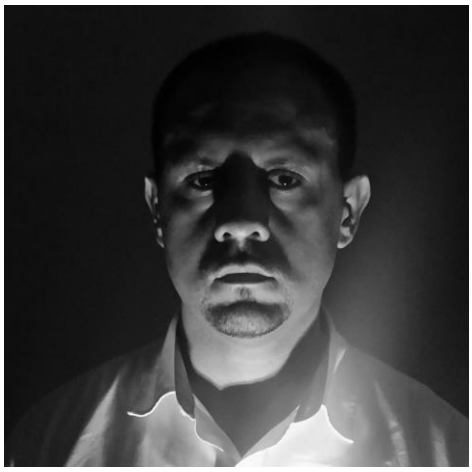

Alexandre Borges

E-mail: alexandreborges@blackstormsecurity.com
E-mail: alex_sun@terra.com.br

blog: http://alexandreborges.org
LinkedIn: http://www.linkedin.com/in/aleborges

Short Profile

Malware Researcher and Consultant in Malware Analysis, Digital Forensics, Memory Forensic Analysis, Exploit Development for Windows, Reverse Engineering.

EC-Council CHFI Advisory Board Member

Reviewer of The Journal of Digital Forensics, Security and Law -- http://www.jdfsl.org/

Referee on Digital Investigation
The International Journal of Digital Forensics & Incident Response
http://www.journals.elsevier.com/digital-investigation/editorial-board

Author of articles on Oracle Technical Network (OTN) and Oracle Solaris 11 Advanced Administration Cookbook book.

Speaker in Conferences

Oracle ACE. ISC2 (CISSP), Oracle, EC-Council instructor.

General Professional Skills

- **Malware Analysis**
- **Memory Forensic Analysis by using Volatility**
- **Digital Forensic Analysis (postmortem)**
- **Reversing Engineering**
- **Windows Internals**
- **Linux Kernel**
- **Windows Crash Dump Analysis**

- **Software Exploitation for Windows (DEP, ASLR, Safe SHE, ROP, Heap Spraying, and so on)**

- **C/C++ language**
- **Python**

- **Hacking (as pentester)**

- **Oracle Instructor**
- **EC-Council Instructor**
- **(ISC)2 CISSP Instructor**
- **Former Symantec Instructor**

- **EC-Council CHFI Advisory Board Member**
- **Reviewer of The Journal of Digital Forensics, Security and Law**
- **Referee on Digital Investigation: The International Journal of Digital Forensics & Incident Response**

- **OTN Writer**

- **Author of the book Oracle Solaris 11 Advanced Administration Cookbook**

Academic

Information Technology – Pontifícia Universidade Católica -PUC (complete)
Physics – University of Sao Paulo - USP (incomplete)

Professional History

AUG/2015– today **BlackStormSecurity**
(Malware Researcher, Consultant and Speaker)

Main achievements: Handling malware infection cases during critical operations and enabling companies to improve their knowledge about Malware Analysis, Memory Analysis, Digital Forensics, Reverse Engineering, Software Exploitation for Windows and Windows Crash Dump Analysis and Hacking.

Job Description: I have worked on Malware Analysis, Digital Forensics and Reverse Engineering as consultant.

My experience and work at BlackStorm composed by skills such as:

- Initial incident handler approach
- Memory analysis by using Volatility
- Dynamic Analysis by using debuggers and emulators
- Static Analysis using IdaPro and Radare2
- Knowledgement in IDA Python and IDC
- C and C++ Programming for reversing
- Python programming

- Exploit Development for Windows
    - DEP
    - ASLR
    - GS
    - SafeSEH
    - Shellcoding
    - ROP
    - Heap Overflow
    - mona!

