

A. P. T.
Mythes et réalités

Nicolas RUFF

EADS Innovation Works

nicolas.ruff@eads.net

Mythe

Google Hack Attack Was Ultra Sophisticated, New Details Show

By [Kim Zetter](#) January 14, 2010 | 8:01 pm | Categories: [Breaches](#), [Cybersecu](#)

Sophisticated attack thought to be state-sponsored.

Hackers have broken into the systems of a web authentication firm in Europe, issuing false certificates that forced Google, Microsoft and Mozilla to issue emergency browser patches.

Latest sophisticated cyber attack targets EU

'This one is a big one,' an official says; many suspect hackers based in China

Le Ministère de l'Economie et des Finances touché par une cyber-attaque sophistiquée, présentée comme "la première attaque contre l'Etat français de cette ampleur"

C'est un scandale qui a éclaté ce matin à l'heure où commençaient à être distribués les premiers journaux. Le peuple français a en effet appris que son ministère de l'Economie et des Finances a été victime d'une attaque numérique très sophistiquée par "des pirates professionnels, déterminés et organisés", ce qui a d'ailleurs déclenché l'ouverture d'une enquête et la mobilisation des services secrets.

Les groupes industriels Thales et Safran visés par des attaques

Thales a porté plainte contre un hacker qui affirme avoir fouillé Safran avoue qu'il a subi deux cyber-attaques entre 2009 et 2010

Actualité. Publié sur [ITespresso.fr](#) par [Philippe Guerrier](#) le 15 avril 2010. [Soyez le premier à réagir](#)

RSA security firm hit by 'sophisticated' hackers

SecurID network security tokens made by the firm may have been compromised

Réalité

 [@cesarcer](#)
Cesar Cerrudo

When an important company is hacked
it's called APT when other companies are
hacked it's called lack of security

