

# **2024 APWG Symposium on Electronic Crime Research (eCrime 2024)**

**Boston, Massachusetts, USA  
24-26 September 2024**



**IEEE Catalog Number: CFP2454F-POD  
ISBN: 979-8-3315-2450-0**

**Copyright © 2024 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:	CFP2454F-POD
ISBN (Print-On-Demand):	979-8-3315-2450-0
ISBN (Online):	979-8-3315-2449-4
ISSN:	2159-1237

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2024 APWG Symposium on Electronic Crime Research (eCrime) **eCrime 2024**

## Table of Contents

Preface .....	vii
Committee Members .....	viii

### **The Emerging AI Conflict at the Cybercrime Frontier**

Multimodal Large Language Models for Phishing Webpage Detection and Identification .....	1
<i>Jehyun Lee (Trustwave), Peiyuan Lim (National University of Singapore), Bryan Hooi (National University of Singapore), and Dinil Mon Divakaran (Institute for Infocomm Research, A*STAR)</i>	

### **Internet Infrastructure Policy and Defense Posture in 2024**

Owned, Pwned or Rented: Whose Domain Is It? .....	14
<i>Mina Erfan (University of Ottawa, Canada), Paula Branco (University of Ottawa, Canada), and Guy-Vincent Jourdan (University of Ottawa, Canada)</i>	
EagleEye: Attention to Unveil Malicious Event Sequences from Provenance Graphs .....	27
<i>Philipp Gysel (Acronis Research, Switzerland), Candid Wüest (Acronis Research, Switzerland), Kenneth Nwafor (Acronis Research, Switzerland, and Constructor Technology, Switzerland), Otakar Jašek (Acronis Research, Switzerland), Andrey Ustyuzhanin (Constructor University Bremen, Germany and Acronis Research, Switzerland), and Dinil Mon Divakaran (Institute for Infocomm Research (I2R), A*STAR, Singapore)</i>	
Risk Assessment & Mitigation for Core Security Capabilities .....	43
<i>Marc Dupuis (University of Washington) and Karen Renaud (University of Strathclyde)</i>	

### **Hygienic Practices for Maintaining Internet and Enterprise Infrastructure**

Exploring Content Concealment in Email .....	58
<i>Lucas Betts (University of Auckland, New Zealand), Robert Biddle (Carleton University, Canada), Danielle Lottridge (University of Auckland, Auckland, New Zealand), and Giovanni Russello (University of Auckland, New Zealand)</i>	

What To Do Against Ransomware? Evaluating Law Enforcement Interventions .....	76
<i>Tom Meurs (University of Twente), Raphael Hoheisel (University of Twente), Marianne Junger (University of Twente), Abhishta Abhishta (University of Twente), and Damon McCoy (New York University)</i>	
Typosquatting 3.0: Characterizing Squatting in Blockchain Naming Systems .....	94
<i>Muhammad Muzammil (Stony Brook University), Zhengyu Wu (Stony Brook University), Lalith Harisha (Stony Brook University), Brian Kondracki (Stony Brook University), and Nick Nikiforakis (Stony Brook University)</i>	

## Human Factors in Evolution of Electronic Crime & AI Crime

"Hey Google, Remind me to be Phished" Exploiting the Notifications of the Google (AI) Assistant on Android for Social Engineering Attacks .....	109
<i>Marie Weinz (University of Liechtenstein), Saskia Laura Schröer (University of Liechtenstein), and Giovanni Apruzzese (University of Liechtenstein)</i>	
Love Bytes Back: Cybercrime Following Relationship Breakdown .....	123
<i>Quincy Taylor (University of Cambridge), Anna Talas (University of Cambridge), and Alice Hutchings (University of Cambridge)</i>	

## Mapping the Cybercrime Economy and Its Marketplaces

A Sinister Fattening: Dissecting the Tales of Pig Butchering and other Cryptocurrency Scams .....	136
<i>Marilyne Ordekian (University College London, United Kingdom), Antonis Papasavva (University College London, United Kingdom), Enrico Mariconti (University College London, United Kingdom), and Marie Vasek (University College London, United Kingdom)</i>	
Showing the Receipts: Understanding the Modern Ransomware Ecosystem .....	149
<i>Jack Cable (Independent Researcher), Ian Gray (New York University), and Damon McCoy (New York University)</i>	
ModZoo: A Large-Scale Study of Modded Android Apps and their Markets .....	162
<i>Luis A. Saavedra (University of Cambridge), Hridoy S. Dutta (University of Cambridge), Alastair R. Beresford (University of Cambridge), and Alice Hutchings (University of Cambridge)</i>	
Identifying Key Expert Actors in Cybercrime Forums Based on their Technical Expertise .....	175
<i>Estelle Ruellan (Université de Montréal, Flare, Canada), François Labrèche (Secureworks, Canada), and Masarah Paquet-Clouston (Université de Montréal, Complexity Science Hub, Canada)</i>	
Dark Web Dialogues: Analyzing Communication Platform Choices of Underground Forum Users .....	187
<i>Raphael Hoheisel (University of Twente), Tom Meurs (University of Twente), Marianne Junger (University of Twente), Erik Tews (University of Twente), and Abhishta Abhishta (University of Twente)</i>	

<b>Author Index</b> .....	<b>203</b>
---------------------------	------------