Dorjan Hitaj
Curriculum Vitae

Part I – General Information

Full Name	Dorjan Hitaj
Spoken Languages	ALBANIAN, ENGLISH, ITALIAN

Part II – Education

Type	Year	Institution	Notes (Degree)
University graduation	2015	EPOKA University	Bsc in Business Informatics
Post-graduate studies	2018	Sapienza Universita di Roma	Msc in Computer Science
PhD	2022	Sapienza Universita di Roma	Phd in Computer Science

Part III – Appointments

IIIA – Academic Appointments

Start	End	Institution	Position
Feb 2022	--------	Sapienza University of Rome	PostDoc Researcher

Part IV – Teaching experience

Year	Institution	Lecture/Course
a.y 22/23	Sapienza University of Rome	Sistemi Operativi – Modulo 1 (Unitelma)

Part V - Society memberberships, Awards and Honors

Year	Title
2015	Certificate of Achievement, Ranked 1st in the Graduating Class of 2015, Bachelor Program in Business Informatics, Epoka University.
2015	High Academic Honour Certificate, for excellent performance during studies of Bachelor in Business Informatics, Epoka University.
2019	High Academic Honour Certificate (Laureato Eccellente), for being among the best graduates of the academic year 2017-2018, Sapienza University of Rome
2020	Premio di Laurea, prize for being among the best graduates of the academic year 2017-2018 in the Lazio region, LazioDiSCO
2022	Premio per ricercatori e assegnisti di ricerca, prize for young researchers in the Lazio region.

Part VI - Funding Information [grants as PI-principal investigator or I-investigator]

Year	Title	Program
2020	Gen4Olive (I)	EU HORIZON 2020

2020	Avvio alla Ricerca Type I (I)	Bandi Ricerca Sapienza
2021	Avvio alla Ricerca Type II (I)	Bandi Ricerca Sapienza
2022	Avvio alla Ricerca Type II (I)	Bandi Ricerca Sapienza

Part VII – Research Activities

Keywords	Brief Description
cybersecurity	I am a researcher in cybersecurity, with a focus on Machine Learning applications to cybersecurity and secure Machine Learning algorithms. During both my master and Phd studies I have focused on the intersection of these two fields developing new ideas on applications of machine learning in cybersecurity for tasks such as ransomware detection, data forensics, password guessing, spam prevention and on the other direction thus applications of cybersecurity concepts tailored to machine learning such as DNN intellectual property protection, steganography in DNN models, covert communication over federated learning and more.
Machine learning	
Deep learning	

Part VIII – Summary of Scientific Achievements

Product type	Number	Data Base	Start	End
Papers [international]	9	scopus	Nov2018	2022

Total Citations	54
Average Citations per Product	6
Hirsch (H) index	4
Normalized H index*	1

*H index divided by the academic seniority.

Part IX– Selected Publications

List of the publications selected for the evaluation. For each publication report title, authors, reference data, journal IF (if applicable), citations, press/media release (if any).

1. Dorjan Hitaj, Briland Hitaj, and Luigi V. Mancini. Evasion Attacks Against Watermarking Techniques found in MLaaS Systems. *IEEE International Conference on Software Defined Systems*, 2019 (citations 15)
2. Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. The Naked Sun: Malicious Cooperation Between Benign-Looking Processes. *ACNS 2020: 18th International Conference on Applied Cryptography and Network Security*. (citations 10)
3. Dorjan Hitaj, Briland Hitaj, Sushil Jajodia, and Luigi V. Mancini. Capture the Bot: Using Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks. *IEEE Intelligent Systems*, 2020. (citations 3)
4. Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. EnCoD: Distinguishing Compressed and Encrypted File Fragments. *14th International Conference on Network and System Security*, 2020. (citations 13)
5. Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. Evading Behavioral Classifiers: A Comprehensive Analysis on Evading Ransomware Detection Techniques. *Neural Computing and Applications*, 2022. (citations 4)

6. Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. Reliable Detection of Compressed and Encrypted Data. *Neural Computing and Applications*, 2022. (citations 5)
7. Giulio Pagnotta, Dorjan Hitaj, Fabio De Gaspari, and Luigi V. Mancini. PassFlow: Guessing Passwords with Generative Flows. *The 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2022. (citations 3)
8. Dorjan Hitaj, Giulio Pagnotta, Briland Hitaj, Luigi V. Mancini, and Fernando Perez-Cruz. MaleficNet: Hiding Malware into Deep Neural Networks using Spread-Spectrum Channel Coding. *27th European Symposium on Research in Computer Security (ESORICS)*, 2022. (citations 0)