

Declaration of Rachel J. Watters on Authentication of Publication

I, Rachel J. Watters, am a librarian, and the Head of Resource Sharing for the General Library System, Memorial Library, located at 728 State Street, Madison, Wisconsin, 53706. Part of my job responsibilities include oversight of Wisconsin TechSearch (“WTS”), an interlibrary loan department at the University of Wisconsin-Madison. I have worked as a librarian at the University of Wisconsin library system since 1998, starting as a graduate student employee in the Kurt F. Wendt Engineering Library and WTS, then as a librarian in Interlibrary Loan at Memorial Library. I began professional employment at WTS in 2002 and became WTS Director in 2011. In 2019, I became of Head of Resource Sharing for UW-Madison’s General Library System. I have a master’s degree in Library and Information Studies from the University of Wisconsin-Madison. Through the course of my studies and employment, I have become well informed about the operations of the University of Wisconsin library system, which follows standard library practices.

This Declaration relates to the dates of receipt and availability of the following:

Nazario, J. (2004). *Defense and Detection Strategies Against Internet Worms*. Artech House.

Standard operating procedures for materials at the University of Wisconsin-Madison Libraries. When a volume was received by the Library, it would be checked in, added to library holdings records, and made available to readers as soon after its arrival as possible. The procedure normally took a few days or at most 2 to 3 weeks.

Declaration of Rachel J. Watters on Authentication of Publication

Exhibit A to this Declaration is a true and accurate copy of the front matter and back matter of the *Defense and Detection Strategies Against Internet Worms* (2004) publication, which includes a stamp on the verso page showing that this book is the property of the General Library System of the University of Wisconsin-Madison.

Attached as Exhibit B is the cataloging system record of the University of Wisconsin-Madison Libraries for its copy of the *Defense and Detection Strategies Against Internet Worms* (2004) publication. As shown in the "Receiving date" field of this Exhibit, the University of Wisconsin-Madison Libraries owned this volume and had it cataloged in the system as of January 14, 2004.

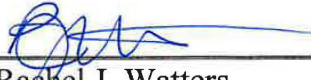
Members of the interested public could locate the *Defense and Detection Strategies Against Internet Worms* (2004) publication after it was cataloged by searching the public library catalog or requesting a search through WTS. The search could be done by title, author, and/or subject key words. Members of the interested public could access the publication by locating it on the library's shelves or requesting it from WTS.

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Declaration of Rachel J. Watters on Authentication of Publication

Date: February 13, 2025

Memorial Library
728 State Street
Madison, Wisconsin 53706



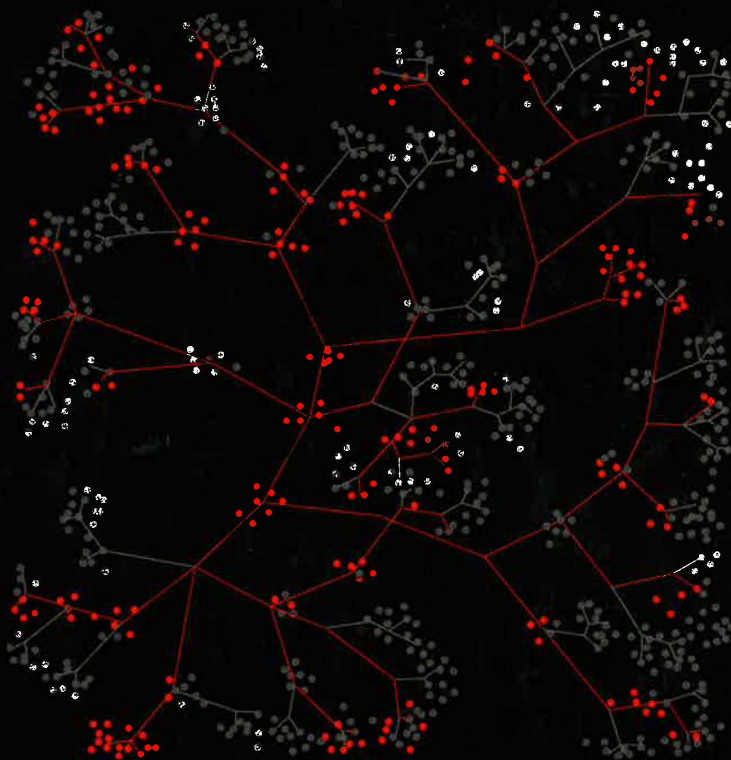
Rachel J. Watters
Head of Resource Sharing

