Loria
Laboratoire lorrain de recherche en informatique et ses applications

De l'analyse morphologique à Cyber-Detect : valorisons les virus !

Jean-Yves Marion

institut universitaire de France

Le 6 Novembre 2017 – Jussieu

Jean-Yves Marion
Lorraine University

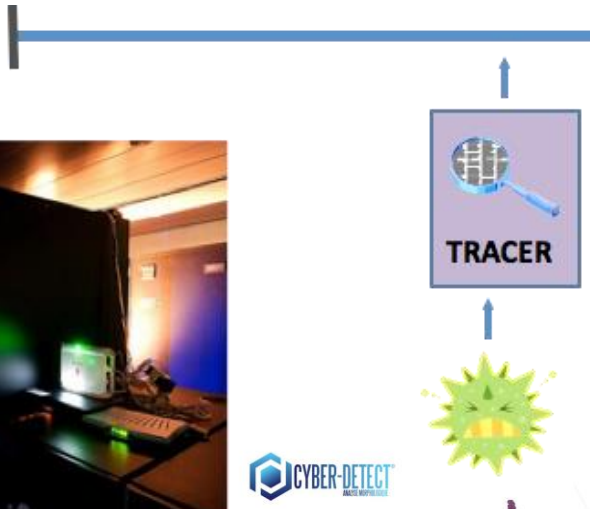
About LORIA@Nancy

- Network security
- Cryptography
- Protocol Security and electronic vote
- Malware
- Scada
- Drones

Research on malware detection

LORIA's High Security Lab

10 millions of malware



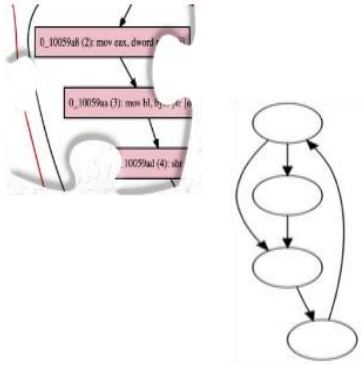
- New approaches to detect malware by morpholigical analysis
- Detection of hidden functionnalities
- Computer forensics

