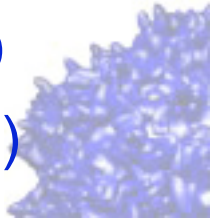
1st International Workshop

Nancy - 4th & 5th May 2006

Evaluation methodology of function-based malware detection

Authors : Grégoire JACOB
Mickaël LE LIARD
Eric FILIOL (ESAT)



Problematic

Concrete problematic

Analysis of the deployed behavioral detection methods and their correlation with other types of detection in commercial antiviral products

Progression

I. Theoretical context of the analysis
   1. Detection techniques
   2. Projection in future
   3. Anti-antiviral strategy
II. Establishment of a procedure
III. Deductions concerning the detection rules
IV. Conclusion

I.1 Detection techniques

- Two functioning modes for an antivirus
  - static mode or "form-based"
    - Signature search by pattern-matching
    - Spectrum analysis of the processor instructions
    - Heuristic analysis by code emulation
    - Integrity check of the file content
  - dynamic mode or "function-based"
    - Behavioral detection in the execution context
    - Code emulation

- An important and necessary documentary phase
  - Few reference articles …
  - … lacking of details ⇨ extrapolation and crossing

I.2 Projection in future

- Form-based analysis vowed to fail
  - Lack of reactivity
    - Increasing propagation speed
    - Signature creation and base update delays
  - Existence of polymorphic viruses
    - cf. next slide
  - Polymorphic virus detection is NP-complete
    - D. Spinellis' works in 2003

- The behavioral solution?

I.3 Anti-antiviral strategy

- Principles stated when creating a virus
  - Auto-reproducing codes
  - Often the vector of a final payload
  - Anti-antiviral techniques
    - Stealth
    - Polymorphism
    - Armoring
- Polymorphism specificity
  - Code ciphering
  - Mutation of the deciphering routine
  - Metamorphic generation of the virus body

Difficulty to extract a discriminating signature

Progression

I. Theoretical context of the analysis

II. Establishment of a procedure

1. Operating mode
2. Listed behaviors
3. Alternative behaviors

III. Deductions concerning the detection rules

IV. Conclusion

II.1 Operating mode

- Preliminary study of a virus from a known strain
  - MyDoom code sources
  - C language specific to Win32
  - Reference declined in a whole range of versions
- Generation of new versions
  - Modification of the **behaviors**
  - Controlled simulation of metamorphism
  - Still hardly automatically proceeded

II.1 Operating mode

Antivirus reaction face to the modifications

- Manual Analysis in **static** mode
  - Information about the signature

- Resident **dynamic** detection
  - Interpretation depending on the static results

- Tested antiviral products:
  - AVG AntiVirus
  - Avast !
  - AntiVirusKit2006
  - OfficeScan
  - Panda Titanium
  - Norton Antivirus

II.2 Listed behaviors

- Inventoried behaviors …

1. Code duplication	
2. Residency	6. Stealth
-New run register key	-Protocol stacks redefined
3. Propagation	7. Polymorphism
-Mass mailing	-String ciphering
4. Overinfection test	8. Information collect
-Existence of a register key	-Recursive scan
5. Activity test	9. Final Payload
-Existence of a mutex	-DDOS attack
	10. (Social engineering)

- … resulting from a functional analysis

/Analyse MyDoom/MyDoom.htm

II.3 Altered behaviors

New variants of the strain

- 15 generated versions
- 6 behaviors modified or suppressed
  - Code duplication
  - Residency
  - Overinfection test
  - Activity test
  - Polymorphism
  - Final payload

Modification example for the overinfection test

- Existence of a "superhidden“ file
  - Used by system files
  - Invisible even with the hidden file display
  - Requires the definition of a specific file attribute in C:

```
#define FILE_ATTRIBUTE_SUPER_HIDDEN 0x00000006
```

II.3 Altered behaviors

New variants of the strain

- 15 generated versions
- 6 behaviors modified or suppressed
  - Code duplication
  - Residency
  - Overinfection test
  - Activity test
  - Polymorphism
  - Final payload

Modification example for polymorphism

- Flow encryption of the strings
  - Plain text XORed with the ciphering sequence
  - Uses three cyclic registers
  - Freedom degrees introduced by the key