EXHIBIT A



ARTECH HOUSE
COMPUTER SECURITY SERIES

*Defense and Detection
Strategies against*
Internet Worms



JOSE NAZARIO

COMPUTER SECURITY

89083321273



b89083321273a

This is the first book focused exclusively on Internet worm detection and mitigation strategies to help professionals with their challenging work in the field. This groundbreaking volume enables practitioners to tackle the ever-increasing presence of Internet worms with practical detection knowledge and defense techniques utilizing data from live networks, real IP addresses, and commercial tools. The book discusses the classifications and groupings of worms, and offers a deeper understanding of how they threaten network and system security.

After examining how a worm is constructed and how its major life-cycle steps are implemented, the book scrutinizes targets that worms have attacked over the years, and the likely targets of the immediate future. Covering both commercial and open-source tools, this unique reference explains how to detect worms using a variety of mechanisms, and evaluates the strengths and weaknesses of three approaches—traffic analysis, honeypots and dark network monitors, and signature analysis. The book concludes with a discussion of four effective defenses against network worms, including host-based defenses, network firewalls and filters, application layer proxies, and a direct attack on the worm network itself.

Jose Nazario is a senior software engineer at Arbor Networks, an Internet security company. He is also a consultant and researcher at Crimelabs Research, a think tank and consulting firm. He holds a Ph.D. in biochemistry from Case Western Reserve University. He has published extensively.

ISBN 1-56053-537-2



9 781580 535373

90000

Artech House Publishers BOSTON • LONDON
www.artechhouse.com

ARTECH
HOUSECOMPUTER
SECURITY
SERIESDefense and Detection
Strategies against

Internet Worms

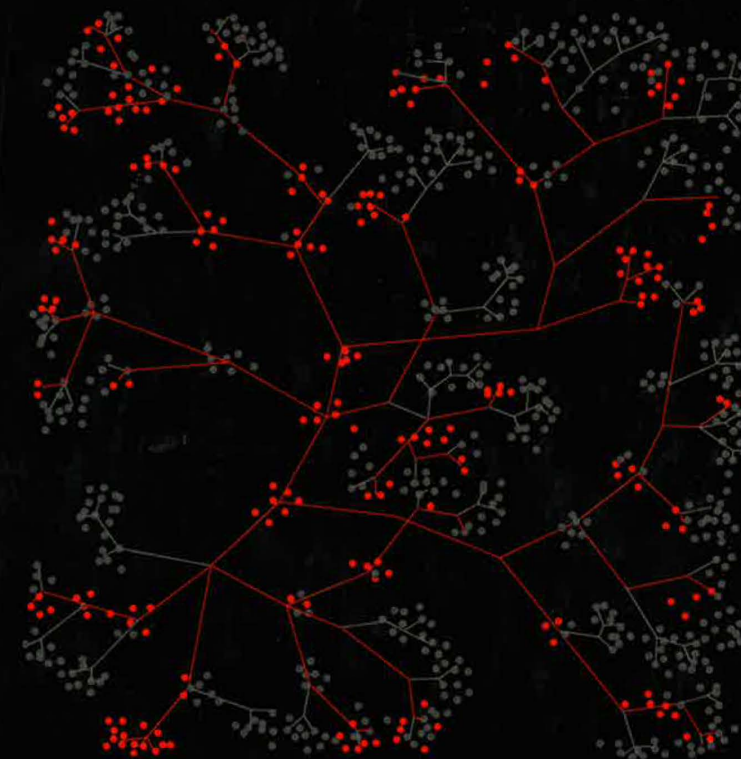
NAZARIO

QA
76.9
A25
N38
2004

WENDT

ARTECH HOUSE
COMPUTER SECURITY SERIES

Defense and Detection Strategies against Internet Worms



JOSE NAZARIO

General Library System
University of Wisconsin - Madison
728 State Street
Madison, WI 53706-1494
U.S.A.

