iAWACS 2010 : Challenge Debriefing

« Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. »

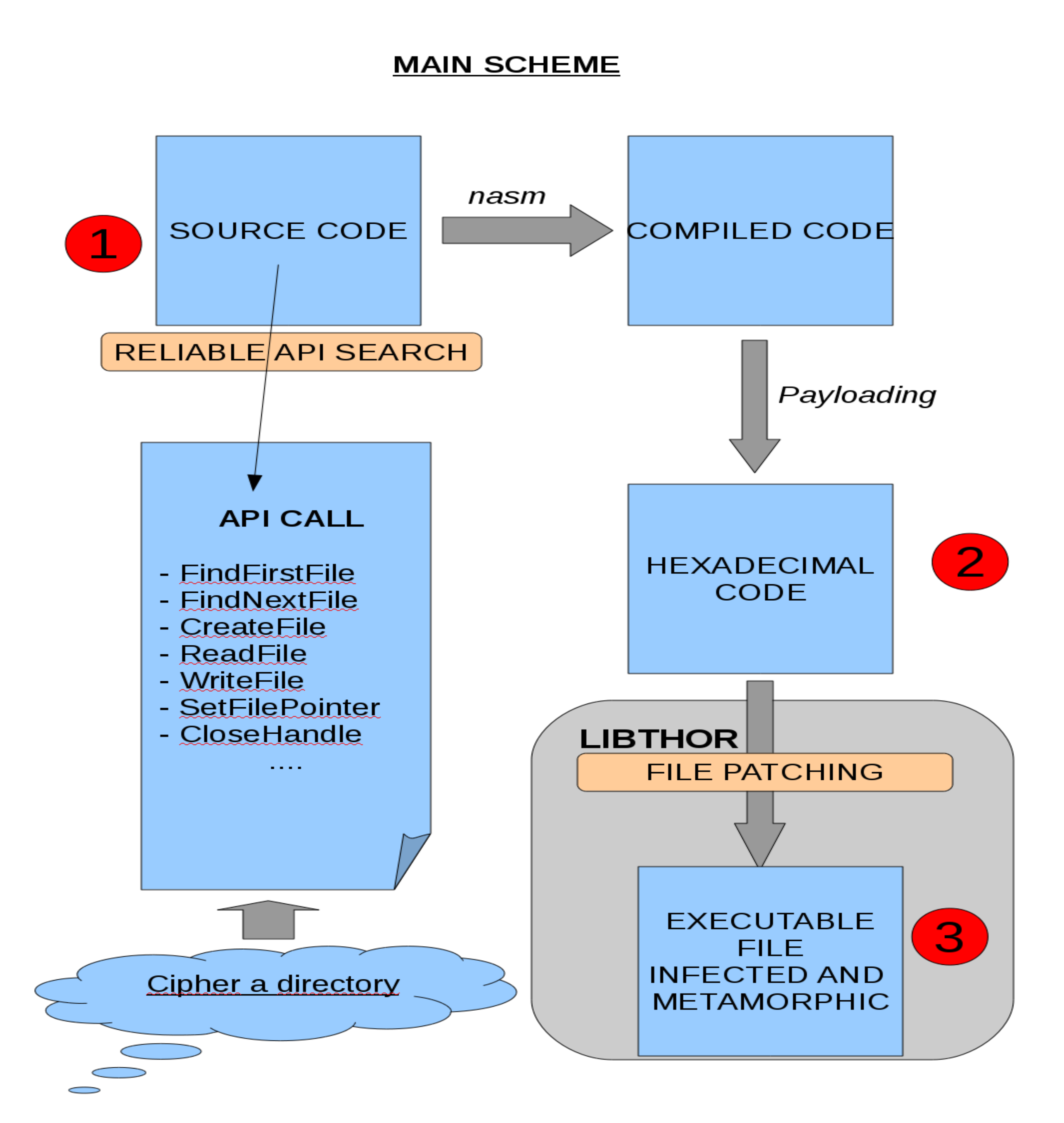
Article 19 of "Universal Declaration of Human Rights"