Progression

I. Theoretical context of the analysis

II. Establishment of a procedure

III. Deductions concerning the detection rules

1. Results for AVG Anti-Virus
2. Results for Avast !
3. Synthesis about the rules

IV. Conclusion

III.1 AVG Anti-virus

First interpretations

AVG Anti-Virus Professional Trial Edition
Version : 7.1.0.375
Company : Grisoft
Signature Base : /

Behavior	Version	Static analysis	Dynamic protection
(none)	Executable original strain		I-Worm/MyDoom
	Shimgapi.dll library	I-Worm/MyDoom	N/A
CHARG	CHARG_TRIG_TARG		I-Worm/MyDoom
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT		I-Worm/MyDoom
	DUPLI_NAM_PATH		I-Worm/MyDoom
RESID	RESID_SERV_KEY		I-Worm/MyDoom
	RESID_WIN_INI		I-Worm/MyDoom
POLYM	POLYM_FLOW_LIB		I-Worm/MyDoom
	POLYM_FLOW_STR		
	POLYM_PLAIN_LIB		I-Worm/MyDoom
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT		I-Worm/MyDoom
	ACTIV_MUTEX		I-Worm/MyDoom
SURINF	SURINF_DIF_KEY		I-Worm/MyDoom
	SURINF_SUP_HID		I-Worm/MyDoom
	SURINF_ENV_VAR		I-Worm/MyDoom

⇨ **Signature localized in the library**

Reference tests

III.1 AVG Anti-virus

First interpretations

AVG Anti-Virus Professional Trial Edition
Version : 7.1.0.375
Company : Grisoft
Signature Base : /

Behavior	Version	Static analysis	Dynamic protection
(none)	Executable original strain		I-Worm/MyDoom
	Shimgapi.dll library	I-Worm/MyDoom	N/A
CHARG	CHARG_TRIG_TARG		I-Worm/MyDoom
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT		I-Worm/MyDoom
	DUPLI_NAM_PATH		I-Worm/MyDoom
RESID	RESID_SERV_KEY		I-Worm/MyDoom
	RESID_WIN_INI		I-Worm/MyDoom
POLYM	POLYM_FLOW_LIB		I-Worm/MyDoom
	POLYM_FLOW_STR		
	POLYM_PLAIN_LIB		I-Worm/MyDoom
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT		I-Worm/MyDoom
	ACTIV_MUTEX		I-Worm/MyDoom
SURINF	SURINF_DIF_KEY		I-Worm/MyDoom
	SURINF_SUP_HID		I-Worm/MyDoom
	SURINF_ENV_VAR		I-Worm/MyDoom

⇨ **Signature localized in the library**

⇨ **Behaviors undetected or ignored without a signature**

⇨ **Confirmed by the detection of the ones with the original library**

III.1 AVG Anti-virus

First interpretations

AVG Anti-Virus Professional Trial Edition
Version : 7.1.0.375
Company : Grisoft
Signature Base : /

Behavior	Version	Static analysis	Dynamic protection
(none)	Executable original strain		I-Worm/MyDoom
	Shimgapi.dll library	I-Worm/MyDoom	N/A
CHARG	CHARG_TRIG_TARG		I-Worm/MyDoom
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT		I-Worm/MyDoom
	DUPLI_NAM_PATH		I-Worm/MyDoom
RESID	RESID_SERV_KEY		I-Worm/MyDoom
	RESID_WIN_INI		I-Worm/MyDoom
POLYM	POLYM_FLOW_LIB		I-Worm/MyDoom
	POLYM_FLOW_STR		
	POLYM_PLAIN_LIB		I-Worm/MyDoom
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT		I-Worm/MyDoom
	ACTIV_MUTEX		I-Worm/MyDoom
SURINF	SURINF_DIF_KEY		I-Worm/MyDoom
	SURINF_SUP_HID		I-Worm/MyDoom
	SURINF_ENV_VAR		I-Worm/MyDoom

⇨ **Signature localized in the library**

⇨ **Behaviors undetected or ignored without a signature**

⇨ **Confirmed by the detection of the ones with the original library**

⇨ **Signature made up of an encrypted string**

⇨ **Non detection proves the signature to be required**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	strain	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	strain	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

⇨ **Different levels of detection between the library and executable**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	strain	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

⇨ **Different levels of detection between the library and executable**

⇨ **Specific signature in an encrypted string from the plain library**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	Executable original root	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

⇨ **Different levels of detection between the library and executable**

⇨ **Specific signature in an encrypted string from the plain library**

⇨ **Generic detection of an encrypted library**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	strain	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

⇨ **Different levels of detection between the library and executable**

⇨ **Specific signature in an encrypted string from the plain library**

⇨ **Generic detection of an encrypted library**

⇨ **Behaviors undetected or ignored without a signature**

III.2 Avast !