Defense and Detection Strategies against Internet Worms

For quite a long time, computer security was a rather narrow field of study that was populated mainly by theoretical computer scientists, electrical engineers, and applied mathematicians. With the proliferation of open systems in general, and of the Internet and the World Wide Web (WWW) in particular, this situation has changed fundamentally. Today, computer and network practitioners are equally interested in computer security, since they require technologies and solutions that can be used to secure applications related to electronic commerce. Against this background, the field of computer security has become very broad and includes many topics of interest. The aim of this series is to publish state-of-the-art, high standard technical books on topics related to computer security. Further information about the series can be found on the WWW at the following URL:

<http://www.esecurity.ch/serieseditor.html>

Also, if you'd like to contribute to the series by writing a book about a topic related to computer security, feel free to contact either the Commissioning Editor or the Series Editor at Artech House.

For a listing of recent titles in the *Artech House Computer Security Series*, turn to the back of this book.

Defense and Detection Strategies against Internet Worms

Jose Nazario



Artech House
Boston • London
www.artechhouse.com

Library of Congress Cataloging-in-Publication Data

A catalog record of this book is available from the U.S. Library of Congress.

British Library Cataloguing in Publication Data

Nazario, Jose

Defense and detection strategies against Internet worms. —

(Artech House computer security library)

1. Computer viruses 2. Computer networks — Security measures 3. Internet — Security measures

I. Title

005.8'4

ISBN 1-58053-537-2

Cover design by Yekaterina Ratner

© 2004 ARTECH HOUSE, INC.

685 Canton Street

Norwood, MA 02062

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-357-2

A Library of Congress Catalog Card Number is available from the Library of Congress.

10 9 8 7 6 5 4 3 2 1

General Library System
University of Wisconsin - Madison
723 State Street
Madison, WI 53706-1494
U.S.A.

Wmott

QA
76.9
A25
N38
2004

6171705

To Beth, Maus, and Miso

Contents

Foreword xvii

Preface xxi

Acknowledgments xxvii

1 Introduction 1

1.1 Why worm-based intrusions? 2

1.2 The new threat model 3

1.3 A new kind of analysis requirement 4

1.4 The persistent costs of worms 5

1.5 Intentions of worm creators 6

1.6 Cycles of worm releases 7

References 8

Part I Background and Taxonomy 9

2 Worms Defined 11

2.1 A formal definition 12

2.2 The five components of a worm 12

2.3 Finding new victims: reconnaissance 14

2.4 Taking control: attack 15

2.5 Passing messages: communication 15

2.6 Taking orders: command interface 16

vii

2.7	Knowing the network: intelligence	17
2.8	Assembly of the pieces	18
2.9	Ramen worm analysis	19
2.10	Conclusions	21
	References	21

3 Worm Traffic Patterns 23

3.1	Predicted traffic patterns	23
3.1.1	Growth patterns	23
3.1.2	Traffic scan and attack patterns	25
3.2	Disruption in Internet backbone activities	26
3.2.1	Routing data	26
3.2.2	Multicast backbone	27
3.2.3	Infrastructure servers	28
3.3	Observed traffic patterns	28
3.3.1	From a large network	28
3.3.2	From a black hole monitor	30
3.3.3	From an individual host	31
3.4	Conclusions	34
	References	34

4 Worm History and Taxonomy. 37

4.1	The beginning	38
4.1.1	Morris worm, 1988	39
4.1.2	HI.COM VMS worm, 1988	41
4.1.3	DECNet WANK worm, 1989	42
4.1.4	Hacking kits	43
4.2	UNIX targets	44
4.2.1	ADMwOrm-v1, 1998	44
4.2.2	ADM Millennium worm, 1999	45
4.2.3	Ramen, 2000	46
4.2.4	liOn worm, 2001	47
4.2.5	Cheese worm, 2001	48
4.2.6	sadmind/IIS worm, 2001	48
4.2.7	X.c: Telnetd worm, 2001	49
4.2.8	Adore, 2001	49

4.2.9	<i>Apache worms, 2002</i>	50
4.2.10	<i>Variations on Apache worms</i>	51
4.3	Microsoft Windows and IIS targets	53
4.3.1	<i>mIRC Script.ini worm, 1997</i>	53
4.3.2	<i>Melissa, 1999</i>	54
4.3.3	<i>Love Letter worm, 2001</i>	54
4.3.4	<i>911 worm, 2001</i>	55
4.3.5	<i>Leaves worm, 2001</i>	56
4.3.6	<i>Code Red, 2001</i>	56
4.3.7	<i>Code Red II, 2001</i>	58
4.3.8	<i>Nimda, 2001</i>	59
4.3.9	<i>Additional e-mail worms</i>	60
4.3.10	<i>MSN Messenger worm, 2002</i>	60
4.3.11	<i>SQL Snake, 2002</i>	61
4.3.12	<i>Deloder, 2002–2003</i>	62
4.3.13	<i>Sapphire, 2003</i>	62
4.4	Related research	63
4.4.1	<i>Agent systems</i>	64
4.4.2	<i>Web spiders</i>	64
4.5	Conclusions	65
	References	65

