Europass
Curriculum Vitae

Personal information

First name(s) / Surname(s)	**Dan Horea Luțaș**
E-mail(s)	dan_lutas@yahoo.com
Nationality	Romanian
Date of birth	1982
Gender	Male

Work experience

Dates	**01/04/2019 →**
Occupation or position held	**Senior Technical Manager**
Main activities and responsibilities	Technical Manager for Bitdefender's Active Threat Defense (ATD) a proactive, run-time, behavior-based malware detection technology and Anti-Exploit technologies.
Name and address of employer	S.C. BitDefender SRL Bucharest (Romania)
Type of business or sector	Information Security

Dates	**01/06/2016 →**
Occupation or position held	**Technical Project Manager**
Main activities and responsibilities	Technical Manager for Bitdefender's Anti-Exploit technology. I was involved in designing and implementing a standalone SDK that detects various binary exploitation techniques on Windows OSes (user-mode and kernel-mode). Involved in researching new / emerging binary exploitation techniques and adding detection for those techniques in the Anti-Exploit module. Managed initially a team of two developers and grew it over the years to eight.
Name and address of employer	S.C. BitDefender SRL Bucharest (Romania)
Type of business or sector	Information Security

Dates	**01/07/2012 → 01/06/2016**
Occupation or position held	**Senior Research Lead**

Main activities and responsibilities

Coordinating a research team on hypervisor development and hypervisor based introspection technologies for advanced anti-malware protection

Experience in
- extensive experience on Microsoft NT OS internals (performed analysis of kernel-mode malware, rootkits)
- experience in Linux OS internals (kernel mode, device drivers) – customizing a specialized Linux kernel for loading in a virtual machine on a dedicated hypervisor
- extensive experience in development of hypervisor technologies (memory management, virtual cpu scheduling, interrupt management, device interfacing, timers, different hypervisor loading scenarios)
- Intel VT-x, EPT / NPT, VT-d, TXT, AMD SVM

Name and address of employer

S.C. BitDefender SRL
Bucharest (Romania)

Type of business or sector

Information Security

Dates **01/03/2009 → 01/07/2012**

Occupation or position held **Proactivity And Kernel Research Software Development Lead**

Main activities and responsibilities

Maintanance and development of the Anti-Rootkit module of BitDefender. Involves analyzing kernel mode rootkits and adding detection techniques, and providing low-level functionality (such as raw disc access / raw windows registry access) to help in removing a rootkit once it is detected.
Development of a thin hypervisor, using the hardware virtualization support of Intel and AMD CPUs. This is part of the Active Virus Control technology of BitDefender.

Experience in
- extensive experience on Microsoft NT OS internals (performed analysis of kernel-mode malware, rootkits)
- Intel VT-x, VT-d, AMD SVM (developed a lightweight hypervisor for Intel VT-x and AMD SVM)

Name and address of employer

S.C. BitDefender SRL
Bucharest (Romania)

Type of business or sector

Information Security

Dates **01/07/2007 - 28/02/2009**

Occupation or position held **Proactivity & Kernel Research Developer**

Main activities and responsibilities

I was involved in developing the core modules of Active Virus Control technology of BitDefender, which is directed at dynamic detection of malware (at runtime). The technology works by monitoring, in real time, the behaviour of a running process and altering (and possibly terminating) it if it exhibits actions that may compromise the system. This is all done intelligently without requiring any user intervention. My work included developing both kernel-mode and user-mode components for this technology.

