Community Experience Distilled

Cuckoo Malware Analysis

Analyze malware using Cuckoo Sandbox

Digit Oktavianto
Iqbal Muhardianto

[PACKT] PUBLISHING open source* community experience distilled

Cuckoo Malware Analysis

Analyze malware using Cuckoo Sandbox

Digit Oktavianto

Iqbal Muhardianto

[PACKT] open source
community experience distilled
PUBLISHING

BIRMINGHAM - MUMBAI

Cuckoo Malware Analysis

First published: October 2013

Production Reference: 1091013

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78216-923-9

www.packtpub.com

Cover Image by Prashant Timappa Shetty (sparkling.spectrum.123@gmail.com)

Credits

Authors

Digit Oktavianto

Iqbal Muhardianto

Reviewers

Charles Lim

Ashley

Acquisition Editors

Anthony Albuquerque

Amarabha Banerjee

Kartikey Pandey

Commissioning Editor

Shaon Basu

Technical Editor

Akashdeep Kundu

Project Coordinator

Akash Poojary

Proofreader

Kelly Hutchinson

Indexer

Priya Subramani

Graphics

Ronak Dhruv

Production Coordinator

Arvindkumar Gupta

Cover Work

Arvindkumar Gupta

About the Authors

Digit Oktavianto is an IT security professional and system administrator with experience in the Linux server, network security, Security Information and Event Management (SIEM), vulnerability assesment, penetration testing, intrusion analysis, incident response and incident handling, security hardening, PCI-DSS, and system administration.

He has good experience in Managed Security Services (MSS) projects, Security Operation Centre, operating and maintaining SIEM tools, configuring and setup of IDS/IPS, Firewall, Antivirus, Operating Systems, and Applications.

He works as an information security analyst in Noosc Global, a security consultant firm based in Indonesia. Currently, he holds CEH and GIAC Incident Handler certifications. He is very enthusiastic and has a good passion in malware analysis as his main interest for research. This book is the first book that he has written, and he plans to write more about malware analysis and incident response books.

Acknowledgement

I would like to thank Allah the God Almighty, my friend from IT Telkom, Indra Kusuma as a contributor and reviewer, and my boss and partner in Noosc Global for giving a facility for my research. I also want to thank my girlfriend, Eva, for her support and motivation in finishing this book.

I want to give you a list of names of persons to acknowledge as a gratitude for their effort in helping us in writing our book:

Chort Z. Row for the Video in Youtube (Using Cuckoobox and Volatility to analyze APT1 malware) at `http://www.youtube.com/watch?v=mxGnjTlufAA`, and thank you for providing Yara rules for Miniasp3 detection.

A.A. Gede Indra Kusuma from IT Telkom. Thank you for your effort in Malware Lab, and produce some resources for the book.

Jaime Blasco and Alberto Ortega from Alienvault. Thank you for providing Yara rules for APT1 detection.

David Bressler (bostonlink) for the great effort on Cuckooforcanari Project.

Alberto Ortega from Alienvault for his post on `http://www.alienvault.com/open-threat-exchange/blog/hardening-cuckoo-sandbox-against-vm-aware-malware` about Hardening Cuckoo Sandbox.

Xavier Mertens (`@xme`) for CuckooMX Project at `http://blog.rootshell.be/2012/06/20/cuckoomx-automating-email-attachments-scanning-with-cuckoo/`

All Cuckoo Sandbox Developers and founder: Claudio "*nex*" Guarnieri, Mark Schloesser, Alessandro "*jekil*" Tanasi, and Jurriaan Bremer. Thank you very much for the great documentation on `http://docs.cuckoosandbox.org/en/latest/`.

Mila Parkour from `http://contagiodump.blogspot.com`. Thank you for providing a lot of information about malware samples.

`http://virusshare.com/` and `http://virusshare.com/` for providing us APT1 malware sample.

Iqbal Muhardianto is a security enthusiast and he is working in the Ministry of Foreign Affairs of the Republic of Indonesia. He loves breaking things apart just to know how it works. In his computer learning career, he first started with learning MS-DOS and some C programming, after being a System admin, Network Admin, and now he is a IT Security Administrator with some skills in Linux, Windows, Network, SIEM, Malware Analysis, and Pentesting.

He currently lives Norway and works as an IT Staff in the Indonesia Embassy in Oslo.

I would like to thank Allah the God Almighty, my parents and family, my friend Digit Oktavianto for inviting me to write this book, and my colleagues for their support and inspiration.

About the Reviewers

Charles Lim is a lecturer and researcher of Swiss German University. He has extensive IT consulting experiences before joining Swiss German University in 2007. His current research interests are Malware, Web Security, Vulnerability Analysis, Digital Forensics, Intrusion Detection, and Cloud Security. He has helped the Indonesia Ministry of Communication and Informatics create a web security assessment and data center regulation.

He is currently leading the Indonesia Chapter of Honeynet Project and is also a member of the Indonesia Academy Computer Security Incident Response Team and Cloud Security Alliance—Indonesia Chapter.

He is a regular contributor to the Indonesia CISO (Chief Information Security Officer) Magazine and also an editor and technical editor of IAES Journal.

I would like to thank Packt Publishing for giving me the opportunity to review the content of this book.

Ashley has a vision to make Mauritius a free and safe Intelligent Island in-line with the vision of the Government of Mauritius. He has completed his Bachelor in Science in Computing from Greenwich University, UK, and his Masters in Science from the University of Technology in Mauritius in Computer Security and Forensics, where he has topped. He has shouldered important positions in Mauritius and is currently a senior lecturer and program coordinator of Information Technology at the Amity University, Mauritius. He has designed and developed several innovative courses ranging from Diploma to Master levels. These courses have proven to be highly relevant according to industry needs and are very much welcomed by all stakeholders. He has also contributed towards several government projects in the field of IT security. In addition to shouldering high responsibilities at Amity, Ashley is a heavily sought consultant in IT security. Mr. Paupiah is of the opinion that he has acquired and mastered most of the tools required to achieve his vision.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents