Romain **THOMAS**
Security Engineer

linkedin.com/in/romain-thomas-3b202174 github.com/romainthomas
me@romainthomas.fr romainthomas.fr
Paris, France

Working on the development of tools to automate de reverse engineering process, I also deal with Android reverse engineering, binary instrumentation, training, (de)obfuscation and software protections.

Skills

Operating Systems	Linux, Android
Programming Languages	C++, Python, Java
Assembly	`x86/x86-64`, `ARM (Thumb/Thumb2)`, `AArch64`
Reverse Engineering	IDA, Ghidra, Frida, QBDI, Intel PIN, Jadx, LLVM
Development Tools	vim, CMake, git, Clang, gcc
Misc	LLVM Framework, Pybind11, Android NDK/SDK, Docker, Travis, Appveyor, CircleCI

Work Experience

Present
September 2016

Security Engineer, Quarkslab, Paris
Security engineer at Quarkslab, I deal with the following topics :
- Tools development : LIEF, QBDI, …
- Automating the reverse engineering process
- Android applications diffing
- Dynamic binary instrumentation to address obfuscation
- Reversing engineering on Android applications and obfuscated libraries
- Android internals : ART, ODEX, VDEX, …
- Android Trainer. It covers the following topics :
  - Malware analysis
  - Android Runtime and file formats
  - IPC and Binder
  - Boot process
  - Securities (dm-verity, SELinux, …)
  - Protections (Obfuscation, packer, anti-debug, …)
- Team leader since April 2019

August 2016
January 2016

Intern | LIEF, Quarkslab, Paris
This internship was about the development of LIEF, a library to parse and modify executable file formats. The project has been open-sourced few years later.
- LIEF : lief.quarkslab.com
- Native packer development for ELF and PE formats
- Internship report : www.romainthomas.fr/files/Rapport-Stage-LIEF.pdf

ELF | PE | Mach-O | Packer | Musl libc

July 2015
April 2015

Intern | Obfuscation, Quarkslab, Paris
The topic of this internship was about obfuscation and contribution to the Quarkslab's obfuscator.
- LLVM compiler infrastructure
- Symbolic execution with Triton

Triton | Intel PIN | Control-flow Graph Flattening | Code Coverage

August 2014
July 2014

Intern | JTAG, Quarkslab, Paris
This internship was about JTAG, and more precisely, how to discover JTAG ports on embedded system like routers or 4G internet keys.
- Development of a JTAG testing tool
- Use of Bus Blaster and JTAGulator with the openOCD library

JTAG | JTAGulator | Bus Blaster | Hardware Reverse Engineering

Publication & Conference

"Un EDR sous Android ?" July, 2021

MISC Magazine, To be published

QBDL : QuarkslaB Dynamic Loader June, 2021

SSTIC, https://www.sstic.org/2021/presentation/qbdl_quarkslab_dynamic_loader/

Talk given with Adrien Guinet about QBDL, a library that aims at providing a modular and portable way to dynamically load and link binaries

Dynamic Binary Instrumentation Techniques to Address Native Code Obfuscation October, 2020

Black Hat Asia, https://www.blackhat.com/asia-20/briefings/schedule/#dynamic-binary-instrumentation-techniques-to-address-nativ

This talk introduces DBI-based techniques that can be used to analyze obfuscated code. The first part introduces QDBI features related to code obfuscation while the second part exposes these features through real examples.

A Glimpse Into Tencent's Legu Packer November, 2019

Blog Post, https://blog.quarkslab.com/a-glimpse-into-tencents-legu-packer.html

This blog post deals with the Legu packer, an Android protector developed by Tencent that is currently one of the state-of-the-art solutions to protect APK DEX files. The packer is updated frequently and this blog post focuses on versions 4.1.0.15 and 4.1.0.18.

Android Native Library Analysis with QBDI June, 2019

Blog Post, https://blog.quarkslab.com/android-native-library-analysis-with-qbdi.html

This blog post deals with QBDI and how it can be used to reverse an Android JNI library.

Android Runtime Restrictions Bypass March, 2019

Article, https://www.romainthomas.fr/publication/android-restrictions-bypass/report.pdf

This article is about techniques to bypass Android runtime Restrictions.

Static Instrumentation Based on Executable Formats June, 2018

Recon Montréal, Pass The Salt https://www.romainthomas.fr/publication/slides/18-06-Recon18-Formats-Instrumentation.pdf

Talk given at Recon and Pass the Salt about static instrumentation based on executable formats.

How Triton can help to reverse virtual machine based software protections November, 2016

CSAW SOS, New York https://triton.quarkslab.com/files/csaw2016-sos-rthomas-jsalwan.pdf

Talk given with Jonathan Salwan about Triton and virtual machine based protection.

Dynamic Binary Analysis and Obfuscated Codes April, 2016

St'Hack, https://triton.quarkslab.com/files/sthack2016-rthomas-jsalwan.pdf

Talk given at St'Hack with Jonathan Salwan about Triton and dynamic binary analysis.

How Triton may help to analyse obfuscated binaries September, 2015

MISC Magazine, https://triton.quarkslab.com/files/misc82-triton.pdf

Open-Source Projects

LIEF 2015 - Present

github.com/lief-project/LIEF

Library to parse and manipulate executable formats : ELF, PE, Mach-O.

C++ | Python | CMake | Executable formats

Legu Unpacker 2019

github.com/quarkslab/legu_unpacker_2019

Scripts to statically unpack Android applications protected by Tencent Legu.

Android | Packer | Reverse Engineering

QBDL 2021 - Present

github.com/quarkslab/QBDL

QuarkslaB Dynamic Loader

LIEF | C++ | Python | Loader

Interests

- Obfuscation and software protections
- Protocole reverse engineering
- Tools development
- Mathematics
- Sport : Running and long distance triathlons

Languages

French	●●●●●
English	●●●○○

Education

2016 Engineering degree - ESIEE Paris

2015 Bachelor's degree, Computer Science - École Polytechnique de Montréal

2011 Baccalauréat - Lycée Maurice Ravel