esiea recherche

Laboratoire de virologie et de cryptologie opérationnelles - Corsaire pas pirate

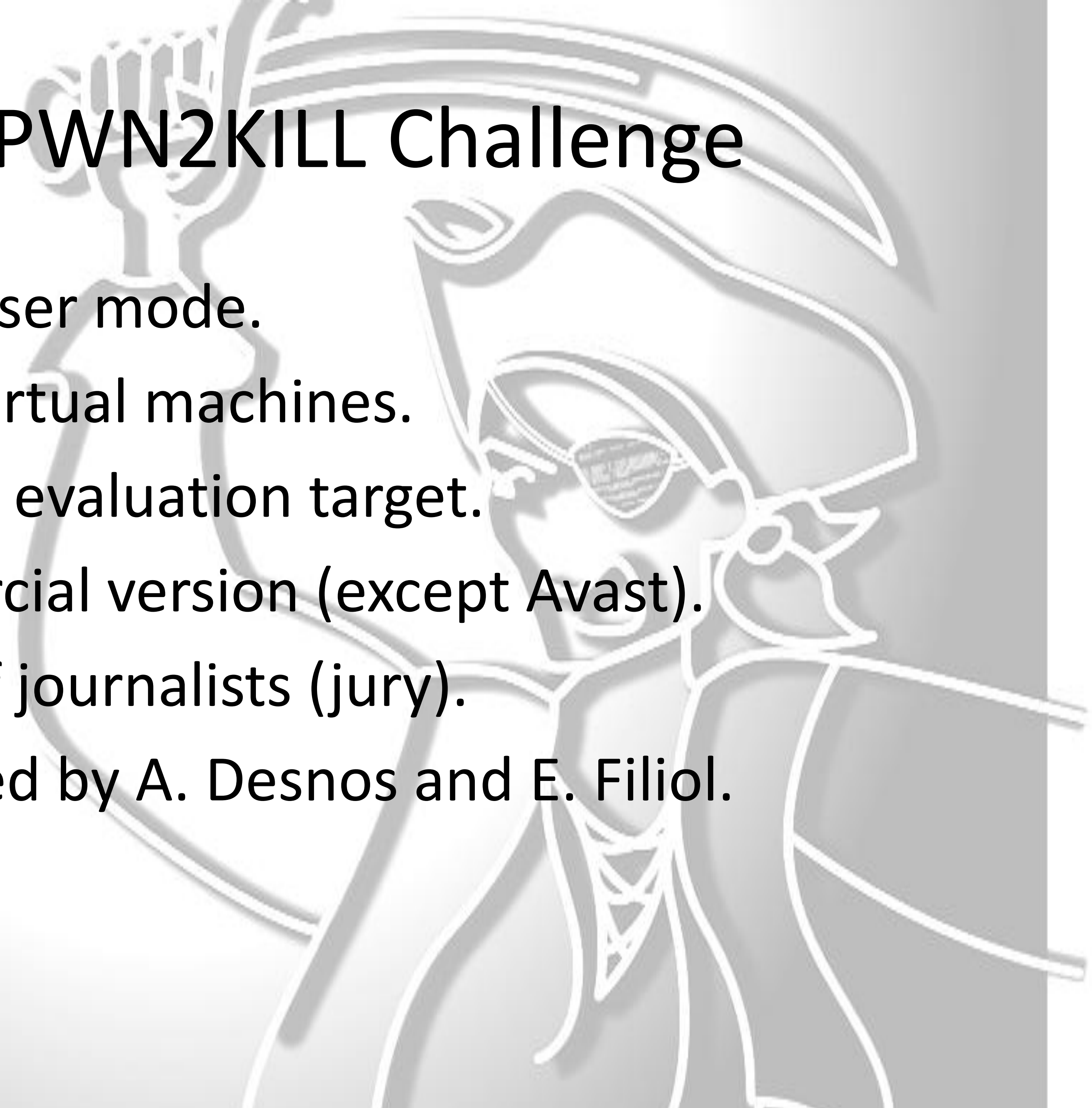
iAWACS 2010

PWN2KILL Debrief

Eric Filiol filiol@esiea.fr

PWN2KILL Challenge

- Win 7/User mode.
- Use of virtual machines.
- 15 AV as evaluation target.
- Commercial version (except Avast).
- Board of journalists (jury).
- Organized by A. Desnos and E. Filiol.



Target of evaluation

- Avast (free edition)
- AVG
- Avira
- BitDefender
- DrWeb
- F-Secure
- G-Data
- Kaspersky
- McAfee
- Microsoft AV
- NOD32
- Norton
- Safe’n’Sec
- Sophos
- Trend Micro.

