SYNGRESS®

Malware Forensics Field Guide for Linux Systems

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina

Malware Forensics Field Guide for Linux Systems

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina

Curtis W. Rose, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG
LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO
SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS®

Acquiring Editor: Chris Katsaropoulos
Editorial Project Manager: Benjamin Rearick
Project Manager: Priya Kumaraguruparan
Designer: Alan Studholme

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described here in. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application Submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-59749-470-0

For information on all Syngress publications,
visit our website at store.elsevier.com/syngress

Printed and bound in the United States of America
14 15 16 17 18   10 9 8 7 6 5 4 3 2 1

Malware Forensics Field Guide for Linux Systems

"To our brothers and sisters—Alecia, David, Daniel, Tony and Jennifer—who have inspired, supported and motivated us since our beginnings. We love you."

Acknowledgments

Cameron is grateful for the wonderful support and input that many people provided to make this book possible.

James and Eoghan I could not ask for a finer team to write with; I continue to be inspired by your talent and creativity. You are my *scriptis fratribus.*

Thanks to the editorial team at Syngress for your patience and commitment to this book: Laura Colantoni, Steve Elliot, Chris Katsaropoulos, and Benjamin Rearick.

Some of the world's finest researchers, developers and forensic practitioners helped us navigate the interesting challenges we encountered during the course of writing this book. Many thanks to Mila Parkour (contagiodump.blogspot.com), Ero Carrera and Christian Blichmann (Zynamics), Matthew Shannon (F-Response), Andrew Tappert (Raytheon Pikewerks), Andrew Rosen (ASR Data), Thorsten Holz (Assistant Professor at Ruhr-University Bochum/ http://honeyblog.org/), and Tark (ccso.com).

To my fellow Honeynet Project members, my sincerest thanks for allowing me to participate in the Project; your passion and innovation is special and I'm fortunate to be a part of such an awesome group.

Many thanks to my friends and colleagues at the NCAVC BAU; it is an honor to be a part of the team. BTAC and CBAC—thank you for infusing motivation and creativity that continue to make me see the beauty of nuances.

Above all, I want to thank my wonderful wife, Adrienne, and little Huddy, who supported and encouraged me during the writing of this book, despite all the time it took me away from them. You are my world.

Cameron H. Malin

Eoghan is deeply grateful to Cameron and James for continuously reminding me that our readers are the reason we write. The thoughtfulness and care this team has devoted to this work is an inspiration. We have dealt with many challenges throughout the lifetime of this book series, and I am proud of the results.

I am grateful for, and continue to be inspired by, Morgan Marquis-Boire's generosity in sharing his deep knowledge and talent. Thanks to Andrew Case, Joe Sylvie, and Andrew Tappert for sharing their experiences in Linux and Android memory forensics. My full gratitude and respect goes to Mike Wooster for tirelessly advancing the availability, capability, and security of Linux.

Finally, thanks to my family for keeping my heart in the right place. My love for you all is vibrant, colorful, always.

Eoghan Casey

James is grateful to his family, friends, and colleagues at Stroz for their patience, support, and care. To Syngress and our friends in the field who shared their thoughts and talents with us, I thank you. To all of those in federal law enforcement I have come to know, trust, and admire over the years – you inspire me. And to my dear co-authors Cameron and Eoghan, the third time has indeed been a charm.

James M. Aquilina

SPECIAL THANKS TO THE TECHNICAL EDITOR

Our sincerest thanks to digital forensic juggernaut and technical editor extraordinaire, Curtis W. Rose. Your insightful comments and guidance made this book possible.

About the Authors

Cameron H. Malin is a Supervisory Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Behavioral Analysis Unit, Cyber Behavioral Analysis Center, where he is responsible for analyzing the behavior of cyber offenders in computer intrusion and malicious code matters. In 2010, Mr. Malin was a recipient of the Attorney General's Award for Distinguished Service for his role as a Case Agent in Operation Phish Phry. In 2011 he was recognized for his contributions to a significant cyber counterintelligence investigation for which he received the National Counterintelligence Award for Outstanding Cyber Investigation by the Office of the Director of National Intelligence.