5**Construction of a Worm 69**

5.1	Target selection	69
5.1.1	<i>Target platform</i>	70
5.1.2	<i>Vulnerability selection</i>	71
5.2	Choice of languages	72
5.2.1	<i>Interpreted versus compiled languages</i>	72
5.3	Scanning techniques	74
5.4	Payload delivery mechanism	75
5.5	Installation on the target host	76
5.6	Establishing the worm network	77
5.7	Additional considerations	78
5.8	Alternative designs	78
5.9	Conclusions	80
	References	80

Part II	Worm Trends	81
6	Infection Patterns	83
6.1	Scanning and attack patterns	83
6.1.1	<i>Random scanning</i>	83
6.1.2	<i>Random scanning using lists</i>	85
6.1.3	<i>Island hopping</i>	86
6.1.4	<i>Directed attacking</i>	87
6.1.5	<i>Hit-list scanning</i>	88
6.2	Introduction mechanisms	89
6.2.1	<i>Single point</i>	89
6.2.2	<i>Multiple point</i>	90
6.2.3	<i>Widespread introduction with a delayed trigger</i>	90
6.3	Worm network topologies	91
6.3.1	<i>Hierarchical tree</i>	91
6.3.2	<i>Centrally connected network</i>	93
6.3.3	<i>Shockwave Rider-type and guerilla networks</i>	94
6.3.4	<i>Hierarchical networks</i>	95
6.3.5	<i>Mesh networks</i>	96
6.4	Target vulnerabilities	97
6.4.1	<i>Prevalence of target</i>	97
6.4.2	<i>Homogeneous versus heterogeneous targets</i>	98
6.5	Payload propagation	99
6.5.1	<i>Direct injection</i>	99
6.5.2	<i>Child to parent request</i>	100
6.5.3	<i>Central source or sources</i>	101
6.6	Conclusions	102
	References	102
7	Targets of Attack	103
7.1	Servers	103
7.1.1	<i>UNIX servers</i>	104
7.1.2	<i>Windows servers</i>	104
7.2	Desktops and workstations	105
7.2.1	<i>Broadband users</i>	105
7.2.2	<i>Intranet systems</i>	107

7.2.3	<i>New client applications</i>	107
7.3	Embedded devices	108
7.3.1	<i>Routers and infrastructure equipment</i>	109
7.3.2	<i>Embedded devices</i>	109
7.4	Conclusions	110
	References	110

8 Possible Futures for Worms 113

8.1	Intelligent worms	113
8.1.1	<i>Attacks against the intelligent worm</i>	117
8.2	Modular and upgradable worms	118
8.2.1	<i>Attacks against modular worms</i>	121
8.3	Warhol and Flash worms	122
8.3.1	<i>Attacks against the Flash worm model</i>	125
8.4	Polymorphic traffic	126
8.5	Using Web crawlers as worms	127
8.6	Superworms and Curious Yellow	129
8.6.1	<i>Analysis of Curious Yellow</i>	130
8.7	Jumping executable worm	130
8.8	Conclusions	131
8.8.1	<i>Signs of the future</i>	132
8.8.2	<i>A call to action</i>	132
	References	132

Part III Detection. 135

9 Traffic Analysis. 137

9.1	Part overview	137
9.2	Introduction to traffic analysis	138
9.3	Traffic analysis setup	139
9.3.1	<i>The use of simulations</i>	141
9.4	Growth in traffic volume	142
9.4.1	<i>Exponential growth of server hits</i>	143
9.5	Rise in the number of scans and sweeps	143
9.5.1	<i>Exponential rise of unique sources</i>	145
9.5.2	<i>Correlation analysis</i>	147

