💣 Software\Wow	6432Node\Microso	ft\Windo	ows\Cum	entVersion\Run	*	Include	•
Adaba ADM All Heave v26 🖾 Adaba Curtame 🍸 EXCLUDE	VIN Adaba ADM	All Llear		1949	Adoba Sustame	T	Exclude	
Properties for "SunJavaUpdateSched"	Properties for "Sun	JavaUpdateSched"					Copy to Clipboard	×
Entry Location y Jump to	Entry Location					\$	Jump to	۱.
Key Path HKLM\Software\Microsoft\Windows\CurrentVersion\F 🕥 Search Online	-					-		

MRI Startup Manager – Delete/Disable example

	MRI Startup Manage	r	-
Tools Options Res	ources		
Filters	Image: Search Online ▼ Image: Search Online ▼	erties 💣 Re te Properties 🧁 F-1 Clipboard 👻	gEdit MOD View Log File
Actions	Informatio	n Jump	Io Notes
Boot Profile data is availa	able for C:\WINDOWS		Opt
🛕 6 cautionary warnings in	the current view.		Show Wa
Entry Name	Analysis User	Signed Company N	ame Description
Software\Microsoft\W	/indows NT\CurrentVersio	n\Winlogon> "Us	erinit"
🐴 🛄 C: \WINDOWS\system3	All Users	-	Reset Entry
C:\WINDOWS\system3	All Users	Micro	Delete Entry
Hisbing volder er (varv.			Delete Entry and Image File
💣 Software\Microsoft\W	/indows NT\CurrentVersio	n\Winlogon	
🗸 😼 Explorer.exe	🦓 🛛 All Users	📑 Micro 🛈 🛙	File Properties
de a lur alla			Certificate Properties
Software (Microsoft (M	Indows (CurrentVersion (F	cun 👘	Include
Proportion for "CullWINDOWS	laustam 22 lucin la gan 22 ava		Exclude
For the location	systemszywiniogonsztexe		
Key Path HK	LM\RemoteOS-HKLM-Softwar	e\Microsoft\Win	Copy to Clipboard
Value Name Use	erinit	>	Jump to 🕨
Entry Properties		🥥 :	Search Online
A11			

MRI Startup Manager – Reset example

© 2010 Geek Squad

25 of 27

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.

- 12 🔍 🎽 🔛 🤻				MRI Start	up Manag	ger			_ =	x
Home	Inspect	Tools Options	Resources							1
 Startup List Boot Profiler App Mode 	Refresh Undo	Filters Actions	e Entry Entry Entry + File	Search Online *	 File P Certif Copy Information 	Properties ficate Properties to Clipboard 👻 ation	📸 RegEdit 🇁 F-MOD Jump To	View Log File Notes		
Startup List		Undo Manager (Ctrl	+Z)	Arch	Signed	Company Name	e Descrip	tion	File Pat	th 📩
Standard Views	-	Opens the Undo Manager and allows for modifications to		Current	/ersion\W	/inlogon> "Use	erinit"			=
🖃 🖅 System Start 🍂 Critical Fi 🎡 Drivers	up iles	startup entries to be The Undo Manager o reverse registry chan deletions.	p entries to be undone. ndo Manager can only e registry changes, not file ions.		/ersion\W	Microsoft Corpo	ration Userinit	Logon Applic	ation Ci\Wind	iow

MRI Startup Manager – Launching Undo Manager

			Acti	ons Available for Undo		x
[Action	Timestamp 🗸	Entry Name	Command	Entry Location	
	Deleted	5/23/2010 7:54 PM	Persistence	C:\Windows\system32\igfxpers.exe	Software\Microsoft\Windows\\Run	
	Reset Disabled	5/23/2010 7:53 PM 5/23/2010 7:53 PM	Adobe Reader S	"C:\Program Files\Ad\Reader_sl.exe"	Software\Microsoft\Windows\\Run	
	Disabled Disabled	5/23/2010 7:53 PM 5/23/2010 7:53 PM	IgfxTray NvCpIDaemon	C:\Windows\system32\igfxtray.exe RUNDLL32.EXE\NvCpl.dll,NvStartup	Software\Microsoft\Windows\Run Software\Microsoft\Windows\Run	
					Perform Undo Close	

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 <u>MRI@geeksquad.com</u>. If you have any technical training questions, feel free to reach out to <u>InternalAffairs@geeksquad.com</u>. 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.



