Anti-virus “PWN2RM” Challenge Results

iAWACS 2009

Christophe & Samir

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
- 7 AV tested: McAfee, Norton, G-DATA, Kaspersky, DrWeb, AVG, ESET

McAfee

- Disabled in 2 minutes

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

- Of course, this can be automated

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

NOD32

- 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

G-DATA

- 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

Kaspersky

- Disabled through \Device\PhysicalMemory

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

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

Q & A

iAWACS 2009

Christophe & Samir