

# Troubleshooting with the Windows Sysinternals Tools

Guidance  
from the  
tools'  
creator



MARK RUSSINOVICH | AARON MARGOSIS

# Troubleshooting with the Windows Sysinternals Tools

Mark Russinovich  
Aaron Margosis

# Troubleshooting with the Windows Sysinternals Tools

## Table of Contents

Cover

Title Page

Copyright Page

Acknowledgments

Table of Contents

Foreword

Introduction

## PART I: GETTING STARTED

### Chapter 1 Getting started with the Sysinternals utilities

Overview of the utilities

The Windows Sysinternals website

Downloading the utilities

Running the utilities directly from the web

Single executable image

The Windows Sysinternals forums

Windows Sysinternals site blog

Marks blog

Marks webcasts

Sysinternals license information

End User License Agreement and the /accepteula switch

Frequently asked questions about Sysinternals licensing

### Chapter 2 Windows core concepts

Administrative rights

# Table of Contents

Processes, threads, and jobs

User mode and kernel mode

Handles

Application isolation

- App Containers

- Protected processes

Call stacks and symbols

- What is a call stack?

- What are symbols?

- Configuring symbols

Sessions, window stations, desktops, and window messages

- Remote desktop services sessions

- Window stations

- Desktops

- Window messages

## Chapter 3 Process Explorer

Procexp overview

- Measuring CPU consumption

- Administrative rights

Main window

- Process list

- Customizing column selections

- Saving displayed data

- Toolbar reference

- Identifying the process that owns a window

- Status bar

DLLs and handles

- Finding DLLs or handles

- DLL view

- Handle view

Process details

# **Table of Contents**

Image tab

Performance tab

Performance Graph tab

GPU Graph tab

Threads tab

TCP/IP tab

Security tab

Environment tab

Strings tab

Services tab

.NET tabs

Job tab

Thread details

Verifying image signatures

VirusTotal analysis

System information

CPU tab

Memory tab

I/O tab

GPU tab

Display options

Procexp as a Task Manager replacement

Creating processes from Procexp

Other user sessions

Miscellaneous features

Shutdown options

Command-line switches

Restoring Procexp defaults

Keyboard shortcut reference

## **Chapter 4 Autoruns**

Autoruns fundamentals

# **Table of Contents**

- Disabling or deleting autostart entries
- Autoruns and administrative permissions
- Verifying code signatures
- VirusTotal analysis
- Hiding entries
- Getting more information about an entry
- Viewing the autostarts of other users
- Viewing ASEPs of an offline system
- Changing the font

## **Autostart categories**

- Logon
- Explorer
- Internet Explorer
- Scheduled Tasks
- Services
- Drivers
- Codecs
- Boot Execute
- Image hijacks
- AppInit
- KnownDLLs
- Winlogon
- Winsock providers
- Print monitors
- LSA providers
- Network providers
- WMI
- Sidebar gadgets
- Office

## **Saving and comparing results**

- Saving as tab-delimited text
- Saving in binary (.arn) format
- Viewing and comparing saved results

# Table of Contents

AutorunsC

Autoruns and malware

## PART II: USAGE GUIDE

### Chapter 5 Process Monitor

Getting started with Procmon

#### Events

Understanding the column display defaults

Customizing the column display

Event Properties dialog box

Displaying profiling events

Finding an event

Copying event data

Jumping to a registry or file location

Searching online

#### Filtering, highlighting, and bookmarking

Configuring filters

Configuring highlighting

Bookmarking

Advanced output

Saving filters for later use

#### Process Tree

#### Saving and opening Procmon traces

Saving Procmon traces

Procmon XML schema

Opening saved Procmon traces

#### Logging boot, post-logoff, and shutdown activity

Boot logging

Keeping Procmon running after logoff

#### Long-running traces and controlling log sizes

Drop filtered events

History depth

# Table of Contents

Backing files

Importing and exporting configuration settings

Automating Procmon: command-line options

Analysis tools

Process Activity Summary

File Summary

Registry Summary

Stack Summary

Network Summary

Cross Reference Summary

Count Occurrences

Injecting custom debug output into Procmon traces

Toolbar reference

## Chapter 6 ProcDump

Command-line syntax

Specifying which process to monitor

Attach to existing process

Launch the target process

Working with Universal Windows Platform applications

Auto-enabled debugging with AeDebug registration

Specifying the dump file path

Specifying criteria for a dump

Monitoring exceptions

Dump file options

Miniplus dumps

ProcDump and Procmon: Better together

Running ProcDump noninteractively

Viewing the dump in the debugger

## Chapter 7 PsTools

Common features



# Table of Contents

Remote operations

Troubleshooting remote PsTools connections

## PsExec

Remote process exit

Redirected console output

PsExec alternate credentials

PsExec command-line options

Process performance options

Remote connectivity options

Runtime environment options

## PsFile

## PsGetSid

## PsInfo

## PsKill

## PsList

## PsLoggedOn

## PsLogList

## PsPasswd

## PsService

Query

Config

Depend

Security

Find

SetConfig

Start, Stop, Restart, Pause, Continue

## PsShutdown

## PsSuspend

## PsTools command-line syntax

PsExec

PsFile

# Table of Contents

PsGetSid

PsInfo

PsKill

PsList

PsLoggedOn

PsLogList

PsPasswd

PsService

PsShutdown

PsSuspend

PsTools system requirements

## Chapter 8 Process and diagnostic utilities

### VMMMap

Starting VMMMap and choosing a process

The VMMMap window

Memory types

Memory information

Timeline and snapshots

Viewing text within memory regions

Finding and copying text

Viewing allocations from instrumented processes

Address space fragmentation

Saving and loading snapshot results

VMMMap command-line options

Restoring VMMMap defaults

### DebugView

What is debug output?