Samir Megueddem – ESIEA CVO
Anthony Desnos – ESIEA SIS

iAWACS 2010 : Challenge Debriefing

- A ransomware like, but inoffensive :)
- The POC is a simple folder encryption (w00t !)
  - A userland executable
  - Simple xor to encrypt file …
    - Can be easily changed by a strong encryption (aes)
  - Use a reliable way to found API address
    - The same as metasploit, but metasploit payloads are not in AV database ?
  - Can be improved to a real ransomware, more sophisticated, using gsm (surtaxed sms)
  - Injected with a new framework (libthor)

iAWACS 2010 : Challenge Debriefing



MAIN SCHEME

1

SOURCE CODE

nasm

COMPILED CODE

RELIABLE API SEARCH

Payloading

API CALL

- FindFirstFile
- FindNextFile
- CreateFile
- ReadFile
- WriteFile
- SetFilePointer
- CloseHandle

....

HEXADECIMAL CODE

2

LIBTHOR

FILE PATCHING

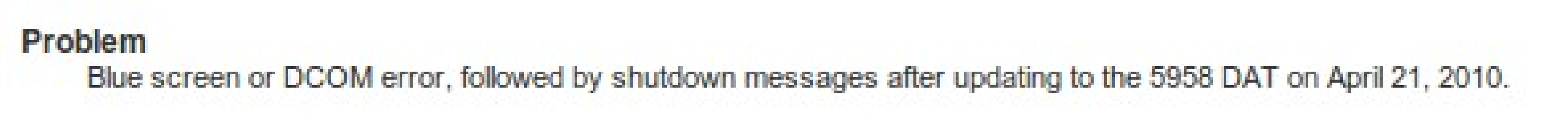
EXECUTABLE FILE INFECTED AND METAMORPHIC

3

Cipher a directory

iAWACS 2010 : Challenge Debriefing

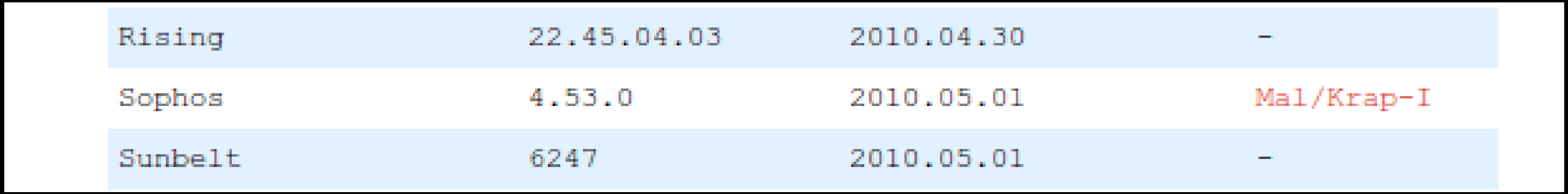
- Funny stories
  - McAfee + svchost.exe = LOL



Problem

Blue screen or DCOM error, followed by shutdown messages after updating to the 5958 DAT on April 21, 2010.

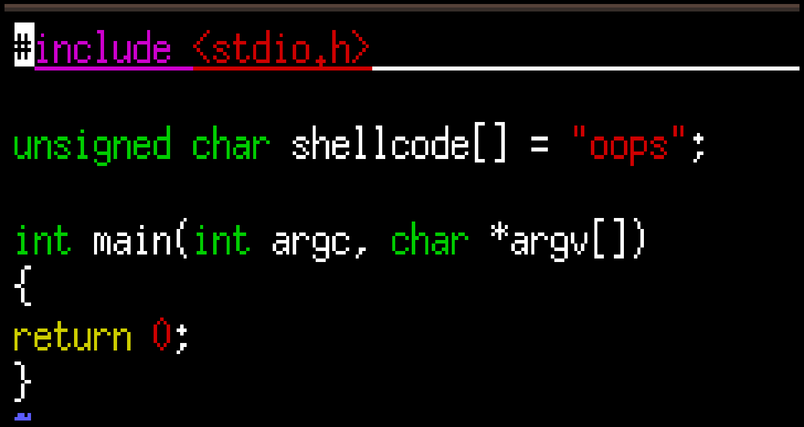
  - Sophos + GO = LOL
    - GO windows executable (a HelloWord)
      - Detecting by sophos as a virus (http://code.google.com/p/go/issues/detail?id=760)