4 Avr via web ☆ Favori ↻ Retweeter ↶ Répondre

Retweeté par [mattch](#) et 43 autres



Réalité

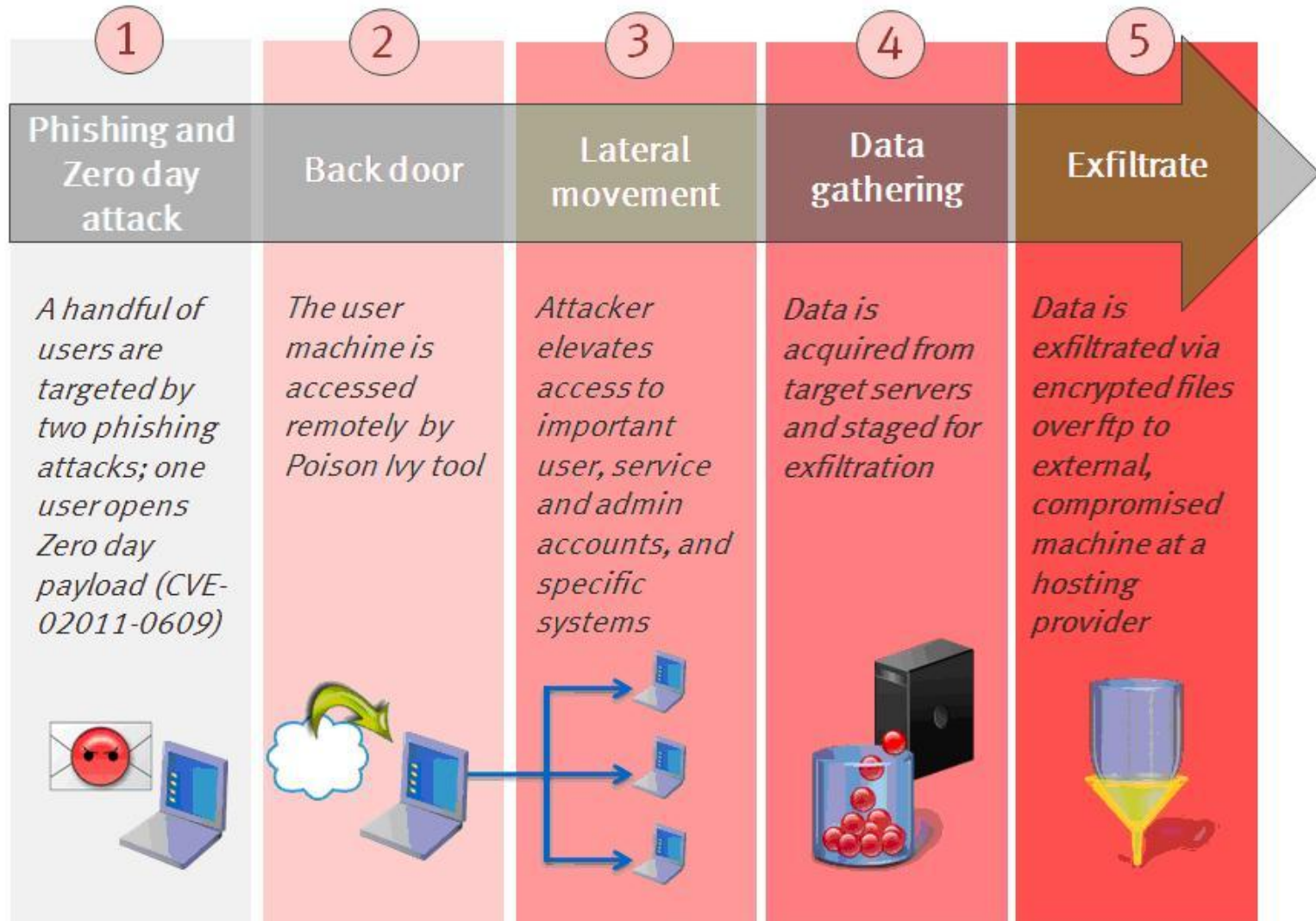
```
1. Hello
2.
3. I'm writing this to all the world, so you'll know more about us..
4.
5. At first I want to give some points, so you'll be sure I'm the hacker:
6.
7. I hacked Comodo from InstantSSL.it, their CEO's e-mail address mfpenco@mfpenco.com
8. Their Comodo username/password was: user: gtadmin password: globaltrust
9. Their DB name was: globaltrust and instantsslcms
```

<http://pastebin.com/74KXCaeZ>

```
1. Some stupids still doesn't believe I pwned the Comodo, here is another proof for tiny brains who
   can't believe:
2.
3. Here is part of decompiled TrustDLL of Comodo partner:
4.
5. ClassName: ASCR
6. Language: C#
```

<http://pastebin.com/DBDqm6Km>

Réalité



Réalité

- Y a-t-il le "bon" et le "mauvais" intrus ?



Zéro Bullshit (1/2)




 @ tim.m.healy	Notice	mar. 23/05/2006 13:05	328 Ko	
 @ tim.m.healy	Notice	dim. 14/05/2006 19:37	327 Ko	

Notice

tim.m.healy [falungster@gmail.com]

Les sauts de ligne en surnombre de ce message ont été supprimés.

À : Johann.hiller@tdw.lfk.eads.net

Pièces jointes :  K-17 Subcommittee .txt (274 o);  Planning Report.2007.doc (159 Ko);  Planning Report.2008.doc (164 Ko)

Weber,
please reference the meeting/planning report Please let me know, if you can open the files.

Thanks for the great support!

terry

--

Directeur de la Communication Financière : Monsieur Pierre de Bausset

Adresse : 37 boulevard de Montmorency, 75781 Paris Cedex 16.

Téléphone : 01 42 24 24 23

Email : iri@eads.net <<mailto:iri@eads.net>>

Site Internet : www.finance.eads.net <<http://www.finance.eads.net>>

Zéro Bullshit (1/2)

The screenshot displays the OffVis malware analysis interface. The main window shows the raw file contents of 'Cases.dll' in OLESSFormat. The content is a list of memory addresses from 00016940 to 00016C10, each followed by a series of hex values (mostly 81) and a corresponding string of characters. The string at 00016940 is 'µÅÅ.5ÅÅ.QÅÅ.....'. The parsing results pane on the right is currently empty. The status bar at the bottom shows 'Offset: 92496', 'Length: 0', '98,0056ms', and '130,0074ms'.