Mr. Malin is the Chapter Lead for the Southern California Chapter of the Honeynet Project, an international, non-profit organization dedicated to improving the security of the Internet through research, analysis, and information regarding computer and network security threats. He is also a Subject Matter Expert for the Department of Defense (DoD) Cyber Security & Information Systems Information Analysis Center (formerly the Information Assurance Technology Analysis Center, "IATAC") and the Weapon Systems Technology and Information Analysis Center (WSTIAC).

Mr. Malin is a Certified Ethical Hacker (CEH) and Certified Network Defense Architect (CNDA) as designated by the International Council of Electronic Commerce Consultants (EC-Council); a GIAC Certified Intrusion Analyst (GCIA) and GIAC Certified Forensic Analysis (GCFA) as designated by the SANS Institute; and a Certified Information Systems Security Professional (CISSP), as designated by the International Information Systems Security Certification Consortium ((ISC)$^{2®}$).

Prior to working for the FBI, Mr. Malin was an Assistant State Attorney (ASA) and Special Assistant United States Attorney in Miami, Florida, where he specialized in computer crime prosecutions. During his tenure as an ASA, he was also an Assistant Professorial Lecturer in the Computer Fraud Investigations Masters Program at George Washington University.

Mr. Malin is co-author of the Malware Forensics book series, *Malware Forensics: Investigating and Analyzing Malicious Code*, and the *Malware Forensics Field Guide for Windows Systems*, published by Syngress, an imprint of Elsevier, Inc.

The techniques, tools, methods, views, and opinions explained by Cameron Malin are personal to him, and do not represent those of the United States Department of Justice, the FBI, or the government of the United States of America. Neither the Federal government nor any Federal agency endorses this book or its contents in any way.

Eoghan Casey is an internationally recognized expert in digital forensics and data breach investigations. He wrote the foundational book *Digital Evidence and Computer Crime*, and created Smartphone Forensics courses taught worldwide. For over a decade, he has dedicated himself to advancing the practice of incident handling and digital forensics. He has worked as R&D Team Lead at the Defense Cyber Crime Center (DC3) helping enhance their operational capabilities and develop new techniques and tools.

Mr. Casey helps client organizations handle security breaches and analyzes digital evidence in a wide range of investigations, including network intrusions with international scope. In his prior work at cmdLabs and as Director of Digital Forensics and Investigations at Stroz Friedberg, he maintained an active docket of cases and co-managed technical operations in the areas of digital forensics, cyber-crime investigation, and incident handling. He has testified in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

He has delivered keynotes and taught workshops around the globe on various topics related to data breach investigation, digital forensics, and cyber security. He has co-authored several advanced technical books including *Malware Forensics*, and is Editor-in-Chief of *Digital Investigation: The International Journal of Digital Forensics and Incident Response*.

As Executive Managing Director of Stroz Friedberg LLC, **James M. Aquilina** serves as part of the Executive Management team, leads the firm's Digital Forensics practice, and oversees the Los Angeles, San Francisco, and Seattle offices. He supervises numerous digital forensic, Internet investigative, and electronic discovery assignments for government agencies, major law firms, and corporate management and information systems departments in criminal, civil, regulatory, and internal corporate matters, including matters involving data breach, e-forgery, wiping, mass deletion, and other forms of spoliation, leaks of confidential information, computer-enabled theft of trade secrets, and illegal electronic surveillance. He has served as a special master, a neutral expert, and has been appointed by courts to supervise the forensic examination of digital evidence. Mr. Aquilina also has led the development of the firm's Online Fraud and Abuse practice, regularly consulting on the technical and strategic aspects of initiatives to protect computer networks from spyware and other invasive software, malware, and malicious code, online fraud, and other forms of illicit Internet activity. His deep knowledge of botnets, distributed denial of service attacks, and other automated cyber intrusions enables him to provide companies with advice and solutions to tackle incidents of computer fraud and abuse and bolster their infrastructure protection.