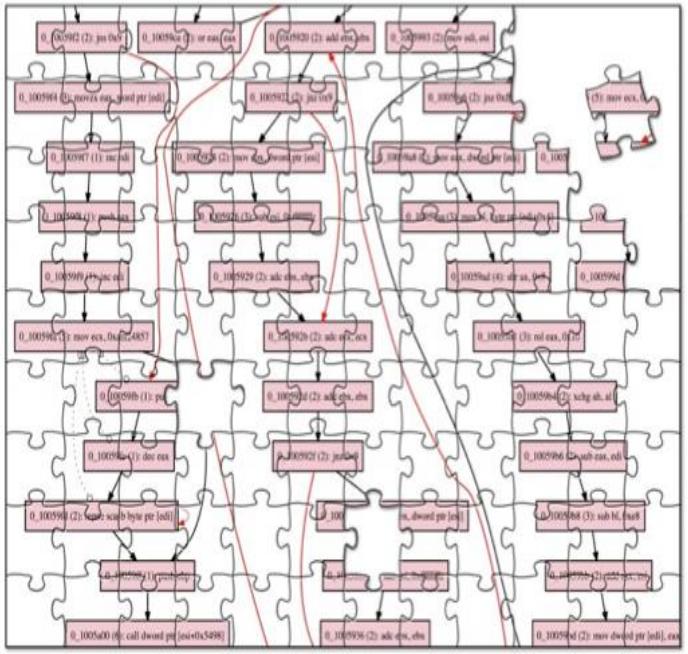
Loria

In a nutshell : **Multi-dimensional Signatures**

Each signature denotes a piece of a functionality

A database of signatures is a collection of functionalities

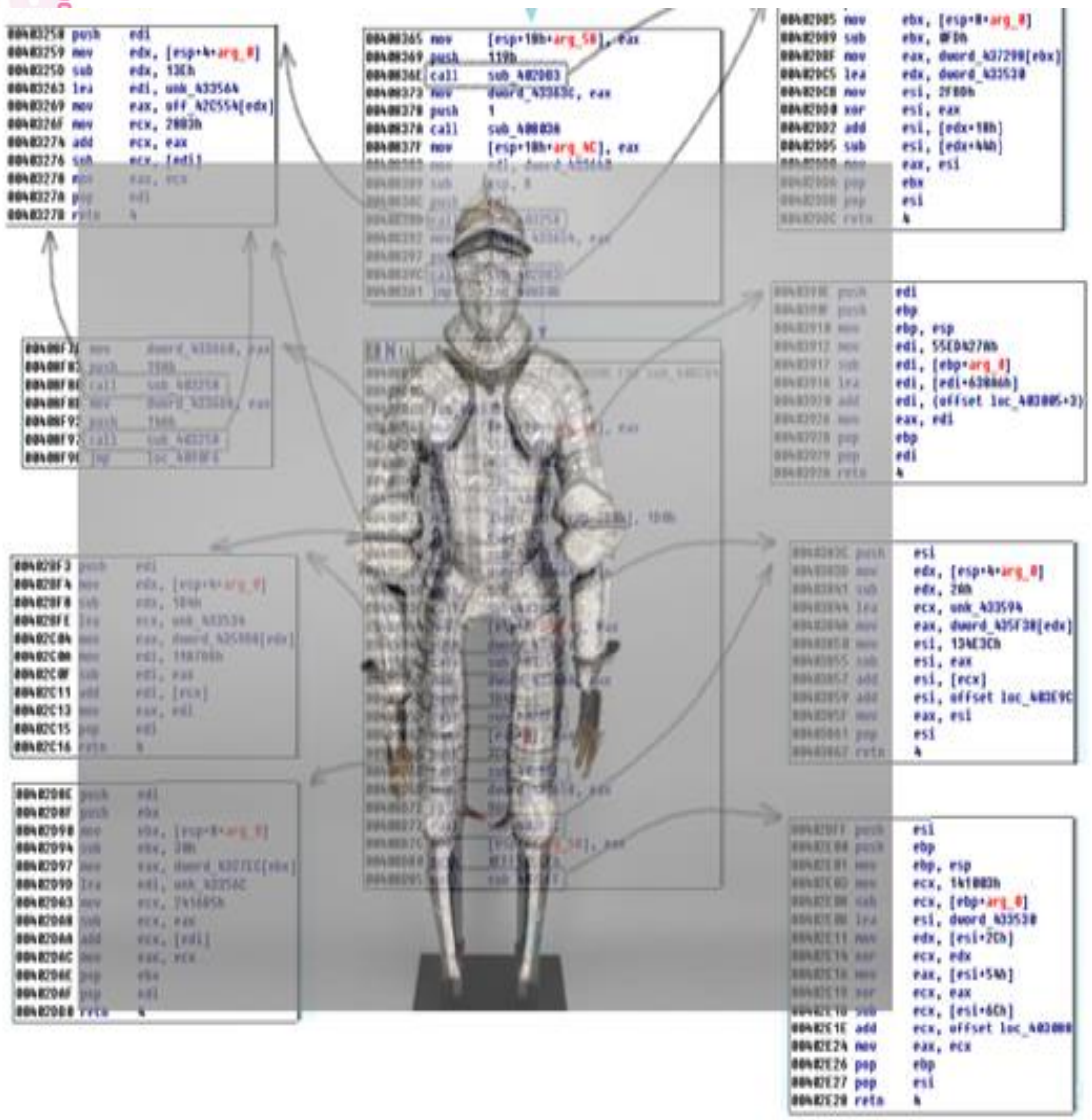




Loria

www.cyber-detect.com

CYBER-DETECT©
MORPHOLOGICAL ANALYSIS



- Obfuscated codes
- Packers
- On the fly code generation
- Anti-debug protections