Experience in
- Win32 API Programming (C)
- Windows Kernel-mode device drivers : file-system minifilters, registry minifilters, function drivers for virtual hardware
- Extensive experience with WinDbg user/kernel debugger - attended "Kernel Debugging and Crash Analysis For Windows" OSR course in 2010.
- extensive experience on Microsoft NT OS internals (performed analysis of kernel-mode malware, rootkits)

Name and address of employer

S.C. BitDefender SRL
Bucharest (Romania)

Type of business or sector

Information Security

Dates **01/05/2005 - 30/06/2007**

Occupation or position held **Virus Researcher**

Main activities and responsibilities

As a virus researcher, my role was to disassemble and analyze new viruses in order to understand the way they function and spread and extracting a signature for a virus, that is incorporated in products and it is used to protect the Bitdefender clients. MAIN DUTIES: Disassembling and rolling of malware in controlled environment, development of internal tools and generic detection routines, analyzing the evolution of viruses and studying new platforms (AMD64 / IA64 / ARM.) in order to foresee and prevent

	informatic threats - experience in reverse engeneering - experience in ASM for x86 and x64. - experience in C (specialized removal routines)
Name and address of employer	BitDefender SRL Bucharest (Romania)
Type of business or sector	Information Security
Dates	**01/05/2002 - 30/04/2005**
Occupation or position held	**Software Developer**
Main activities and responsibilities	- bug fixing and adding features to a suite of C applications running under VMS OS. - porting parts of the suite from VMS to Unix (Solaris) and Windows(NT) - database programming and administration (Oracle 7, 9, 10g AS) - developing multi-tier applications using Struts / JSP, Servlet (Oracle 10g AS)
Name and address of employer	Net Brinel SRL Cluj Napoca (Romania)
Type of business or sector	Information Technology

Education and training

Dates	**2016**
Title of qualification awarded	**PhD in Computers and Information Technology, thesis title *"Contributions to the improvement of cyber-incident response process by using hardware virtualization technologies"***
Name and type of organisation providing education and training	Technical University of Cluj Napoca Cluj Napoca (Romania)
Dates	**2006 - 2008**
Title of qualification awarded	**Master of Science**
Name and type of organisation providing education and training	Technical University of Cluj Napoca Cluj Napoca (Romania)
Dates	**2001 - 2006**
Title of qualification awarded	**Engineer, Computer Science**
Name and type of organisation providing education and training	Technical University Of Cluj Napoca Cluj Napoca (Romania)

Personal skills and competences

In 18+ years of experience in Information Security, I tried to grasp many aspects of this complex topic – technical (operating systems internals, networking, hypervisor technologies), non-technical (auditing of information systems, security management), defensive (malware analysis, development of advanced detection and prevention technologies) and offensive (penetration testing) – in order to have a holistic view of the domain.

Professional Certifications :

- CISSP – Certified Information Systems Security Professional (expired)
- CEH v7 – Certified Ethical Hacker version 7
- CISA - Certified Information Systems Auditor (expired)
- OSCP – Offensive Security Certified Professional
- Passed exam for CISM (Certified Information Security Manager – ISACA)
- OSCE – Offensive Security Certified Expert

Courses :

- attended "Kernel Debugging and Crash Analysis For Windows" OSR course in 2010
- attended "Advanced Windows Exploitation" course by Offensive Security in 2015

Teaching :

- taught laboratories for the *Operating Systems* (2008) and *Programming in Assembly Language* (2011) courses at Technical University of Cluj Napoca (UTCN)
- teaching “Information Systems Auditing and Security Risk Management” and “Digital Forensics And Incident Response” master-level courses (in romanian) at SISC Master Program at Technical University of Cluj-Napoca (UTCN)

Author / co-author for 6 US Patents (granted) :

- US Patent Number US10630643 B2 : **D. H. Lutas,** D.I. Ticle, R.I. Ciocas, S. Lukacs, I.C. Anichitei, *Dual memory introspection for securing multiple network endpoints*, 2020
- US Patent Number US8875295 B2 : A. V. LUTAS, S. Lukacs, and **D. H. Lutas**, *Memory Introspection Engine for Integrity Protection of Virtual Machines*, 2014
- US Patent Number US8656482 B1 : R. V. Tosa, S. Lukacs, and **D. H. Lutas**, *Secure communication using a trusted virtual machine*, 2014
- US Patent Number US8910238 B2 : S. Lukacs, **D. H. Lutas**, and R. V. Tosa, *Hypervisor-based enterprise endpoint protection*, 2014
- US Patent Number US9202046 B2 : B.C.Dumitru, S. Lukacs, **D. H. Lutas,** R. V. Tosa, *Systems and methods for executing arbitrary applications in secure environments*, 2015
- US Patent Number US9117081 B2 : S. Lukacs, C. B. SIRB, **D. H. Lutas**, A. V. Colesa, *Strongly isolated malware scanning using secure virtual containers*, 2015