Prior to joining Stroz Friedberg, Mr. Aquilina was an Assistant U.S. Attorney (AUSA) in the Criminal Division of the U.S. Attorney's Office for the Central District of California, where he most recently served in the Cyber and Intellectual Property Crimes Section. He also served as a member of the Los Angeles Electronic Crimes Task Force and as chair of the Computer Intrusion Working Group, an interagency cyber-crime response organization. As an AUSA, Mr. Aquilina conducted and supervised investigations and prosecutions of computer intrusions, extortionate denial of service attacks, computer and Internet fraud, criminal copyright infringement, theft of trade secrets, and other abuses involving the theft and use of personal identity. Among his notable cyber cases, Mr. Aquilina brought the first U.S. prosecution of malicious botnet activity against a prolific member of the "botmaster underground," who sold his armies of infected computers for the purpose of launching attacks and spamming and used his botnets to generate income from the surreptitious installation of adware; tried to jury conviction the first criminal copyright infringement case involving the use of digital camcording equipment; supervised the government's continuing prosecution of Operation Cyberslam, an international intrusion investigation involving the use of hired hackers to launch computer attacks against online business competitors; and oversaw the collection and analysis of electronic evidence relating to the prosecution of a local terrorist cell operating in Los Angeles.

During his tenure at the U.S. Attorney's Office, Mr. Aquilina also served in the Major Frauds and Terrorism/Organized Crime Sections, where he investigated and tried numerous complex cases including: a major corruption trial against an IRS Revenue Officer and public accountants, a fraud prosecution against the French bank Credit Lyonnais in connection with the rehabilitation and liquidation of the now defunct insurer Executive Life, and an extortion and kidnapping trial against an Armenian organized crime ring. In the wake of the September 11, 2001, attacks, Mr. Aquilina helped establish and run the Legal Section of the FBI's Emergency Operations Center.

Before public service, Mr. Aquilina was an associate at the law firm Richards, Spears, Kibbe & Orbe in New York, where he focused on white collar defense work in federal and state criminal and regulatory matters.

Mr. Aquilina served as a law clerk to the Honorable Irma E. Gonzalez, U.S. District Judge, Southern District of California. He received his B.A. magna cum laude from Georgetown University, and his J.D. from the University of California, Berkeley School of Law, where he was a Richard Erskine Academic Fellow and served as an Articles Editor and Executive Committee Member of the California Law Review.

He currently serves as an Honorary Council Member on cyber-law issues for the EC-Council, the organization that provides the CEH and CHFI (Certified Hacking Forensic Investigator) certifications to leading security industry professionals worldwide. Mr. Aquilina is a member of Working Group 1 of the Sedona Conference, the International Association of Privacy Professionals, the Southern California Honeynet Project, the Los Angeles Criminal Justice Inn of Court, and the Los Angeles County Bar Association. He also serves on the Board of Directors of the Constitutional Rights Foundation, a non-profit educational organization dedicated to providing young people with access to and understanding of the law and the legal process.

Mr. Aquilina is co-author of the widely acclaimed books, *Malware Forensics: Investigating and Analyzing Malicious Code* and *Malware Forensics Windows Field Guide*, both published by Syngress Publishing, Elsevier Science & Technology Books, which detail the process of responding to the malicious code incidents victimizing private and public networks worldwide.

About the Technical Editor

Curtis W. Rose is the President and founder of Curtis W. Rose & Associates LLC, a specialized services company in Columbia, Maryland which provides computer forensics, expert testimony, litigation support, computer intrusion response and training to commercial and government clients. Mr. Rose is an industry-recognized expert with over 20 years of experience in investigations, computer forensics, technical, and information security.

Mr. Rose was a coauthor of *Real Digital Forensics: Computer Security and Incident Response*, and was a technical editor or contributing author for many popular information security books including *Malware Forensics Field Guide for Windows Systems, Handbook of Digital Forensics and Investigations, Malware Forensics: Investigating and Analyzing Malicious Code, SQL Server Forensic Analysis, Anti-Hacker Toolkit, 1st Edition, Network Security: The Complete Reference; and Incident Response and Computer Forensics, 2nd Edition.* He has also published white papers on advanced forensic methods and techniques including *Windows Live Response Volatile Data Collection: Non-Disruptive User & System Memory Forensic Acquisition* and *Forensic Data Acquisition & Processing Utilizing the Linux Operating System.*

