

GIORGIO SEVERI

🌐 severi.xyz

✉ severi.g@northeastern.edu

🔗 <https://github.com/ClonedOne>

🌐 <https://www.linkedin.com/in/giorgioseveri/>

Boston, MA, 02446

Research Interests Software Security and Adversarial Machine Learning.

Education **Ph.D.**, Northeastern University, Boston, MA Fall 2018 - Present
Major: Computer Science.
Advisor: Prof. Alina Oprea.

Master of Science, Sapienza University of Rome, Rome, Italy 2015 - 2018
Major: Computer Science and Engineering.
Final grade: 110/110 cum Laude.
Thesis: Malwords, Malware classification and clustering based on textual memory content.

Bachelor of Science, Sapienza University of Rome, Rome, Italy 2011 - 2014
Major: Computer Science and Engineering
Final grade: 107/110
Thesis: FreebleApp, Development of a smart, location based, mobile advertisement platform on Android OS.

Experience **Data Science Intern**, FireEye, Reston, VA 05/2019 - 08/2019
- Developed techniques to perform backdoor poisoning attacks in the context of malware classification.

Graduate Assistantship, Northeastern University, Boston, MA Fall 2018 - Present
Network and Distributed Systems Security Lab (NDS2), Khoury College.
- Graduate Fellowship for academic year 2018-2019.
- Conducting research on machine learning security and adversarial ML.

Junior Research Scientist, New York University, New York, NY 07/2017 - 10/2017
Center for Cybersecurity CCS, Tandon School of Engineering
- Conducted research on malware analysis and classification.
- Employed text mining and machine learning techniques to classify and cluster malicious software samples.

Student Internship, European Space Agency ESA, Italy 03/2016 - 06/2016
ESRIN, Earth Observation Directorate.
- Evaluated usability of satellite image resources for Hackathon participants.
- Developed a mobile application in Java to test a newly deployed web service.

Internal work placement, Sapienza University, Rome, Italy 2014 - 2015
Department of Computer, Control, and Management Engineering Antonio Ruberti.

Publications	<p>Jagielski, Matthew, Giorgio Severi, Niklas Pousette Harger, and Alina Oprea. "Subpopulation data poisoning attacks." arXiv preprint arXiv:2006.14026 (2020)¹.</p> <p>Giorgio Severi, Jim Meyer, Scott Coull, and Alina Oprea. "Exploring Backdoor Poisoning Attacks Against Malware Classifiers." ArXiv:2003.01031 [Cs], March 2, 2020².</p> <p>Giorgio Severi, Tim Leek, and Brendan Dolan-Gavitt. "Malrec: Compact Full-Trace Malware Recording for Retrospective Deep Analysis." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3-23. Springer, Cham, 2018³.</p>
Talks	<p>"Exploring Backdoor Poisoning Attacks Against Malware Classifiers". Giorgio Severi, Jim Meyer, Scott Coull. Conference on Applied Machine Learning in Information Security, CAMLIS, 2019, Washington, DC.</p>
Additional Experience	<p>Staff member at Codemotion Rome, 2017 and 2015.</p> <p>Mentor at "Tech My Cosplay", Arduino Hackathon Rome, 2017.</p> <p>Staff member at Data Driven Innovation Rome 2017.</p> <p>Staff member at Maker Faire Rome 2014.</p>
Languages	<p>Italian, native speaker.</p> <p>English, European level CEFR C2.</p> <ul style="list-style-type: none"> • International English Language Testing System, IELTS - score: 8.5/9. • University of Cambridge ESOL Certificate of Proficiency in English, CPE.
Awards	<p>Winner Accenture Digital Hackathon Rome⁴ 2016.</p> <p>NASA International SpaceApps Challenge 2015.</p> <ul style="list-style-type: none"> • Project CROPP, Global winner for category Galactic Impact and Rome competition local winner.⁵

¹<https://severi.xyz/publication/2020-06-14-Subpopulation>

²<https://severi.xyz/publication/2020-05-07-Exploring>

³<https://severi.xyz/publication/2018-06-28-Malrec>

⁴<https://www.accenture.com/it-it/Careers/accenture-digital-hackathon-2016>

⁵<https://2015.spaceappschallenge.org/award/>