# John J. Seymour, III

seymour1@umbc.edu 410-350-4877
sites.google.com/site/jjseymour3 github.com/seymour1

Research Interests: Machine Learning, Malware Analysis

## Education

**University of Maryland, Baltimore County (UMBC)**

Ph.D. in Computer Science (Expected Fall 2017)
Graduate GPA: 4.0/4.0

M.S. in Computer Science (Fall 2014)
Thesis Title: Quantum Classification of Malware

B.S./B.S./B.A. *cum laude* in Computer Science/Mathematics/Philosophy (Fall 2011)
Undergraduate GPA: 3.70/4.00, Certificate of General Honors

## Work Experience

**ZeroFOX**

*Senior Data Scientist*, September 2016 - Present

- Piloted ZeroFOX FoxThreats program for threat hunting on social media.
- Conveyed complex machine learning concepts to press and conference attendees.
- Interviewed and mentored new hires.

*Data Scientist*, September 2015 - September 2016

- Led development of SNAP_R, a machine learning based pen-testing tool to automate generation of individually tailored phishing messages on Twitter.
- Developed solution to detect money-flipping scam posts on Instagram.
- Created high-quality datasets and classifiers for product offerings.

**CyberPoint International, LLC**

*Student Intern*, Summer 2015

- Researched bleeding-edge malware classification techniques and integrated them into the CyberPoint Machine Learning Model Training Pipeline.
- Created algorithm and data structure vulnerabilities for DARPA STAC competition.

**University of Maryland, Baltimore County**

*Graduate Research Assistant, UMBC DREAM Lab*, January 2014 - May 2015

- Scraped urlquery.net for links to websites redirecting to exploit kits.
- Intercepted and recorded traffic to exploit kit landing pages for use in data analysis.

*Graduate Teaching Assistant*, August 2012 - December 2013

- Teaching Assistant for Network Security, Computer Security, Cryptography, Automata Theory, and Introduction to Object-Oriented Programming.
- Taught Metasploit, Kali Linux, and infosec theory to undergraduate students.

*Graduate Research Assistant, UMBC Cyber Defense Lab*, January 2012 - August 2013

- Designed, deployed, and maintained LAMP stack to host government-funded gamification initiative for teaching high school students basic concepts in infosec.

**Army Research Lab**

*Student Intern*, Summer 2014

- Transformed satisfiability problems into problems the D-Wave SR10V6 could solve.
- Demonstrated and reduced bias in D-Wave chips using statistical techniques.

**Pyxis Engineering/Applied Signals Technology**

*Associate Engineer*, June 2009 - January 2010

- Designed and deployed a Training Request Management System.

# John J. Seymour, III

seymour1@umbc.edu
410-350-4877
sites.google.com/site/jjseymour3
github.com/seymour1

Research Interests: Machine Learning, Malware Analysis

## Publications

- John Seymour,"Hacking a Corporate Social Media Page", ZeroFOX white paper, December 2016.
- John Seymour and Charles Nicholas,"How to build a malware classifier [that doesnt suck on real-world data]", SecTor, October 2016. Also presented at Data Science MD (October 2016).
- Philip Tully, John Seymour, and Spencer Wolfe, "Post Grams Not Scams: Detecting Money Flipping Scams on Instagram Using Machine Learning", ZeroFOX white paper, September 2016. Covered by BBC News, NBC News, TechCrunch, and The Verge, among others.
- John Seymour and Philip Tully, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter", Black Hat USA, August 2016. Also presented at DEF CON 24 (August 2016), CyberGamut (December 2016), BrightTalk (December 2016), Baltimore Python (July 2016). Covered by The Atlantic, MIT Technology Review, and Forbes, among others.
- John Seymour and Charles Nicholas, "Labeling the VirusShare Corpus: Lessons Learned", BSidesLV, August 2016. Also presented at SPARSA South (July 2016), Baltimore Python (June 2016).
- Alan T. Sherman, John Seymour, Akshayraj Kore and William Newton, "Chaum's protocol for detecting man-in-the-middle: Explanation, demonstration, and timing studies for a text-messaging scenario", Cryptologia, May 2016.
- John Seymour and Charles Nicholas, "An Introduction to Malware Classification", BSidesCharm, April 2016.
- John Seymour and Charles Nicholas, "Quantum" Classification of Malware, DEF CON 23, August 2015. Also presented at CyberPoint International (July 2015), UMBC DREAM LAB (July 2015).
- John Seymour, "Overgeneralization in Feature Set Selection for Classification of Malware", CSEE Technical Report TR-CS-14-06, August 2014. Also presented at Malware Technical Exchange Meeting (June 2015, poster session), CyberPoint International (July 2015).
- John Seymour, "Skew Removal from SAT Instances using the D-Wave Quantum Annealer", Army Research Laboratory, July 31.
- Charles Nicholas, Robert Brandon, Joshua Domangue, Andrew Hallemeyer, Peter Olsen, Alison Pfannenstein and John Seymour, "The Exploit Kit Club", Malware Technical Exchange Meeting, July 22-24, 2014, Albuquerque, NM. (poster session)
- Charles Nicholas, Robert Brandon, Andrew Coates, Andrew Hallemeyer, Brian Hillsley, Victoria Lentz, Edward Mukasey, Peter Olsen, Alison Pfannenstein and John Seymour, "Tracking Exploit Kit Activity Through Landing Page Analysis", UMBC Computer Science and Electrical Engineering Department Technical Report 14-005, May 7, 2014.
- John Seymour, Joseph Tuzo, and Marie desJardins,"Ant Colony Optimization in a Changing Environment," Working Notes of the AAAI Fall Symposium on Complex Adaptive Systems, November 2011.
- Joseph Tuzo, John Seymour and Marie desJardins, "Using a Cellular Automaton Simulation to Determine an Optimal Lane Changing Strategy on a Multi-lane Highway," Working Notes of the AAAI Fall Symposium on Complex Adaptive Systems, November 2011.

## Affiliations

Admin: Baltimore Python
Member: MD Data Science
Judge: Code SLAM
Volunteer: CMPC Cold Weather Shelter
UMBC Honors College Alumn
Member: MLSecProject
Member: SPARSA South
Technical Consultant: UMBC Ethics Bowl Team
Member: United States Fencing Association
Eagle Scout