Publications:

- *“Load Value Injection in the Line Fill Buffers: How to Hijack Control Flow without Spectre”*, Andrei Vlad Luțaș, **Dan Horea Luțaș**, Bitdefender Labs Blog, March 10, 2020

- *„Security implications of speculatively executing segmentation related instructions on Intel CPUs*”, **Dan Horea Luțaș,** Andrei Vlad Luțaș, Bitdefender Labs Blog, Aug 6, 2019

- *„Bypassing KPTI Using the Speculative Behavior of the SWAPGS Instruction”*, Andrei Vlad Luțaș, **Dan Horea Luțaș,** Bitdefender Labs Blog, Aug 6, 2019, BlackHat Europe, 2019

- "*Secure Virtual Machine for Real Time Forensic Tools on Commodity Workstations*", **Dan Horea Luțaș**, Adrian Coleșa, Sándor Lukács, Andrei Luțaș, SECITC 2016, International Conference on Information Technology And Communications Security, June 9-10 2016, Bucharest

- "*Towards secure network communications with clients having cryptographically attestable integrity*", **Dan Horea Luțaș**, Sándor Lukács, Raul Vasile Toșa, Andrei Vlad Luțaș in PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A, Volume 14, Special Issue 2013, pp. 338–356 - RCD-2013

- “*Hardware Virtualization Based Security Solution for Embedded Systems*”, Lukacs, Sandor; Lutas, Andrei V.; **Lutas, Dan H.**; Sebestyen, Gheorghe, in 2014 IEEE INTERNATIONAL CONFERENCE ON AUTOMATION, QUALITY AND TESTING, ROBOTICS, DOI 10.1109/AQTR.2014.6857879

- "*Proposed Processor Extensions for Significant Speedup of Hypervisor Memory Introspection*", Andrei Luțaș, Sándor Lukács, Adrian Coleșa and **Dan Luțaș**, 8th International Conference on Trust & Trustworthy Computing TRUST-2015, Volume 9229 of the series Lecture Notes in Computer Science pp 249-267

- "*U-HIPE: hypervisor-based protection of user-mode processes in Windows*", Andrei Luțaș, Adrian Coleșa , Sándor Lukács, **Dan Luțaș**, Journal of Computer Virology and Hacking Techniques, Volume 12, Issue 1 , pp 23-36

Other research :

- Part of a small Microarchitectural CPU security research team, credited, together with my colleague Andrei Luțaș, with the discovery of the following CPU Vulnerabilities (responsibly disclosed) :
    - A variant of MDS (Microarchitectural Data Sampling) – MFBDS (Microarchitectural Fill Buffer Data Sampling) **CVE-2018-12130 -** Intel Security Advisory**,** Intel Deep Dive on MDS
    - SWAPGS (**CVE-2019-1125**) and Speculative only Segment Loads -Intel CVE-2019-1152 Security Advisory, Microsoft CVE-2019-1152 Security Advisory, Intel Deep Dive on the issues
    - A variant of LVI (Load Value Injection) **CVE-2020-0551 -** Intel CVE-2020-0551 Security Advisory, Intel Deep Dive on LVI
- Microsoft **CVE-2018-8174** Security Advisory Windows VBScript Engine Remote Code Execution Vulnerability

Mother tongue(s) **Romanian**

Other language(s)

Self-assessment	**Understanding**				**Speaking**				**Writing**	
European level (*)	Listening		Reading		Spoken interaction		Spoken production			
English	C2	Proficient user	C2	Proficient user	B2	Independent user	B2	Independent user	B2	Independent user

(*) Common European Framework of Reference (CEF) level