- Assembly programming
- Windows Kernel
- Windows System Programming
- Processor concepts.
- Unix System Programming
- Device Drivers concepts
- Postmortem forensics analysis (disk and network) by using filesystem analysis, Windows Registry Forensics (RegRipper), timelines, shadow copies, and so on.
- Anti-Forensic tricks such as:

    - Malware Stealth: process injection, DLL Injection, Hook Injection, Hollowing, APC Injection, DLL Load-Order Hijacking, IAT Hooking, EAT Hooking
    - Rootkits techniques such as SSDT hooking, IDT hooking, GDT hooking, Detours, DKOM, Kernel Callbacks,
    - Anti-debugging techniques
    - Anti-disassembly techniques
    - Anti-VM techniques
    - Packers
    - Shellcode

Additionally, I've spoken at few companies, conferences and universities about Memory Analysis (Volatility) and Malware Analysis such as:

- **SBS Consultores and BNP-PARIBAS / Cardif (Malware and Memory Analysis)**

- **Hackers to Hackers Conference 2016 (H2HC), FutureCom 2016, GUOB Tech Day 2016, Oracle Open World 2016 Latin America, BSIDES LATAM 2016, (ISC)2/Kafinet Information Security Trends 2016, (ISC)2 Security Congress Latam, Hacker To Hackers Conference University (H2HC) 2015, MindTheSec Conference 2015 and SecureBrasil Conference (Malware and Memory Analysis)**

- **Universidade de Santos, PUC Campinas, USCS (Universidade de Sao Caetano do Sul), UniSanta University, UNASP SP University, Uninove University, PUC-SP University, FMU University, UNASP Centro Universitário Adventista de São Paulo, Instituto Tecnológico da Aeronáutica (ITA) , Unimonte Universitiy, UnG (Guarulhos University), PUC SP University, UNISA University, BandTec University, FATEC Santos (Malware Analysis, Memory Analysis and Hacking)**

NOV/2016 – today **Referee on Digital Investigation The International Journal of Digital Forensics & Incident Response**

website: http://www.journals.elsevier.com/digital-investigation/editorial-board

Main role: I am reviewer of articles about Malware Analysis, Digital Forensics and Reversing.

NOV/2016 – today **Reviewer of The Journal of Digital Forensics, Security and Law**

website: http://www.jdfsl.org/

Main role: I am reviewer of articles about Malware Analysis, Digital Forensics and Reversing.

JUL/2010 – Aug/2015 - SECURITYHACK SERVICES

Malware Researcher and Consultant in Malware Analysis, Memory Forensic Analysis, Reverse Engineering, Digital Forensics Analysis , Hacking, Software Exploitation.

Main achievements: Malware Analsys, Memory Forensic Analysis, Memory Forensics, Software Exploitation, Hacking, Reversing and Forensics courses.

My experience, work and and knowledgment at Securityhack is composed by:

- Memory analysis by using Volatility
- Dynamic Analysis by using debuggers.
- Static Analysis using IdaPro.
- Knowledgement in IDA Python and IDC
- C and C++ Programming for reversing
- Python and Perl programming
- Assembly programming
- Windows Kernel
- Windows System Programming

- Exploit Development for Windows
    - DEP
    - ASLR
    - GS

    - SafeSEH
    - Shellcoding
    - ROP
    - Heap Overflow
    - mona!

- Unix System Programming
- Device Drivers concepts
- Postmortem forensics analysis (disk and network) by using filesystem analysis, Windows Registry Forensics (RegRipper), timelines, shadow copies, and so on
- Anti-Forensic tricks such as:
    - Malware Stealth: process injection, DLL Injection, Hook Injection, Hollowing, APC Injection, DLL Load-Order Hijacking, IAT Hooking, EAT Hooking
    - Rootkits techniques such as SSDT hooking, IDT hooking, GDT hooking, Detours, DKOM, Kernel Callbacks., and so on.
    - Anti-debugging techniques
    - Anti-disassembly techniques
    - Anti-VM techniques
    - Packers
    - Shellcode

JAN/2001– today ORACLE/SUN MICROSYSTEMS BRAZIL
(Contracted IT Instructor and Consultant)

Main achievements: Enabling Oracle/Sun Education to increase their profits, eficiency and quality on training delivery well as teaching clients and partners on main Sun/Oracle technologies.

