esiea recherche

http://www.esiea-recherche.eu/iawacs_2010.html

Rules of the iAWACS 2010 PWN2KILL Contest

The PWN2KILL Contest aims at performing a comparative evaluation of commercial antivirus software against actual threats. An actual threat can be defined as any threat that is operationally viable. The purpose is to show that given fixed actual malware threats, the different existing antivirus software are of unequal quality. While a few of them are able to proactively detect unknown malware using known malware techniques, most of them are just able to detect most of the known malware (not all of them).

Moreover, the in-depth analysis of existing antivirus software shows that a significant number of malware technique that have been published -- by hackers, malware writers, researchers in computer security and computer virology -- are still not taken into account by commercial antivirus products while those techniques indeed represent actual threats. Consequently, it is more than useful for the end user and the final consumer (since AV software are products that we buy) to know which antivirus at the less worst and which are the worst.

The contest board will be composed of a bailiff, of five professional journalists from the computer technical press and of three personalities from the scientific/hacking community renowned for their personal ethics and skills. Its role will be to record the test results, decide of their validity and elect the three most efficient attacks.

The contest will be based on the only admissible approach: the experiment and the attacker's view.

The rules are very simple:

1. A number of computers -- each of them with an antivirus installed -- will be available. The environment will be

    - Windows 7 (in a virtual machine for an easy reconfiguration purpose).
    - User mode (without privilege).
    - No connection to the Internet (to avoid ``external'' attacks or manipulation during the contest). However to enable truly network-based attacks (input and/or output data), it will be possible upon request to open temporarily an access to the Internet provided that no attack will be launched from the testing machine towards external systems.
    - Common applications installed (Microsoft suite, Open Office Suite, PDF reader...). Any additional application can be added upon request or can be freely used through personal USB devices.
    - A printer will be available through the network (spec data available upon request).

2. Each participant will come with his (malware) code(s) to test against the antivirus software. He can perform any action that a normal user can do (including rebooting the computer, closing a session, using USB devices...). In case of ``proactive'' warning from the operating system or from any application, the user is free to follow them or not. Any user has not to be an expert in computers in order to evaluate and interpret technical warnings that sometimes refers to normal behaviours. As an example, warnings like ``*an application is attempting to become resident. Do you allow it?*'' has no meaning for a grandmother using a computer. She is free to allow it (and she actually and systematically does it)!

3. In order to make a comparative and fair testing, any code must be tested against ALL antivirus selected for the challenge. The test will consist in two steps:
    a. firstly the code(s) will be scanned (on demand analysis),
    b. then used as intended (on-access analysis).

4. Any participant will have first to announce what effect/attack he intends to perform. The board will decide whether this attack is admissible or not. An admissible attack is an attack which affects availability, integrity and/or confidentiality of the system and/or the data (data system, user data...).

5. Any participant will have to write a short technical summary of his attack(s) which will be published on the iAWACS 2010 website. He will have to present his attack(s) during the contest debriefing. A copy of its code will be given to the organizers of the challenge.

For fairness purposes, no participants working for any AV company or any company sharing common interest with any AV company will be allowed to participate. Any participant will thus have to sign an assessment form confirming he is not working for such companies.

The organizers of iAWACS 2010 and of the PWN2KILL challenge have selected the following antivirus software (this is an initial list; additional software may be considered):

- Avast
- AVG
- Avira
- BitDefender
- DrWeb
- F-Secure
- GData
- Kaspersky
- McAfee
- Microsoft AV
- NOD32
- Norton Symantec
- Trend Micro

Only commercial licences will be tested -- in other words they will be anonymously bought in public stores/website (no demo or free version). The antivirus will be updated right before the beginning of the challenge.

The organizers will publish a technical summary of the results once validated by the contest board. No communication will be done directly towards the AV vendors. Only a technical communication and press conference will be organized during the iAWACS 2010 event. A technical summary will be available on the iAWACS 2010 website. The complete data and codes collected will be communicated only to the French CERT-A for analysis and feedbacks. No code will be neither published nor distributed.

Any participant is free to communicate later on about his test/code/attack performed during the contest. In this case, iAWACS 2010 organizers are nor responsible for that communication.