General information

CYBER-DETECT
In a nutshell :

Laurent Werner
l.werner@cyber-detect.com
06 81 70 81 31

Laurent Werner CEO	Stephane Gegout Chairman of the board	Jean-Yves Marion co-inventor director of LORIA	Guillaume Bonfante co-inventor	Fabrice Sabatier CNRS ingieneer

A LORIA spin-off
A breakthrough technology based on
*'**Morphological Analysis'***
And now used by military administration

is research unit composed of : the University of Lorraine, INRIA and CNRS

Targeted topics

SU-FCT02-2018-2019-2020 subtopic 2	Technologies to enhance the fight against crime and terrorism - subtopic 2: Digital forensics in the context of criminal investigations
SU-FCT02-2018-2019-2020 subtopic 4	Technologies to enhance the fight against crime and terrorism - subtopic 4: Open
SU-GM03-2018-2019-2020	Pre-commercial procurements of innovative solutions to enhance security

Competencies

- *Organisation competencies*
  - World licence of Morphological analysis*© solutions
  - Focus on highly protected, highly obfuscated binary codes
  - Detection of unknown or targeted malwares

- *Organisation experience in the European project*
  - Academic experience (i.e. FP7)

- *The skills you can bring*
  - Fast and scalable comparison of binary code, similarity measurement
  - Functionality identification, algorithm localisation
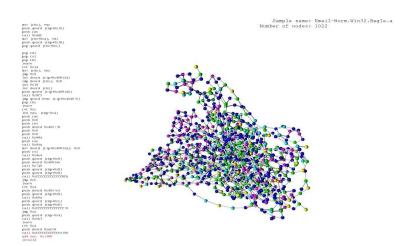 - Generic de-packing framework, payload extraction

Project idea

- *Describe your project idea*
    - **Investigation support for malwares and compromised devices**
    - **For the police and judiciary authorities**
    - **Automatic report based on forensic tools**

= Family extraction
= Self-protection witnesses
= Functionality identification
= Clustering
= OS function usage,
= Behavioral description

```
mov [rbx], eax
push qword [rip+0x10]
push rax
call 0xddf
mov [rbx+0x4], edi
push qword [rip+0x18]
pop qword [rbx+0xc]

pop rdi
pop rsi
pop rbx
leave
ret 0x14
mov [rdx], ebx
jmp 0x9
inc dword [rip+0x40812a]
cmp dword [rbx], 0x0
jnz 0x1d
inc dword [rbx]
push qword [rip+0x408146]
call 0x9f5
jmp qword near [rip+0x40407b]
pop rbx
leave
ret 0xc
lea eax, [rbp-0x4]
push rax
push 0x0
push rbx
push dword 0x402778
push 0x0
push 0x0
call 0x98a
push rax
call 0x95a
mov dword [rip+0x40812a], 0x0
push rsi
call 0xde4
push qword [rbp+0x8]
push dword 0x40814e
call 0x740
push qword [rbp+0x8]
push qword [rbp+0x8]
call 0xfffffffffffff8fb
jmp 0xf
leave
ret 0x4
push dword 0x405?e5
push qword [rbp+0x8]
call 0x66a
push qword [rbp+0xc]
push qword [rbp+0x8]
call 0xffffffffffffff70
jmp 0xa
push qword [rbp-0x4]
call 0x5b?
leave
ret 0x4
push dword 0xafc8
call 0xffffffffffffr=106
add eax, 0x1388
invalid
```

Sample name: Email-Worm.Win32.Bagle.a
Number of nodes: 1022

- *List of the complementary skills you need for your consortium*
    - **Knowledge on European norms, working organisation, security management**
    - **Interfaces with current tool**
    - **IOT, mobile phone and networks**