Job Description: Responsible for teaching all Oracle courses (Solaris, Oracle Database, MySQL, Oracle Servers)

MAY/2009 – OUT/2015 SYMANTEC DO BRASIL
(Contracted Instructor)

Main achievements: Helping Symantec to consolidate as the main company on Backup and Cluster software, well as enabling clients and partners to know about the main Symantec technologies and to understand how to use them in a appropriated scenarios, decreasing the wasted time in a project deployment.

Job Description: I taugh classes about NetBackup, Veritas Cluster, Storage Foundation, Backup Exec, Global Cluster Option (GCO), VVR (Veritas Volume Replicator), SF CFS (Storage Foundation Cluster File System) and Security Endpoint Protection (SEP).

MAY/2014 – today (ISC)2 CISSP INSTRUCTOR

Main achievements: Training (ISC)2 clients to improve their experience and enable them to take the CISSP exam.

OCT/2014 – Author of Oracle Solaris 11 Advanced Administration Cookbook

website: http://alexandreborges.org/2014/10/13/my-book-about-oracle-solaris-11-advanced-administration/

AUGUST/2013 – today ORACLE TECHNICAL NETWORK (OTN) WRITER

Job Description: Author of articles on OTN (Oracle Technical Network)

Main achievements: Spreading the view about Solaris as being the best operating of the world well as encouraging and teaching readers to use and deploy Oracle Solaris 11 in order to increase the eficiency and profit in their companies.

Published Articles:

http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris-install-borges-1989211.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris11-net-svcs-ips-2086656.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/comstar-zfs-virtualized-storage-2159053.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/monitor-swap-solaris-zfs-2216650.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris-zfs-dataset-2227061.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris-zfs-encryption-2242161.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris-zfs-snapshots-2254189.html
http://www.oracle.com/technetwork/articles/servers-storage-admin/solaris-zfssmb-sharing-2390458.html
https://community.oracle.com/docs/DOC-912067
https://community.oracle.com/docs/DOC-912496
https://community.oracle.com/docs/DOC-914874
https://community.oracle.com/docs/DOC-922240
https://community.oracle.com/docs/DOC-991968
https://community.oracle.com/docs/DOC-1004909
https://community.oracle.com/docs/DOC-1004910

JAN/2011-today **STRONG SECURITY**
(Contracted EC-Council Instructor)

Main achivement: Enabling Strong Security to increase their profit as well to spread their brand among main IT security professionals.

Job Description: I've taught classes as Certified ECCouncil Instructor for clients about Ethical Hacker (CEH) and ECSA v8 and v9.

MAY/2009- APR/2014 **LINUX MAGAZINE BRAZIL**
(Columnist and Author of Articles)

Main achievements: Getting Linux Magazine more known among IT professionals well as motivating readers to try and search new technologies using simple procedures.

Job Description: I wrote about several themes like OpenSolaris, Linux Kernel, Security,

C programming, Performance, etc...

Courses

- **Windows Malware and Memory Forensic Training – taught my Michael Ligh, Jamie Levy and Andrew Case from Volatility Group (Reston / VA / USA)**

- **Corelan Advanced Exploit Development course – taught by Peter van Eeckhoutte – DerbyCon 2015 in Louisville (Kentucky – USA)**

- **Special Topics in Malware Analysis (Mandiant/FireEye - Black Hat USA 2015) in Las Vegas (USA)**

- **VMware vSphere: Install, Configure, Manage [V4]**
- **Brocade Trainer the Trainers (CFA and CFP)**
- **Brocade Trainer the Trainers (Protocols and BPIPA)**

International Trips

Black Hat 2015 – USA (Las Vegas) – training
DerbyCon 2015 - USA (Louisville – Kentucky) – training
Volatitility Group – USA (Reston / Virginia)
USA (California) and Argentina (Buenos Aires) – Training
Venezuela (Caracas) – Teaching Class (in english)