www.cyber-detect.com

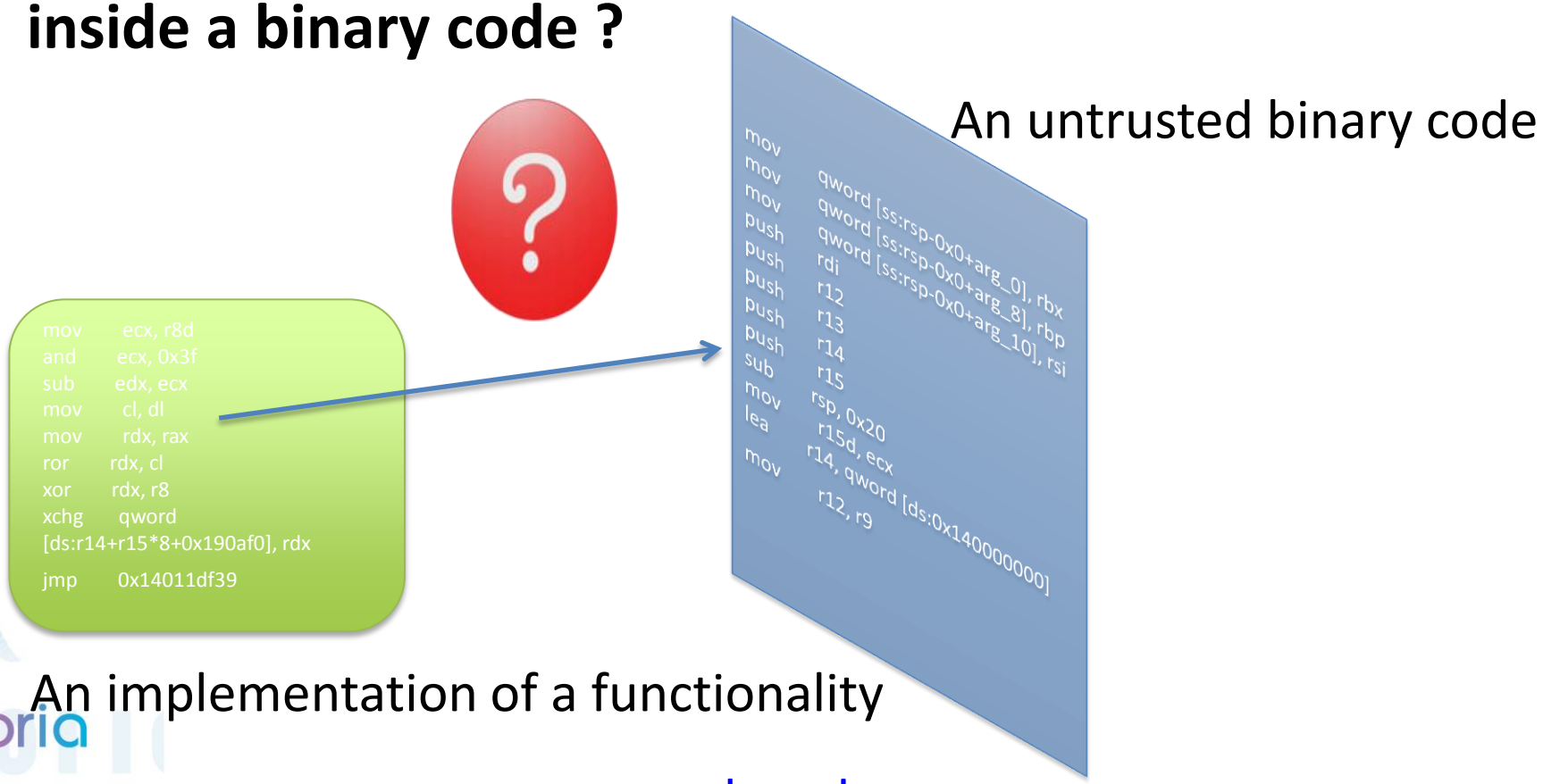
Morphological analysis in a nutshell

Loria

Functionality identification

A scenario

Is the functionality AES Encrypt implemented inside a binary code ?



Loria

www.cyber-detect.com

Functionality identification

CYBER-DETECT©
MORPHOLOGICAL ANALYSIS

The compilation environment

OpenSSL version 1.1.0f
Visual Studio 2013 – 64 bit
Compilation option 01

OpenSSL™
Cryptography and SSL/TLS Toolkit

6 functionalities from demo programs of the OpenSSL distribution

aesni_set_encrypt_key
b64_read
MD5_Update
x86_64_AES_set_encrypt_key
SEH_begin_AES_cbc_encrypt
RC5_32_ecb_encrypt

Goal : Find these 6 functionalities inside Openssl.exe

Loria

Functionality identification

version 1.1.0f VS 2013 64 bit O1	aesccm.exe (version 1.1.0f)		
	aesni_set_encrypt_key	b64_read	MD5_Update
OpenSSL.exe	0x14000cc10 : 0x14000fb10	0x14010c27c : 0x1400feb0c	0x1400af384 : 0x140156e6c

version 1.1.0f VS 2013 64 bit O1	aesgcm.exe (version 1.1.0f)		
	AES_set_encrypt_key	SEH_begin_AES_cbc_encrypt	RC5_32_ecb_encrypt
OpenSSL.exe	0x140002040 : 0x140002040	0x14000251d : 0x14000251d	0x1400b55e0 : 0x14019f2b0