Rising	22.45.04.03	2010.04.30	-
Sophos	4.53.0	2010.05.01	Mal/Krap-I
Sunbelt	6247	2010.05.01	-

iAWACS 2010 : Challenge Debriefing

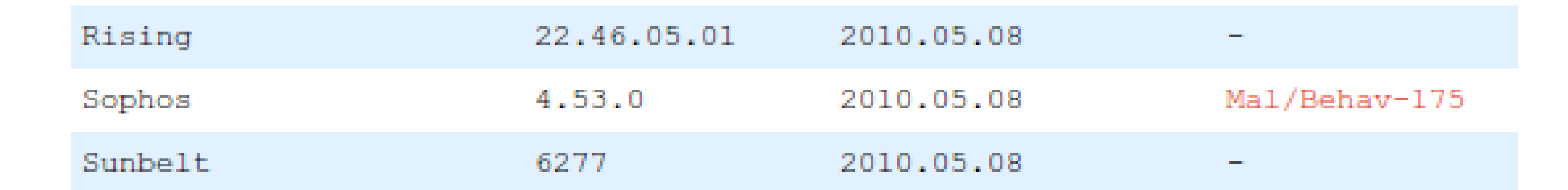
- Funny stories 2
  - Sophos + debug symbols = LOL



```
#include <stdio.h>

unsigned char shellcode[] = "oops";

int main(int argc, char *argv[])
{
return 0;
}
```



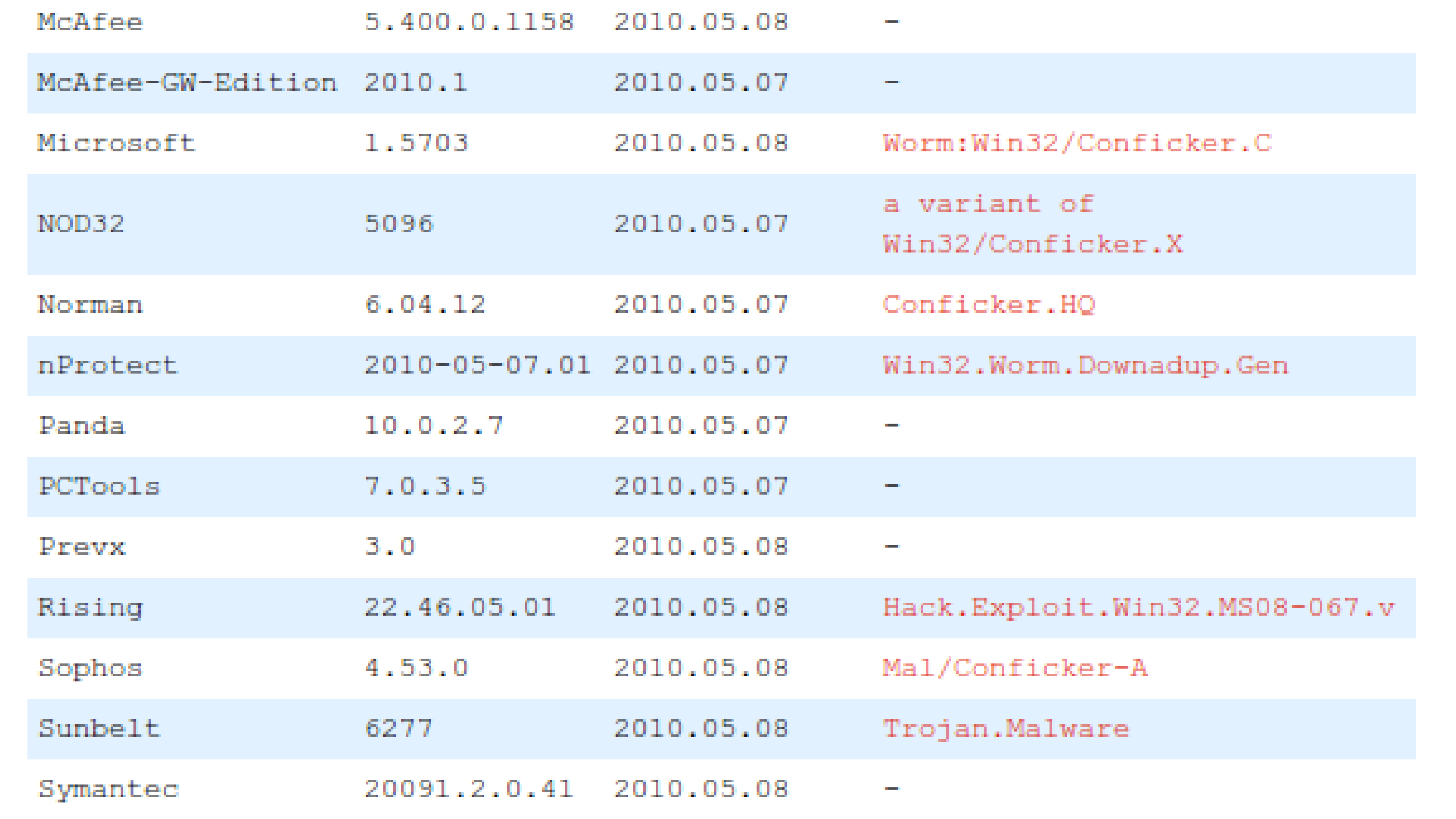
Rising	22.46.05.01	2010.05.08	-
Sophos	4.53.0	2010.05.08	Mal/Behav-175
Sunbelt	6277	2010.05.08	-