Certifications

ORACLE ACE in SOLARIS

Sun Microsystems Instructor of the Year (fy 2003-2004) ;
Sun Microsystems Instructor of the Year (fy 2004-2005) ;

Sun Solaris 7,8, 9 e 10 Certified System Administration
Sun Solaris 8, 9 e 10 Systems Administrator Network
Sun Certified Data Management Engineer with Veritas Volume Manager
Sun Certified Security Administrator for the Solaris Operating System 9 and 10
Sun Certified Engineer for Sun One Directory Server
Sun Certified System Administrator for Sun Cluster 3.2 Software
Sun Certified Solaris Associate

Oracle Certified Associate, MySQL 5.0/5.1/5.5
Oracle Certified Professional, MySQL 5.0 Developer
Oracle Certified Professional, MySQL 5.0 Database Administrator
Oracle Certified Expert, MySQL 5.1 Cluster Database Administrator

Oracle Certified Associate 9i

CommVault Certified for Administrator v.9

Brocade Certified Administration Gen 5- Certificate Verification Number: TK88WDECBF4110F1

Oracle Solaris 11 System Administration

VMware Certified Professional 4.1 (VCP 4.1) - Certification #: 94636
VMware Certified Professional 5.1 (VCP 5.1) - Certification #: 94636

Certified Ethical Hacker (CEH-v.6) - membership ID: ECC944163
Certified Ethical Hacker (CEH-v.7) - membership ID: ECC957814
Certified Ethical Hacker (CEH-v.8) - membership ID: ECC957398
Computer Hacking Forensic Investigator (CHFI-v4) - membership ID: ECC944017
CompTIA Security+ ce – Carreer ID: COMP001020238221

Certified Chief Information Security Officer (C|CISO)
EC-Council Certified Security Analyst (ECSAv8)
EC-Council Certified Network Defense (CND)

Certified Information Systems Security Professional (CISSP) - Certificate/ID number:377249

CERTIFIED EC-COUNCIL INSTRUCTOR (CEI) – membership ID: ECC944163

Data Protection Administration for Unix using NetBackup 6.5
Veritas Storage Foundation 5.0 Administration for Unix

Administration of Symantec NetBackup 7.0 for Unix
Administration of Symantec NetBackup 7.0 for Windows
Administration of Symantec Backup Exec 2010 for Windows
Symantec Backup Exec 2012 Administration Certified

RHCSA 6 (Red Hat Certified System Admnistrator)
Administration of Symantec NetBackup 7.5 for Unix Symantec
Administration of Symantec NetBackup 7.5 for Windows Symantec
Administration of Veritas Storage Foundation 6.0 for Unix Symantec
Administration of Veritas Cluster Server 6.0 for Unix Symantec
Symantec Certified Professional in Storage Management and High Availability for UNIX Symantec

Linux Professional Institute Certified 1 (LPI-1)
Linux Professional Institute Certified 2 (LPI-2)
Novell Certified Linux Administrator (CLA)
Novell Data Center Technical Specialist

Spoken Langauge

Fluent English

Volunteer Work

- **JUN/2015 – AUG/2015 – Team Leader**
  (Cobit Framework 2015 and Errata 2015)

Other Articles

Administering Oracle Linux 7: Part 1—Service Management:
http://www.profissionaloracle.com.br/gpo/artigo/sistema-operacional/525-administering-oracle-linux-7-part-1-service-management

Administering Oracle Linux 7: Part 2—Network Management:
http://www.profissionaloracle.com.br/gpo/artigo/sistema-operacional/526-administering-oracle-linux-7-part-2-network-management

Administering Oracle Linux 7: Part 3 - The systemd Journal:
http://www.profissionaloracle.com.br/gpo/artigo/sistema-operacional/528-administering-oracle-linux-7-part-3-the-systemd-journal

See my personal blog to additional articles:

http://alexandreborges.org