9.5.3	<i>Detecting scans</i>	148
9.6	Change in traffic patterns for some hosts	148
9.7	Predicting scans by analyzing the scan engine	150
9.8	Discussion	156
9.8.1	<i>Strengths of traffic analysis</i>	156
9.8.2	<i>Weaknesses of traffic analysis</i>	156
9.9	Conclusions	158
9.10	Resources	158
9.10.1	<i>Packet capture tools</i>	158
9.10.2	<i>Flow analysis tools</i>	158
	References	159

10 Honeypots and Dark (Black Hole) Network Monitors 161

10.1	Honeypots	162
10.1.1	<i>Risks of using honeypots</i>	163
10.1.2	<i>The use of honeypots in worm analysis</i>	163
10.1.3	<i>An example honeypot deployment</i>	164
10.2	Black hole monitoring	164
10.2.1	<i>Setting up a network black hole</i>	166
10.2.2	<i>An example black hole monitor</i>	167
10.2.3	<i>Analyzing black hole data</i>	167
10.3	Discussion	170
10.3.1	<i>Strengths of honeypot monitoring</i>	170
10.3.2	<i>Weaknesses of honeypot monitoring</i>	171
10.3.3	<i>Strengths of black hole monitoring</i>	171
10.3.4	<i>Weaknesses of black hole monitoring</i>	172
10.4	Conclusions	172
10.5	Resources	173
10.5.1	<i>Honeypot resources</i>	173
10.5.2	<i>Black hole monitoring resources</i>	173
	References	173

11 Signature-Based Detection 175

11.1	Traditional paradigms in signature analysis	176
11.1.1	<i>Worm signatures</i>	177
11.2	Network signatures	177

11.2.1	<i>Distributed intrusion detection</i>	179
11.3	Log signatures	180
11.3.1	<i>Logfile processing</i>	181
11.3.2	<i>A more versatile script</i>	184
11.3.3	<i>A central log server</i>	188
11.4	File system signatures	190
11.4.1	<i>Chkrootkit</i>	190
11.4.2	<i>Antivirus products</i>	192
11.4.3	<i>Malicious payload content</i>	194
11.5	Analyzing the Slapper worm	195
11.6	Creating signatures for detection engines	198
11.6.1	<i>For NIDS use</i>	198
11.6.2	<i>For logfile analysis</i>	200
11.6.3	<i>For antivirus products and file monitors</i>	201
11.7	Analysis of signature-based detection	204
11.7.1	<i>Strengths of signature-based detection methods</i>	204
11.7.2	<i>Weaknesses in signature-based detection methods</i>	205
11.8	Conclusions	206
11.9	Resources	206
11.9.1	<i>Logfile analysis tools</i>	206
11.9.2	<i>Antivirus tools</i>	207
11.9.3	<i>Network intrusion detection tools</i>	207
	References	208

Part IV Defenses 209

12

Host-Based Defenses 211

12.1	Part overview	211
12.2	Host defense in depth	213
12.3	Host firewalls	213
12.4	Virus detection software	214
12.5	Partitioned privileges	216
12.6	Sandboxing of applications	219
12.7	Disabling unneeded services and features	221
12.7.1	<i>Identifying services</i>	221
12.7.2	<i>Features within a service</i>	223

12.8	Aggressively patching known holes	223
12.9	Behavior limits on hosts	225
12.10	Biologically inspired host defenses	227
12.11	Discussion	229
12.11.1	<i>Strengths of host-based defense strategies</i>	229
12.11.2	<i>Weaknesses of host-based defense strategies</i>	229
12.12	Conclusions	230
	References	230
13	Firewall and Network Defenses	233
13.1	Example rules	234
13.2	Perimeter firewalls	236
13.2.1	<i>Stopping existing worms</i>	237
13.2.2	<i>Preventing future worms</i>	238
13.2.3	<i>Inbound and outbound rules</i>	238
13.3	Subnet firewalls	239
13.3.1	<i>Defending against active worms</i>	239
13.4	Reactive IDS deployments	239
13.4.1	<i>Dynamically created rulesets</i>	240
13.5	Discussion	242
13.5.1	<i>Strengths of firewall defenses</i>	242
13.5.2	<i>Weaknesses of firewall systems</i>	242
13.6	Conclusions	242
	References	243
14	Proxy-Based Defenses	245
14.1	Example configuration	246
14.1.1	<i>Client configuration</i>	248
14.2	Authentication via the proxy server	249
14.3	Mail server proxies	249
14.4	Web-based proxies	251
14.5	Discussion	253
14.5.1	<i>Strengths of proxy-based defenses</i>	253
14.5.2	<i>Weaknesses of proxy-based defenses</i>	253
14.6	Conclusions	254