Rules

- Any behaviour a normal user is used to.
- The user profile
  - A typical home user (your mother).
  - A typical office user.
- Proactive warning can be bypassed

  “*Your application is trying to modify the registry base. Do you accept it?”* is not understood by users.
- Having a PhD is not mandatory to use computers!

Rules (cont.)

1. Each candidate describes shortly his attack.
2. For each AV (mandatory)
    1. Perform a on-demand scanning (sequence-based detection).
    2. Execute his attack (on-access scanning automatically involved).
3. Detection ? Attack successful ?
4. Next candidate.

Presentation of attacks

- F.-X. Bru & F. Bertrand.
- G. Fahrner.
- S. Megguedem & A. Desnos.
- A. Zaccardelle.
- B. David
- Dechaux - Fizaine – Grivaux – Jaafar.

Last minute candidates

- F. Déchelle and his Korf Bmob

```
:loop
Start /realtime %0
Goto :loop
```

Known for a few year

http://www.youtube.com/watch?v=_F_JKHWhmmg

Guess what it is ?

AV product	Attack 1	Attack 2	Attack 3	Attack 4	Attack 5	Attack 6	Attack 7
Avast	F	D	F	F	F	F	F
AVG	F	D	F	F	F	F	F
Avira	F	D	F	F	F	F	F
BitDefender	F	D	D	F	F	F	F
DrWeb	F	D	F	F	F	F	DDDF
F-Secure	F	D	D	F	F	F	F
G-Data	F	D	D*	F	F	F	F
Kaspersky	F	D	F	F	F	F	DDDF
McAfee	F	D	F	F	F	F	F
MSE	F	D	F	F	F	F	F
NOD32	F	D	F	F	F	F	F
Norton	F	D	F	F	F	F	F
Safe’n’Sec	F	D	F	F	F	F	F
Sophos	F	D	F	F	F	F	DDF
Trend	F	D	F	F	F	F	F

On-demand scanning (sequence-based detection)) – F (failed) – D (detect)
*** just a proactive, not blocking message (attack still possible)**

AV product	Attack 1	Attack 2	Attack 3	Attack 4	Attack 5	Attack 6	Attack 7
Avast	F	D	F	F	F	F	F
AVG	F	D	F	F	F	F	F
Avira	F	D	F	F	F	F	F
BitDefender	F	D	D	F	F	F	F
DrWeb	F	D	F	F	F	F	DDDF
F-Secure	F	D	D	F	F	F	F
G-Data	F	D	F	F	D*	F	F
Kaspersky	F	D	F	F	F	F	FDDF
McAfee	F	D	F	F	F	F	F
MSE	F	D	F	F	F	F	F
NOD32	F	D	F	F	F	F	F
Norton	F	D	F	F	F	F	F
Safe'n'Sec	F	D	F	F	F	F	F
Sophos	F	D	F	F	F	F	DDF
Trend	F	D	F	F	D	F	F

On-access scanning (behaviour-based detection) – F (failed) – D (detect) –
*** just a proactive, not blocking message (attack still possible)**

Facts

- Most of these attacks rely on techniques published during the recent years.
  - K-ary viruses (2007).
  - Sophisticated armored viruses (2005).
  - Encryption techniques (2000, 2001, 2002…).
  -

Conclusion

- Any AV can be bypassed…
- … but a few can be bypassed TOO easily!
- It is no longer admissible from a user/decision-maker perspective!
- No differences between products.
  - The problem lies in the technological and economic models of AV industry!
  - They have to understand that they have to change.
- Marketing and events budgets should be replaced by R&D budgets for a few vendors.

Conclusion (2)

- In a growing context of cyber warfare
  - Our systems and networks are totally unprotected.
  - Any new attack is bound to remain undetected.
- Extremely concerning situation of weakness
- Part of the solution:
  - do not connect sensitive systems to Internet
  - Physically control the use of USB device
  - Enforce strict mail attachment filtering
- It is security policy above all.

Conclusion (3)

- Use your freedom to choose the less inefficient product…
- But
  1. Keep using an antivirus!
  2. Have safe behaviours and rules of conducts when using a computer (security policy first).
  3. Update your OS and applications
- Your destiny is essentially in YOUR hands not in AV (as good or bad as it might be).

Thousands of thanks

- To the board
  - Christophe Devine (Sogeti) Chair
  - Dominique Ciupa (Mag-Securs).
  - Solange Belkhayat-Fuchs (CNIS-Mag)
  - Marc Olanie (CNIS-Mag)
  - Christophe Auffray (Zdnet.fr)
  - Vincent Guyot (ESIEA – SI&S)
- To Anthony Desnos (as an excellent contest manager).
- To the candidates.
- To the attendees.

Now it is time to have Gala Dinner

A short journey in Asterix & Obelix realm