First interpretations

Avast ! Familial Edition 2006
Version : 4.6.763
Company : alwil software
Signature Base : 0611-2

Behavior	Version	Static analysis	Dynamic protection
(none)	strain	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	Shimgapi.dll library	[Wrm]	N/A
CHARG	CHARG_TRIG_TARG	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	CHARG_NO_BDOOR		
DUPLI	DUPLI_SH_CUT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	DUPLI_NAM_PATH	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
RESID	RESID_SERV_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	RESID_WIN_INI	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
POLYM	POLYM_FLOW_LIB		[Wrm]
	POLYM_FLOW_STR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	POLYM_PLAIN_LIB	[Wrm]	[Wrm]
	POLYM_PLAIN_STR		
ACTIV	ACTIV_EVENT	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	ACTIV_MUTEX	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
SURINF	SURINF_DIF_KEY	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_SUP_HID	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]
	SURINF_ENV_VAR	Win32:Agent-EZ[Unp]	Win32:Agent-EZ[Unp]

⇨ **Signature localized in the library**

⇨ **Different levels of detection between the library and executable**

⇨ **Specific signature in an encrypted string from the plain library**

⇨ **Generic detection of an encrypted library**

⇨ **Behaviors undetected or ignored without a signature**

⇨ **Generic detection prevails on the precision search**

III.3 Rules synthesis

- Detection rules using several methods
  - Correlation of the results in the dynamic mode

T_{sig} : *Detection by Signature*

T_{behav} : *Behavioral Detection*

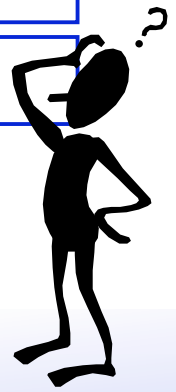
Two possible hypothesises on the correlation

$H_1 : \varphi(T_{behav} \wedge T_{sig})$

$H_2 : \varphi(T_{sig})$

H_1: Behavioral detection implemented but ignored without corroboration from an additional signature

H_2: Behavioral detection non deployed or inefficient



- In every case, questionable utility?

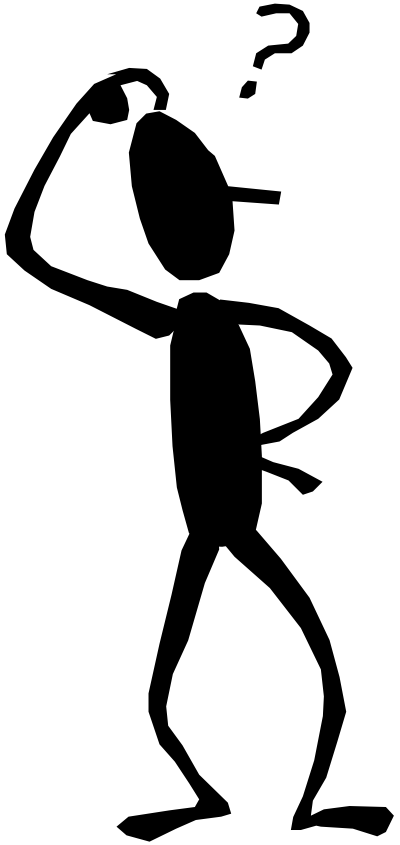
Progression

I. Theoretical context of the analysis
II. Establishment of a procedure
III. Deductions concerning the detection rules
IV. Conclusion

Conclusion

- Obscurantism of the antiviral background
  - Confidentiality of the documents
  - Few investment in research
- Lying commercial speeches
  - Detection of 90% of the unknown viruses announced…
  - … thanks to behavioral detection engines
    - Questioning face to the results
- Perspectives for the project
  - Complementary tests of behaviors
  - Automation of the tests ?

Any question ?



Thanks for your attention