OffVis: malware.vir

File Edit View Tools Help

Parser: Cases.dll : OLESSFormat Parse

Raw File Contents

Address	Hex Data	String
00016940	B5 C0 C1 81 35 C1 C1 81 51 C1 C1 81 81 81 81 81	µÅÅ.5ÅÅ.QÅÅ.....
00016950	81 81 81 81 81 81 81 81 80 81 81 81 81 81 81
00016960	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016970	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016980	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016990	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169A0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169B0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169C0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169D0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169E0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
000169F0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A00	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A10	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A20	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A30	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A40	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A50	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A60	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A70	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A80	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016A90	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AA0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AB0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AC0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AD0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AE0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016AF0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B00	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B10	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B20	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B30	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B40	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B50	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B60	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B70	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B80	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016B90	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BA0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BB0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BC0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BD0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BE0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016BF0	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016C00	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81
00016C10	81 81 81 81 81 81 81 81 81 81 81 81 81 81 81

Parsing Results

Name	Value	Offset	Size	Type
------	-------	--------	------	------

Parsing Notes

Type	Notes	Offset	Length	Vuln ID
------	-------	--------	--------	---------

Offset: 92496 Length: 0 98,0056ms 130,0074ms

Zéro Bullshit (1/2)

```
C:\Windows\system32\cmd.exe

Z:\_ARTICLES_\GS Days 2011\OfficeMalScanner>OfficeMalScanner.exe ..\malware.vir scan brute

-----+
| OfficeMalScanner v0.53 |
| Frank Boldwin / www.reconstructor.org |
+-----+

[*] SCAN mode selected
[*] Opening file ..\malware.vir
[*] Filesize is 162177 (0x27981) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Scanning now...

FS:[30h] (Method 1) signature found at offset: 0xb30
API-Hashing signature found at offset: 0xd84

Brute-forcing for encrypted PE- and embedded OLE-files now...
XOR encrypted embedded OLE signature found at offset: 0x1d174 - encryption KEY: 0x81

Dumping Memory to disk as filename: malware__EMBEDDED_OLE__OFFSET=0x1d174__XOR-KEY=0x81.bin

XOR encrypted MZ/PE signature found at offset: 0x11400 - encryption KEY: 0x81

Dumping Memory to disk as filename: malware__PEFILE__OFFSET=0x11400__XOR-KEY=0x81.bin

XOR encrypted MZ/PE signature found at offset: 0x128d8 - encryption KEY: 0x81

Dumping Memory to disk as filename: malware__PEFILE__OFFSET=0x128d8__XOR-KEY=0x81.bin

Bruting XOR Key: 0xff
Bruting ADD Key: 0xff

Analysis finished!

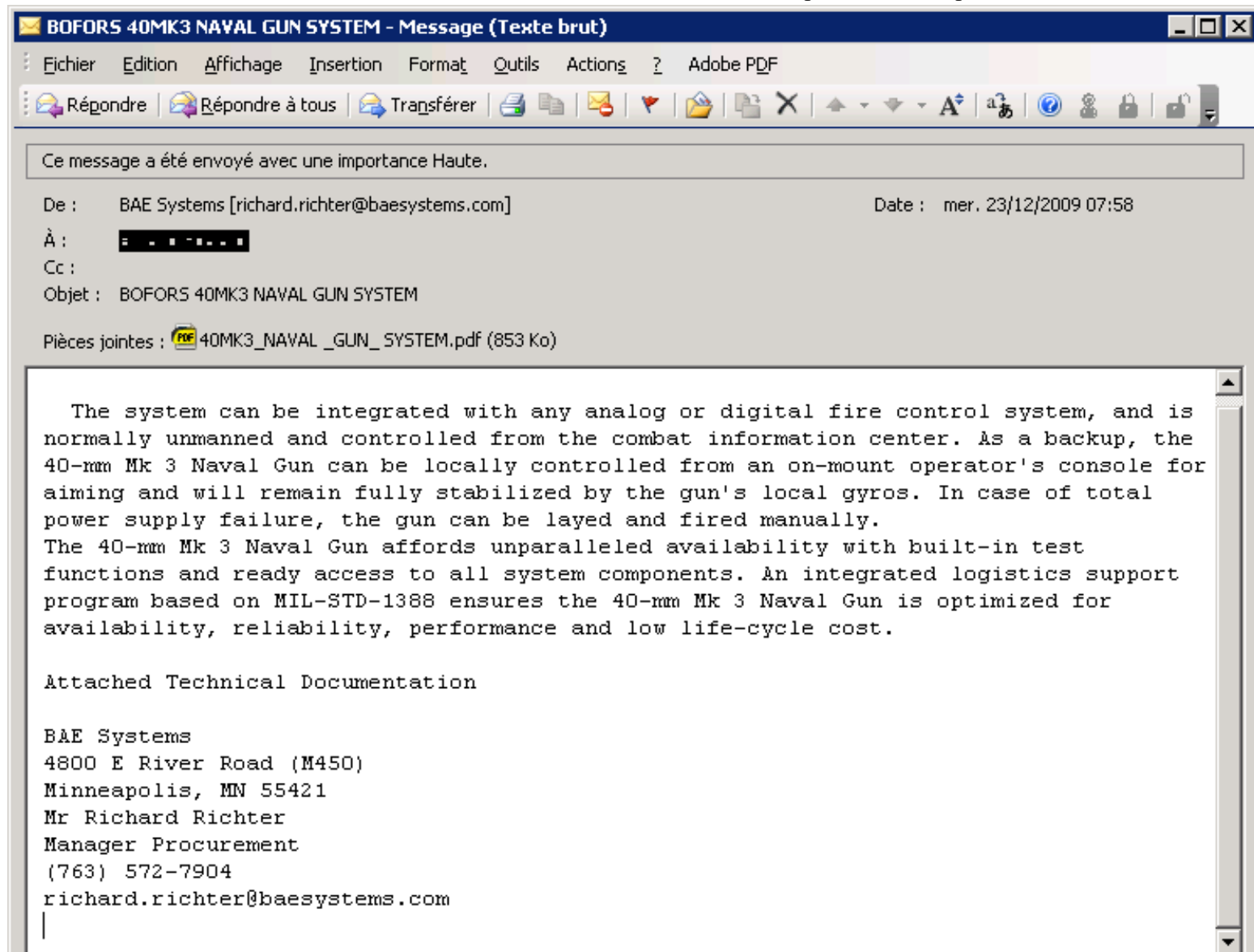
-----+
| malware.vir seems to be malicious! Malicious Index = 61 |
+-----+

Z:\_ARTICLES_\GS Days 2011\OfficeMalScanner>
```

Zéro Bullshit (1/2)

- Synthèse
 - Un document malveillant
 - Exploitation d'une faille Office
 - Un exécutable embarqué
 - ... pour relancer Word sur un document "propre"
 - Chiffré par XOR 0x81
 - Un exécutable embarqué
 - ... de type "*download & execute*"
 - Chiffré par XOR 0x81
- Date de l'attaque: 2006 ...
- Opération "*Titan Rain*": 2003

Zéro Bullshit (2/2)



BOFORS 40MK3 NAVAL GUN SYSTEM - Message (Texte brut)

Fichier Edition Affichage Insertion Format Outils Actions ? Adobe PDF

Répondre Répondre à tous Transférer

Ce message a été envoyé avec une importance Haute.