Conclusion

Multi-purpose set of tools to identify similarities between binary codes

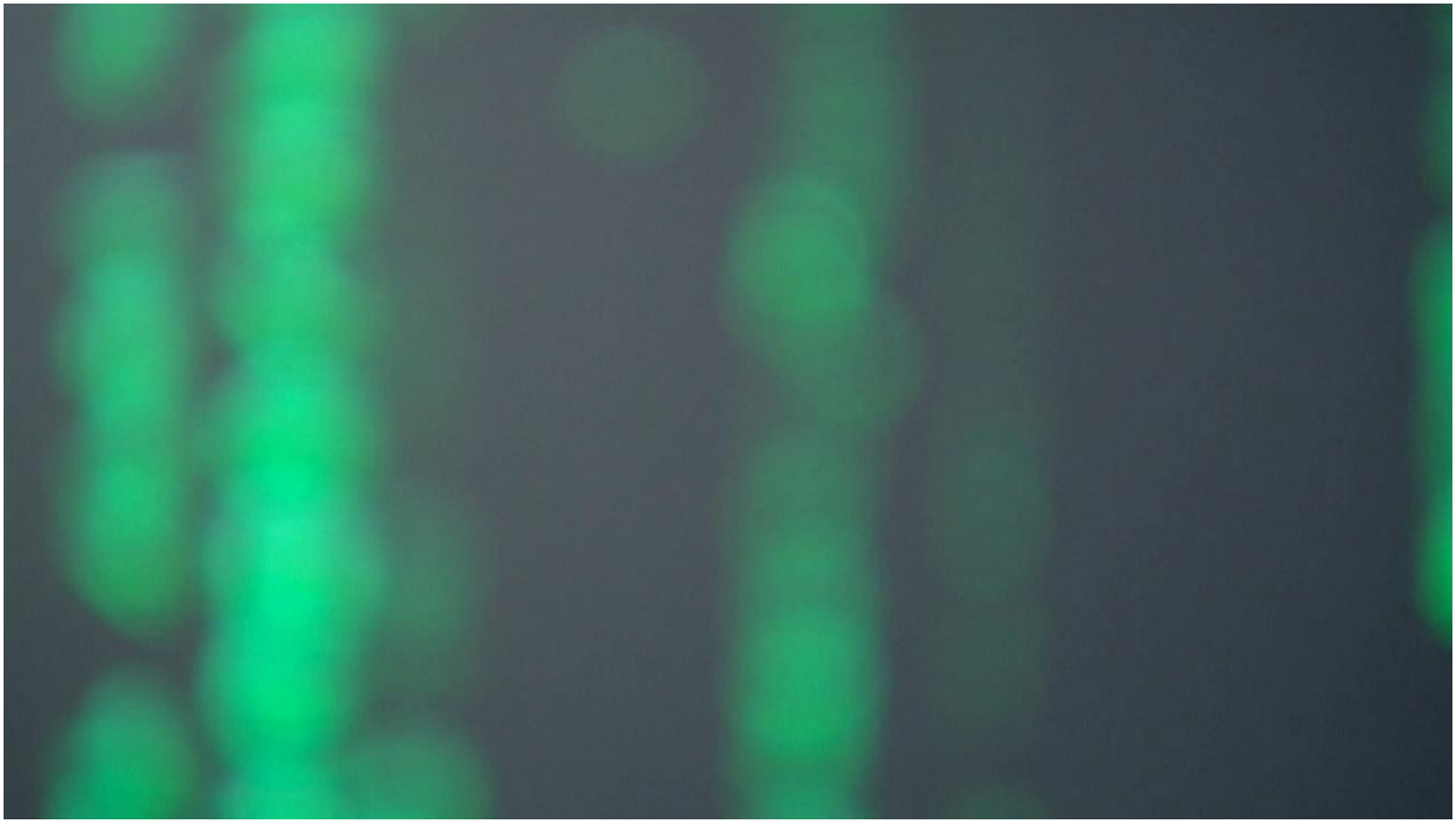
- Works on highly obfuscated X86 (arm) codes
- Fast file investigation
- Speed-up reverse engineering
- Simple Integration (IDA, RPC, Scriptable)

- Accurate with Code synchronization
- Home-made signature data-bases of functionalities

Loria

www.cyber-detect.com

Questions ?



Loria

Thank you !