Introduction to Malware Forensics

Since the publication of *Malware Forensics: Investigating and Analyzing Malicious Code* in 2008,[1] the number and complexity of programs developed for malicious and illegal purposes has grown substantially. The most current Symantec Internet Security Threat Report announced that threats to online security grew and evolved considerably in 2012. Noted was the burgeoning cyber espionage trend, as well as the increasing sophistication and viciousness of new malware threats. The report revealed that malware authors are conducting more targeted attacks aimed at spying on victims for profit and/or data collection—while attribution of the malware attackers is becoming more difficult. An identified increase in malicious e-mail, Web domains, and mobile malware families demonstrates a continued upward threat trajectory; a predicted increase in these trends further confirms that the malware threatscape will continue to present significant challenges.[2] Other anti-virus vendors, including F-Secure, document a recent increase in malware attacks against mobile devices (particularly the Android platform) and Mac OS X, and in attacks conducted by more sophisticated and organized hacktivists and state-sponsored actors.[3]

In the past, malicious code has been categorized neatly (e.g., viruses, worms, or Trojan Horses) based upon functionality and attack vector. Today, malware is often modular and multifaceted, more of a "blended-threat" with diverse functionality and means of propagation. Much of this malware has been developed to support increasingly organized, professional computer criminals. Indeed, criminals are making extensive use of malware to control computers and steal personal, confidential, or otherwise proprietary information for profit.[4] In Operation Trident Breach,[5] hundreds of individuals were arrested for their involvement in digital theft using malware such as Zeus. A thriving gray market ensures that today's malware are professionally developed to avoid detection by current AntiVirus programs, thereby remaining valuable and available to any cyber-savvy criminal group.

[1] http://store.elsevier.com/product.jsp?isbn=9780080560199&pagename=search.

[2] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[3] http://www.f-secure.com/en/web/labs_global/2011/2011-threat-summary.

[4] http://money.cnn.com/2012/09/04/technology/malware-cyber-attacks/.

[5] http://krebsonsecurity.com/tag/operation-trident-breach/.

Of growing concern is the development of malware to disrupt power plants and other critical infrastructure through computers, referred to by some as cyberwarfare. The StuxNet and Duqu malware that has emerged in the past few years powerfully demonstrate the potential for such attacks.[6] This sophisticated malware enabled the attackers to alter the operation of industrial systems, like those in a nuclear reactor, by accessing programmable logic controllers connected to the target computers. Such attacks could shut down a power plant or other components of a society's critical infrastructure, potentially causing significant harm to people in a targeted region.

Foreign governments are funding teams of highly skilled hackers to develop customized malware to support industrial and military espionage.[7] The intrusion into Google's systems demonstrates the advanced and persistent capabilities of such attackers.[8] These types of well-organized attacks are designed to maintain long-term access to an organization's network, a form of Internet-enabled espionage known as the "Advanced Persistent Threat" (APT).[9] Recently, malware researchers have revealed other cyber espionage malware campaigns, such as "Flame,"[10] "Red October,"[11] "Gauss,"[12] "SPE/miniFlame,"[13] "Safe,"[14] "Shady RAT,"[15] and "Dark Seoul."[16]

[6] http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices; http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[7] The New E-spionage Threat," available at http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm; "China accused of hacking into heart of Merkel administration," available at http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece.

[8] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[9] For more information about APT, see, https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/; http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[10] https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers; http://www.pcworld.com/article/256370/researchers_identify_stuxnetlike_cyberespionage_malware_called_flame.html.

[11] http://usa.kaspersky.com/about-us/press-center/in-the-news/kaspersky-labs-finds-red-october-cyber-espionage-malware; https://www.securelist.com/en/analysis/204792265/Red_October_Detailed_Malware_Description_1_First_Stage_of_Attack;https://www.securelist.com/en/analysis/204792268/Red_October_Detailed_Malware_Description_2_Second_Stage_of_Attack; https://www.securelist.com/en/analysis/204792264/Red_October_Detailed_Malware_Description_3_Second_Stage_of_Attack; https://www.securelist.com/en/analysis/204792273/Red_October_Detailed_Malware_Description_4_Second_Stage_of_Attack.

[12] http://www.symantec.com/connect/blogs/complex-cyber-espionage-malware-discovered-meet-w32gauss.

[13] http://www.networkworld.com/community/blog/flames-vicious-little-sibling-miniflame-extremely-targeted-cyber-espionage-malware.

[14] http://www.dfinews.com/news/2013/05/cyber-espionage-campaign-uses-professionally-made-malware#.Ug-jj21Lgas.

[15] http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html.

[16] http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea; http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf; http://www.infoworld.com/t/data-security/mcafee-uncovers-massive-cyber-espionage-campaign-against-south-korea-222245.