14.7 Resources	254
References	254

15 Attacking the Worm Network 257

15.1 Shutdown messages	259
15.2 "I am already infected"	260
15.3 Poison updates	261
15.4 Slowing down the spread	262
15.5 Legal implications of attacking worm nodes	263
15.6 A more professional and effective way to stop worms	264
15.7 Discussion	266
15.7.1 Strengths of attacking the worm network	266
15.7.2 Weaknesses of attacking the worm network	266
15.8 Conclusions	267
References	267

16 Conclusions 269

16.1 A current example	269
16.2 Reacting to worms	270
16.2.1 Detection	271
16.2.2 Defenses	272
16.3 Blind spots	273
16.4 The continuing threat	273
16.4.1 Existing worms	274
16.4.2 Future worms	274
16.5 Summary	275
16.6 On-line resources	275
16.6.1 RFC availability	275
16.6.2 Educational material	275
16.6.3 Common vendor resources	275
16.6.4 Vendor-neutral sites	276
References	277

About the Author	279
----------------------------	-----

Index	281
-----------------	-----

89083321273



B89083321273A

K.F. WENDT LIBRARY
UW COLLEGE OF ENGR.
215 N. RANDALL AVENUE
MADISON, WI 53706

89083321273



b89083321273a

This is the first book focused exclusively on Internet worm detection and mitigation strategies to help professionals with their challenging work in the field. This groundbreaking volume enables practitioners to tackle the ever-increasing presence of Internet worms with practical detection knowledge and defense techniques utilizing data from live networks, real IP addresses, and commercial tools. The book discusses the classifications and groupings of worms, and offers a deeper understanding of how they threaten network and system security.

After examining how a worm is constructed and how its major life-cycle steps are implemented, the book scrutinizes targets that worms have attacked over the years, and the likely targets of the immediate future. Covering both commercial and open-source tools, this unique reference explains how to detect worms using a variety of mechanisms, and evaluates the strengths and weaknesses of three approaches—traffic analysis, honeypots and dark network monitors, and signature analysis. The book concludes with a discussion of four effective defenses against network worms, including host-based defenses, network firewalls and filters, application layer proxies, and a direct attack on the worm network itself.

Jose Nazario is a senior software engineer at Arbor Networks, an Internet security company. He is also a consultant and researcher at Crimelabs Research, a think tank and consulting firm. He holds a Ph.D. in biochemistry from Case Western Reserve University. He has published extensively.

ISBN 1-58053-537-2



9 781580 535373

**Artech House Publishers** BOSTON • LONDONwww.artechhouse.com

EXHIBIT B



Resource
Description
[Defense and detection strategies against Internet worms / Jose Nazario. Nazario, Jose. Art ech House, Boston : 2004 \[1580535372 \(alk. paper\)\]](#)

Holdings [Verona Shelving Facility: Shelving Verona : Q476.9 A25 N38 2004](#)
Holdings ID 2281923990002122 [View all holdin...](#)
Barcode 89083321273 **Item ID** 23650364380002122 [View all items](#)
Process type [Loan](#) **MMS ID** 9961717053602122 [Browse shelf li...](#)
Status Item not in place

General

ENUM/CHRON

Notes

History

General Information

Barcode 89083321273 **Copy ID** 1

Material type Book **Item policy** general (book)

Provenance - **Is magnetic** No

PO Line **Issue date** -

Receiving date 01/14/2004 **Expected receiving date** -

Enumeration A - **Enumeration B** -

Chronology I - **Chronology J** -

Description - **Pieces** 1

Pages - **Receiving operator** import

Replacement cost -

Physical condition -

Process type

Inventory Information

Inventory number - **Inventory date** -

Inventory price -

Location Information

Permanent location Verona Shelving Facility: Shelving Verona (vsf)

Item call number type - **Item call number** -

Source (Subfield 2) -

Storage location ID -

Temporary Location Information

Item is in temporary location	No	
Temporary location	-	
Temporary call number type	-	Temporary call number -
Temporary source (Subfield 2)	-	
Temporary item policy	-	Due back date -

Retention Information		▼
Committed to Retain	-	
Retention Reason	-	Retention Note -