

2018 13th International Conference on Malicious and Unwanted Software (MALWARE 2018)

**Nantucket, Massachusetts, USA
22 – 24 October 2018**



**IEEE Catalog Number: CFP1859F-POD
ISBN: 978-1-7281-0156-9**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1859F-POD
ISBN (Print-On-Demand):	978-1-7281-0156-9
ISBN (Online):	978-1-7281-0155-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Session 1 – Measurement: The Effectiveness of Anti-Malware Techniques

Static Malware Detection and Subterfuge: Quantifying the Robustness of Machine Learning and Current Anti-Virus	3
<i>William Fleshman, Edward Raff, Richard Zak, Mark McLean, Charles Nicholas</i>	
Is Eval () Evil : A Study of JavaScript in PDF Malware	13
<i>Antoine Lemay, Sylvain P. Leblanc</i>	
An In-Depth Study of Open-Source Command and Control Frameworks	23
<i>Julien Piet, Blake Anderson, David McGrew</i>	

Session 2 – Malware in the Times of Mobile Devices

SpyDroid: A Framework for Employing Multiple Real-Time Malware Detectors on Android	33
<i>Shahreaz Iqbal, Mohammad Zulkernine</i>	
PRAST: Using Logic Bombs to Exploit the Android Permission Model and a Module based Solution	41
<i>Ramon P. Medina, Elijah B. Neundorfer, Radhouane Chouchane, Alfredo Perez</i>	
Android Malware Detection using Step-Size based Multi-Layered Vector Space Models	49
<i>Colby Parker, J. Todd McDonald, Tom Johnsten, Ryan G. Benton</i>	

Session 3 – Botnets

An Adversarial Coupon-Collector Model of Asynchronous Moving-Target Defense against Botnet Reconnaissance	61
<i>George Kesidis, Yuquan Shan, Daniel Fleck, Angelos Stavrou, Takis Konstantopoulos</i>	
Attacking OMG Data Distribution Service (DDS) based Real-Time Mission Critical Distributed Systems	68
<i>Michael James Michaud, Thomas Dean, Sylvain P. Leblanc</i>	
Resilience of Pruned Neural Network against Poisoning Attack	78
<i>Bingyin Zhao, Yingjie Lao</i>	

Session 4 – Anti Malware Techniques

PIDS: A Behavioral Framework for Analysis and Detection of Network Printer Attacks	87
<i>Asaf Hecht, Adi Sagi, Yuval Elovici</i>	

METICS: A Holistic Cyber Physical System Model for IEEE 14-Bus Power System Security	95
<i>Ananth A. Jillepalli, Daniel Conte de Leon, Brian K. Johnson, Yacine Chakhchoukh, Ibukun A. Oyewumi, Mohammad Ashrafuzzaman, Frederick T. Sheldon, Jim Alves-Foss, Michael A. Haney</i>	

Behavioral Malware Classification using Convolutional Recurrent Neural Networks	103
<i>Bander Alsulami, Spiros Mancoridis</i>	

Session 5 – Defense Techniques and Other Musings

A Hybrid Static Tool to Increase the Usability and Scalability of Dynamic Detection of Malware	115
<i>Danny Kim, Daniel Mirsky, Amir Majlesi-Kupaei, Rajeev Barua</i>	

Malware Anomaly Detection on Virtual Assistants	124
<i>Ni An, Alexander Duff, Mahshid Noorani, Steven Weber, Spiros Mancoridis</i>	

Model-Driven Timing Consistency for Active Malware Redirection	132
<i>Rory Klein, Tyler Barkley, Weston Clizbe, Jennifer Bateman, Julian L. Rrushi</i>	

Session 6 – Anti Malware

SCRaaPS: X.509 Certificate Revocation using the Blockchain-Based Scrybe Secure Provenance System ..	145
<i>Sai Medury, Anthony Skjellum, Richard R. Brooks, Lu Yu</i>	

Binary Obfuscation based Reassemble	153
<i>Chang Wang, Zhaolong Zhang, Xiaoqi Jia, Donghai Tian</i>	

Unmasking Criminal Enterprises: An Analysis of Bitcoin Transactions	161
<i>Jonathan Oakley, Carl Worley, Lu Yu, Richard Brooks, Anthony Skjellum</i>	