

# Luca Demetrio

+393482849328 | [luca.demetrio93@unica.it](mailto:luca.demetrio93@unica.it) | [linkedin/luca.demetrio](https://www.linkedin.com/in/luca.demetrio) | [github/zangobot](https://github.com/zangobot) | [twitter/zangobot](https://twitter.com/zangobot)

## WORK EXPERIENCE


**UNIVERSITÀ DEGLI STUDI DI CAGLIARI** | POSTDOCTORAL RESEARCHER Cagliari, IT | January 2021 – current  
**MINICLIP** | INTERNSHIP, GAME DEVELOPMENT Genova, IT | July 2016 – September 2016

## EDUCATION

**Ph.D. in Computer Science** Genova, IT | January 2021  
UNIVERSITÀ DEGLI STUDI DI GENOVA  
**Master degree (110/110 cum laude) in Computer Science** Genova, IT | July 2017  
UNIVERSITÀ DEGLI STUDI DI GENOVA  
**Bachelor degree (110/110 cum laude) in Computer Science** Genova, IT | July 2015  
UNIVERSITÀ DEGLI STUDI DI GENOVA

## RESEARCH PAPERS

**ADVERSARIAL EXAMPLES: A SURVEY AND EXPERIMENTAL EVALUATION OF PRACTICAL ATTACKS ON MACHINE LEARNING FOR WINDOWS MALWARE DETECTION**  ACM TOPS 2021  
Luca Demetrio, Scott E. Coull, Battista Biggio, Giovanni Lagorio, Alessandro Armando, Fabio Roli


**FUNCTIONALITY-PRESERVING BLACK-BOX OPTIMIZATION OF ADVERSARIAL WINDOWS MALWARE**  IEEE TIFS 2021  
Luca Demetrio, Battista Biggio, Giovanni Lagorio, Fabio Roli, Alessandro Armando

**SLOPE: A FIRST-ORDER APPROACH FOR MEASURING GRADIENT OBFUSCATION**  ESANN 2021  
Maura Pintor, Luca Demetrio, Giovanni Manca, Battista Biggio, Fabio Roli


**WAF-A-MOLE: EVADING WEB APPLICATION FIREWALLS THROUGH ADVERSARIAL MACHINE LEARNING**  SAC 2020  
Luca Demetrio, Andrea Valenza, Gabriele Costa, Giovanni Lagorio

**WAF-A-MOLE: AN ADVERSARIAL TOOL FOR ASSESSING ML-BASED WAFS**  SOFTWAREX 2020  
Andrea Valenza, Luca Demetrio, Gabriele Costa, Giovanni Lagorio

**ZENHACKADEMY: ETHICAL HACKING@ DIBRIS.**  CSEDU 2019  
Luca Demetrio, Giovanni Lagorio, Marina Ribaudò, Enrico Russo, Andrea Valenza

**EXPLAINING VULNERABILITIES OF DEEP LEARNING TO ADVERSARIAL MALWARE BINARIES**  ITASEC 2019  
Luca Demetrio, Battista Biggio, Giovanni Lagorio, Fabio Roli, Alessandro Armando

## PREPRINTS

**INDICATORS OF ATTACK FAILURE: DEBUGGING AND IMPROVING OPTIMIZATION OF ADVERSARIAL EXAMPLES**  ARXIV 2021  
Maura Pintor, Luca Demetrio, Angelo Sotgiu, Giovanni Manca, Ambra Demontis, Nicholas Carlini, Battista Biggio, Fabio Roli

**SECML-MALWARE: PENTESTING WINDOWS MALWARE CLASSIFIERS WITH ADVERSARIAL EXAMPLES IN PYTHON**  ARXIV 2021  
Luca Demetrio, Battista Biggio

## TALKS

**MLDM - AIXIA, 2021** Adversarial EXEmples: Functionality-preserving Optimization of Adversarial Windows Malware

**Huawei AI4Sec, 2021** Adversarial EXEmples: Functionality-preserving Optimization of Adversarial Windows Malware

**Alan Turing Institute, 2021** Adversarial EXEmples: Functionality-preserving Optimization of Adversarial Windows Malware

**S3AI Group, 2021** Formalizing evasion attacks against machine learning Windows malware detectors

**CyberSec&AI, Avast, 2020** Efficient black-box optimization of adversarial windows malware with constrained manipulations

**SAC, 2020** WAF-A-MoLE: Evading Web Application Firewalls through Adversarial Machine Learning

**ITASEC, 2019** Explaining Vulnerability of Deep Learning to Adversarial Windows Malware

## POSTERS

**ICML Workshop, 2021** Poster: Adversarial EXEmples: Functionality-preserving Optimization of Adversarial Windows Malware

**CyberSec&AI, Avast, 2019** Poster: Explaining Vulnerability of Deep Learning to Adversarial Windows Malware

## REVIEWER

### 2021

- Program Committee at the 9th International Conference on Learning Representations (ICLR)
- Program Committee at 14th ACM Workshop on Artificial Intelligence and Security (AISec)
- Program Committee at 35th Conference on Neural Information Processing Systems (NeurIPS)
- Reviewer for IEEE Transactions on Information Forensics and Security (TIFS)

### 2020

- Program Committee at 34th Conference on Neural Information Processing Systems (NeurIPS)
- Reviewer for IEEE Transactions on Information Forensics and Security (TIFS)