De : BAE Systems [richard.richter@baesystems.com] Date : mer. 23/12/2009 07:58
À : [REDACTED]
Cc :
Objet : BOFORS 40MK3 NAVAL GUN SYSTEM

Pièces jointes : PDF 40MK3_NAVAL_GUN_SYSTEM.pdf (853 Ko)

The system can be integrated with any analog or digital fire control system, and is normally unmanned and controlled from the combat information center. As a backup, the 40-mm Mk 3 Naval Gun can be locally controlled from an on-mount operator's console for aiming and will remain fully stabilized by the gun's local gyros. In case of total power supply failure, the gun can be layed and fired manually. The 40-mm Mk 3 Naval Gun affords unparalleled availability with built-in test functions and ready access to all system components. An integrated logistics support program based on MIL-STD-1388 ensures the 40-mm Mk 3 Naval Gun is optimized for availability, reliability, performance and low life-cycle cost.

Attached Technical Documentation

BAE Systems
4800 E River Road (M450)
Minneapolis, MN 55421
Mr Richard Richter
Manager Procurement
(763) 572-7904
richard.richter@baesystems.com

Zéro Bullshit (2/2)

The screenshot shows the PDF Walker application interface. The left sidebar displays a tree view of the PDF structure for the file `/mnt/sdb1/_presta/_malware`. The tree includes: Header (version 1.6), Revision 1, Revision 2, Revision 3, Body, MetadataStream, Page, Dictionary, Stream (selected), Stream Dictionary, ObjectStream, XRefStream, and Trailer.

The main window is titled "PDF Walker" and shows the PDF code for the selected object. The code is as follows:

```
42 0 obj
<<
  /Filter [ /FlateDecode ]
  /Length 1421
>>stream
[Binary data]
endstream
```

Below the code, a hex dump is displayed, showing the binary data in hexadecimal and ASCII. The hex dump starts with `0000000000` and ends with `0000000400`. The ASCII column shows the beginning of a JavaScript function `function urpl(sc)`.

At the bottom of the window, the status bar indicates: `Viewing /mnt/sdb1/_presta/_malware/malware.pdf`

Zéro Bullshit (2/2)

- Synthèse
 - Un document malveillant
 - Exploitation d'une faille Adobe Reader
 - Un exécutable embarqué
 - ... pour relancer Adobe Reader sur un document "nettoyé"
 - Chiffré par XOR
 - Un exécutable embarqué
 - ... de type "Poison Ivy"
 - Chiffré par XOR

Intrusion

- Ce qui frappe
 - Le mode opératoire est toujours le même
 - Les attaques sont (relativement) simples
 - Exploitation de failles connues
 - Nécessite JavaScript (Adobe Reader)
 - Ne supporte pas DEP
 - Outils publics
 - <http://www.poisonivy-rat.com/>

Intrusion

- La situation en 2011
 - Le mode opératoire ne change pas
 - Les failles sont de plus en plus sophistiquées
 - Exploitation de failles "0day"
 - <http://blog.fireeye.com/research/2011/03/who-is-exploiting-the-flash-0-day-cve-2011-0609.html>
 - A tout instant, il faut partir du principe qu'il y a des failles dans:
 - Adobe Reader, Flash Player, ShockWave et Oracle JVM

Post-intrusion

- Ce qui frappe
 - Le mode opératoire est toujours le même
 - C'est celui d'un *pentester*
 - Les outils de sécurité ne voient rien
 - Les compromissions sont souvent découvertes "par hasard"
 - Des outils publics sont utilisés
 - Ex. "*Pass the Hash Toolkit*"

Conclusion

- Les "APT" existent ... depuis longtemps !
- Les "APT" n'ont rien d'*Advanced*
- Les outils de sécurité existants ont échoué
 - Il est donc temps de réfléchir à de nouvelles solutions
 - ... qui ne seront pas forcément chères ni compliquées !
- Aphorisme
 - Pour lutter contre des outils, il suffit de déployer de la technologie
 - Pour lutter contre des humains, il est nécessaire de déployer des humains

Références

- JSSI 2010
 - "Les PME contre la mafia"
 - <http://www.ossir.org/jssi/jssi2010/3A.pdf>
- El Jefe
 - <http://www.immunityinc.com/products-eljefe.shtml>