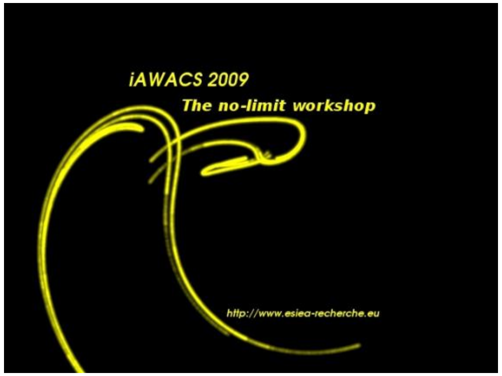
iAWACS2009 Anti-virus “PWN2RM” Challenge Results

iAWACS 2009
Christophe Devine & Samir Megueddem



Goals of the challenge

- Find weak points of AV programs, show how they can be disabled on-the-fly
- Use the EICAR standard anti-virus test to prove deactivation is successful
  - No real malware used!
  - No reverse-engineering of AV either.
  - No reboot.
- 7 AV tested: McAfee, Norton, G-DATA, Kaspersky, DrWeb, AVG, ESET

- Whatever the scope and the legitimity (according to AV vendors) of the attack
  - Give an interesting relative score (which is the lamest which the less worse!).
  - Give a fully verifiable evaluation.
    - Most of the AV test and awards are NOT reproducible at all.

Goals of the challenge (2)

- Disabled in 2 minutes

1. Gain SYSTEM privileges (“at” command)
2. Stop the service (net stop)

- Of course, this can be automated

McAfee

Norton

- Virus scan done in kernel
- Disabled by removing signatures

1. Create a RW shared folder for the "virusdefs" directory
2. Mount \\127.0.0.1\virusdefs as SYSTEM, and simply remove all signatures

- Disabled through \Device\PhysicalMemory (an XP-only trick, wouldn’t work on Vista/7)

1. Fill every page of ekrn.exe with nulls
2. Process crashed, detection disabled

- POC code developed for this purpose

NOD32

- Disabled by removing driver

1. Open the Device Manager then show all non-PNP devices
2. Stop the main G-DATA driver and EICAR test is no longer detected

G-DATA

- Disabled through \Device\PhysicalMemory

1. Trash all code pages of avzkrn, procmon, hips (user-land DLLs)
2. Detection no longer works

Kaspersky

AVG

- Also disabled through \Device\PhysicalMemory

1. Similarly, in-memory overwrite of the user-land scanning component
2. Detection no longer works

Dr Web

- So far, hasn’t been disabled
- NtOpenSection() is blocked (used to access PhysicalMemory mapping)
- But Dr. Web doesn’t block kernel driver loading, so it’s only a matter of time

Comments

- The challenge conditions are realistic (contrary to AV lame comments):
  - Most of users prefer working in « *User with privilege* » modes.
  - Virus can easily work at admin level (even at a lower level).
    - A few AV vendors seems to ignore what critical vulnerabilities are.
- All those attacks can be fully automated.
- Pseudo-code about to be released (if legally possible !).

- Only « proof-by-experiment » approach is valid.
- Other such initiatives everywhere must appear
  - Be inventive and proactive.
  - Create yours!
- Attend iAWACS 2010 in Paris (12-14th may right after the EICAR conference).
  - We intend to go farther and further.
  - User mode, Windows 7, more Avs, poc writing…
- http://www.esiea-recherche.eu/iawacs_2009.html

Conclusion

Q & A

iAWACS 2009
Christophe & Samir