


## PERSONAL INFORMATION

## Doina Cosovan

 4B, Socola, 700186 Iasi (Romania)

 +40 748362115

 doina.cosovan@gmail.com

 Skype cosovan.doina

Sex Female | Date of birth 04/02/1988 | Nationality Romanian

## WORK EXPERIENCE

06/2010–04/2015

## Senior Malware Researcher

Bitdefender, Iasi (Romania)

- virus disinfection

- adding malware detection

- malware analysis / reverse engineering

- training new people on reverse engineering and malware detection

- developing a sinkhole system from scratch and reverse engineering and implementing DGAs for sinkholing

- analyzing some pieces of malware in order to collaborate with BitDefender's communication team, responsible for writing technical articles; this resulted in more than 50 articles being published on labs.bitdefender.com, hotforsecurity.com (known in the past as malwarecity.com).

- researching, implementing, writing papers regarding botnet analysis and machine learning techniques for malware detection and presenting them at conferences:

\* "A Comparative Study of Malware Detection Techniques Using Machine Learning Methods", 18th International Conference on Information Systems Security (ICISS)

\* "A Practical Guide for Detecting JavaScript-based Malware using Hidden Markov Models and Linear Classifiers", International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)

\* "In-depth Analysis of PushDO Botnet", Association of Anti-Virus Asia Researchers (AAVAR)

\* "The money behind the ransomware botnets", CyberSecurity Summit, 17th International Conference on Information Systems Security

\* "Practical Aspects Related to Botnet Analysis", The Doctoral Summer School on Evolutionary Computing in Optimisation and Data Mining (ECODAM)

\* "Sinkholing botnets", The Doctoral Summer School on Evolutionary Computing in Optimisation and Data Mining (ECODAM)

04/2015–Present

## Senior Malware Researcher

Security Scorecard Inc., Iasi (Romania)

- finding samples with great probability of containing DGAs, reverse engineering those samples to extract and implement the DGAs for sinkholing

- extracting NXDOMAINS from malicious samples for sinkholing

- automating seed extraction for known DGAs by implementing plugins for Immunity Debugger

- setting up open relays and honeypots

- implementing behavior-based javascript detection using PhantomJS and hooks

## EDUCATION AND TRAINING

01/10/2013–Present

## PhD

Faculty of Computer Science, University Alexandru Ioan Cuza, Iasi (Romania)  
 Theme: "Machine Learning Techniques for Threat Detection"

01/10/2011–30/07/2013 **MSc**  
 Faculty of Computer Science, University Alexandru Ioan Cuza, Iasi (Romania)  
 Theme: "Distributed systems"  
 Dissertation: "Sinkholing Botnets"

01/10/2008–30/07/2011 **BSc**  
 Faculty of Computer Science, University Alexandru Ioan Cuza, Iasi (Romania)  
 Thesis: "Attacks on SSL/TLS"

01/10/2004–30/06/2008 **High School**  
 Garabet Ibraileanu, Iasi (Romania)

01/09/1996–30/06/2004 **Secondary School**  
 Iulia Hasdeu, Chisinau (Moldova)

PERSONAL SKILLS

Mother tongue(s) Romanian

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	B2	B2	B2	B2	B2
Russian	C1	C1	B2	B1	B1
Spanish	A2	A2	A2	A2	A2

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user  
 Common European Framework of Reference for Languages

**Organisational / managerial skills** as a collaborator of Faculty of Computer Science in Iasi, I conducted laboratories of Functional Programming (Haskell), Introduction to Programming (C), Advanced Programming Techniques (Java), and Genetic Algorithms;

**Job-related skills** Programming Languages: Assembler x86/IA64, Python, C/C++, C#, Java  
 Knowledge/Skills: reverse engineering, malware analysis, Windows API, executable structure

**Digital competence** IDA Pro, HexRays, Olly Debugger, Immunity Debugger