iAWACS 2010 : Challenge Debriefing

- Funny stories 3
  - Compression
    - zip/gzip/bzip2 : OK

iAWACS 2010 : Challenge Debriefing

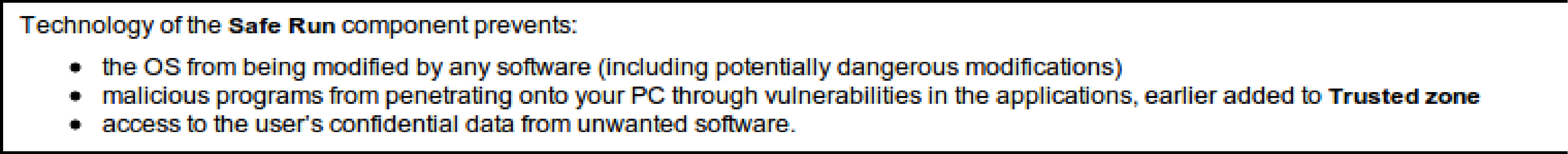
- Funny stories 3
  - Compression
    - 7zip (thx to Johann Maillard + Alan Zaccardelle)



McAfee	5.400.0.1158	2010.05.08	-
McAfee-GW-Edition	2010.1	2010.05.07	-
Microsoft	1.5703	2010.05.08	Worm:Win32/Conficker.C
NOD32	5096	2010.05.07	a variant of Win32/Conficker.X
Norman	6.04.12	2010.05.07	Conficker.HQ
nProtect	2010-05-07.01	2010.05.07	Win32.Worm.Downadup.Gen
Panda	10.0.2.7	2010.05.07	-
PCTools	7.0.3.5	2010.05.07	-
Prevx	3.0	2010.05.08	-
Rising	22.46.05.01	2010.05.08	Hack.Exploit.Win32.MS08-067.v
Sophos	4.53.0	2010.05.08	Mal/Conficker-A
Sunbelt	6277	2010.05.08	Trojan.Malware
Symantec	20091.2.0.41	2010.05.08	-

iAWACS 2010 : Challenge Debriefing

- Funny stories 4
  - Kaspersky sandbox bug (thx to anonymous authors :))
    - New feature in the product (old bugs ?)
    - Run an executable (exe, bat, ...) into a sandbox
    - Don't handle properly file path access → Ooops.bat :
      - DEL "C:\Users\iawacs\Desktop\toto.txt" → don't work
      - DEL "\\IAWACS-PC\Users\iawacs\Desktop\toto.txt" → works
      - DEL "\\127.0.0.1\C$\Users\iawacs-user\X\Y.txt"
        - – On the fly by Guiheux Goulven (Amossys)



Technology of the **Safe Run** component prevents:

- the OS from being modified by any software (including potentially dangerous modifications)
- malicious programs from penetrating onto your PC through vulnerabilities in the applications, earlier added to **Trusted zone**
- access to the user's confidential data from unwanted software.