The DebugView display

Capturing user-mode debug output

Capturing kernel-mode debug output

Searching, filtering, and highlighting output

Saving, logging, and printing

# Table of Contents

Remote monitoring

## LiveKd

LiveKd requirements

Running LiveKd

Kernel debugger target types

Output to debugger or dump file

Dump contents

Hyper-V guest debugging

Symbols

LiveKd examples

## ListDLLs

## Handle

Handle list and search

Handle counts

Closing handles

## Chapter 9 Security utilities

### SigCheck

Which files to scan

Signature verification

VirusTotal analysis

Additional file information

Output format

Miscellaneous

### AccessChk

What are effective permissions?

Using AccessChk

Object type

Searching for access rights

Output options

### Sysmon

Events recorded by Sysmon

Installing and configuring Sysmon

# Table of Contents

Extracting Sysmon event data

AccessEnum

ShareEnum

ShellRunAs

Autologon

LogonSessions

SDelete

Using SDelete

How SDelete works

## Chapter 10 Active Directory utilities

AdExplorer

Connecting to a domain

The AdExplorer display

Objects

Attributes

Searching

Snapshots

AdExplorer configuration

AdInsight

AdInsight data capture

Display options

Finding information of interest

Filtering results

Saving and exporting AdInsight data

Command-line options

AdRestore

## Chapter 11 Desktop utilities

BgInfo

Configuring data to display

Appearance options

Saving BgInfo configuration for later use

# Table of Contents

Other output options

Updating other desktops

## Desktops

## ZoomIt

Using ZoomIt

Zoom mode

Drawing mode

Typing mode

Break Timer

LiveZoom

## Chapter 12 File utilities

Strings

Streams

NTFS link utilities

Junction

FindLinks

Disk Usage (DU)

Post-reboot file operation utilities

PendMoves

MoveFile

## Chapter 13 Disk utilities

Disk2Vhd

Sync

DiskView

Contig

Defragmenting existing files

Analyzing fragmentation of existing files

Analyzing free-space fragmentation

Creating a contiguous file

DiskExt

LDMDump

# Table of Contents

VolumeID

## Chapter 14 Network and communication utilities

### PsPing

- ICMP Ping

- TCP Ping

- PsPing server mode

- TCP/UDP latency test

- TCP/UDP bandwidth test

- PsPing histograms

### TCPView

### Whois

## Chapter 15 System information utilities

### RAMMap

- Use Counts

- Processes

- Priority Summary

- Physical Pages

- Physical Ranges

- File Summary

- File Details

- Purging physical memory

- Saving and loading snapshots

### Registry Usage (RU)

### CoreInfo

- c: Dump information on cores

- f: Dump core feature information

- g: Dump information on groups

- l: Dump information on caches

- m: Dump NUMA access cost

- n: Dump information on NUMA nodes

- s: Dump information on sockets

- v: Dump only virtualization-related features

# Table of Contents

WinObj

LoadOrder

PipeList

ClockRes

## Chapter 16 Miscellaneous utilities

RegJump

Hex2Dec

RegDelNull

Bluescreen Screen Saver

Ctrl2Cap

## PART III: TROUBLESHOOTING THE CASE OF THE UNEXPLAINED

### Chapter 17 Error messages

Troubleshooting error messages

The Case of the Locked Folder

The Case of the File In Use Error

The Case of the Unknown Photo Viewer Error

The Case of the Failing ActiveX Registration

The Case of the Failed Play-To

The Case of the Installation Failure

    The troubleshooting

    The analysis

The Case of the Unreadable Text Files

The Case of the Missing Folder Association

The Case of the Temporary Registry Profiles

The Case of the Office RMS Error

The Case of the Failed Forest Functional Level Raise

### Chapter 18 Crashes

# **Table of Contents**

Troubleshooting crashes

The Case of the Failed AV Update

The Case of the Crashing Proksi Utility

The Case of the Failed Network Location Awareness Service

The Case of the Failed EMET Upgrade

The Case of the Missing Crash Dump

The Case of the Random Sluggishness

## **Chapter 19 Hangs and sluggish performance**

Troubleshooting hangs and sluggish performance

The Case of the IExplore-Pegged CPU

The Case of the Runaway Website

The Case of the Excessive ReadyBoost

The Case of the Stuttering Laptop Blu-ray Player

The Case of the Company 15-Minute Logons

The Case of the Hanging PayPal Emails

The Case of the Hanging Accounting Software

The Case of the Slow Keynote Demo

The Case of the Slow Project File Opens

The Compound Case of the Outlook Hangs

## **Chapter 20 Malware**

Troubleshooting malware

Stuxnet

Malware and the Sysinternals utilities

The Stuxnet infection vector

Stuxnet on Windows XP

Looking deeper

Filtering to find relevant events

Stuxnet system modifications

The .PNF files

Windows 7 elevation of privilege



# **Table of Contents**

Stuxnet revealed by the Sysinternals utilities

The Case of the Strange Reboots

The Case of the Fake Java Updater

The Case of the Winwebsec Scareware

The Case of the Runaway GPU

The Case of the Unexplained FTP Connections

The Case of the Misconfigured Service

The Case of the Sysinternals-Blocking Malware

The Case of the Process-Killing Malware

The Case of the Fake System Component

The Case of the Mysterious ASEP

## **Chapter 21 Understanding system behavior**

The Case of the Q: Drive

The Case of the Unexplained Network Connections

The Case of the Short-Lived Processes

The Case of the App Install Recorder

The Case of the Unknown NTLM Communications

## **Chapter 22 Developer troubleshooting**

The Case of the Broken Kerberos Delegation

The Case of the ProcDump Memory Leak

**Index**

**About the Authors**

**Survey**