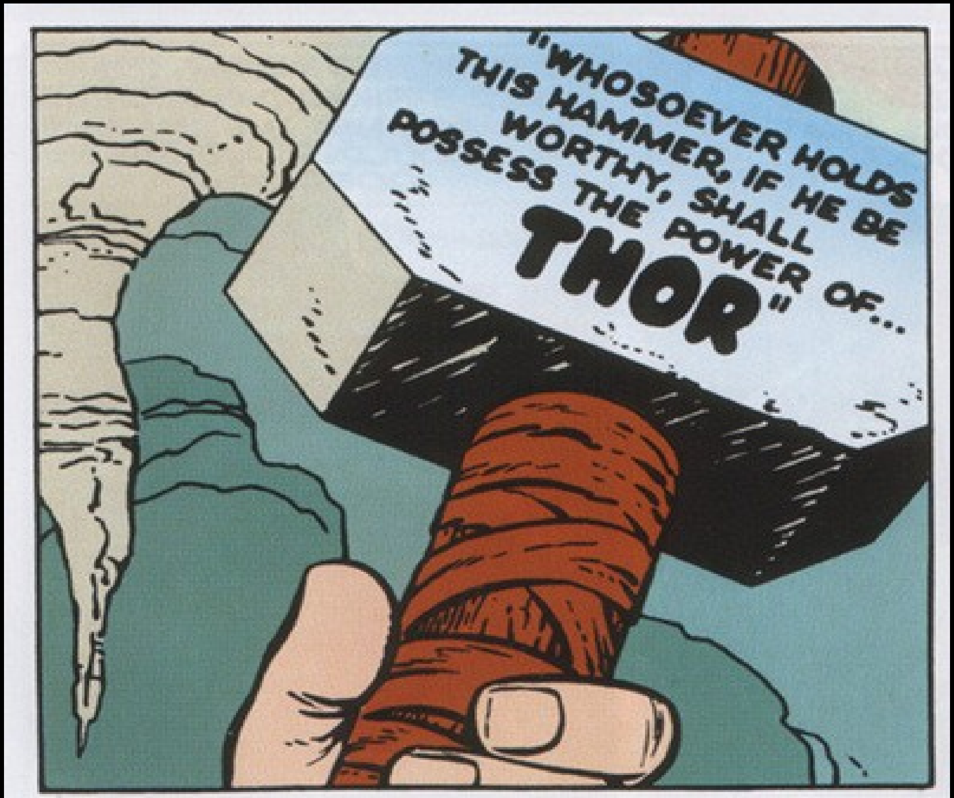
iAWACS 2010 : Challenge Debriefing

- LIBTHOR
  - A new opensource framework to play with ASM instructions
    - Control Flow Graph
    - Intermediate Representation
    - Metamorphism
      - Like Metaphor (Mental Driller)
      - VW (presentation tomorrow by E.Filiol and G.Gueguen)
      - Junk code
        - Math obfuscation
      - uVM
    - Virtual Machines
      - Embedded like a shellcode
      - Dynamic bytecodes
      - Using libthor features (ex : metamorphic codes and IR)

iAWACS 2010 : Challenge Debriefing

- LIBTHOR
  - Can be used to :
    - play with a code.
    - protect a software ?
    - have real and open tests for AV softwares ?
    - ...

iAWACS 2010 : Challenge Debriefing


"WHOSOEVER HOLDS THIS HAMMER, IF HE BE WORTHY, SHALL POSSESS THE POWER OF... THOR"

A first release in July/August 2010 ...

To be continued .....