Achilles v. 1.0

Developed by: EDG/AED

DESCRIPTION

- Achilles is a capability that provides an operator the ability to Trojans an OS X disk image (.dmg) installer with one or more desired operator specified *executables* for a one time execution.

TOOL REQUIREMENTS

- Target Computer.....................Intel Core 2 Processor, OS X
    - Tested on OS X 10.6

BUILD/INSTALLATION INSTRUCTIONS

- Make a *tools_directory* containing the desired execution files and a bash script *inst*
    - Edit *inst* to call all *executables* with the appropriate flags
    - *inst* will run from the directory where it is saved therefore it can call an *executable* as if it were in the same directory
- Obtain the dmg installer *installer-name.dmg* that you want to trojan
- Run *achilles.sh* with the appropriate parameters (*Usage: ./achilles.sh {tools directory name} {DMG file}*)
    - Example: *./achilles tools_directory_name installer-name.dmg*
- Trojaned dmg will have the name *installer-name-final.dmg*
- The trojaned DMG files now contains the *executables*

EXECUTION

- The trojaned DMG should behave similar to the original DMG
- Upon running the trojaned DMG on target, a window should appear prompting the user to drag the Application to the Applications directory
- The first time a user runs the Application all *executables* will run after the real application has launched
- After *executables* have run, they, and all other traces of Achilles based files, will be removed securely from the ".app"
- The resulting ".app" will exactly resemble the original un-trojaned ".app"
- Subsequent calls to the ".app" will no longer call the *executables* since they will have been deleted

ISSUES

- If a User Agreement is presented in the original non-trojaned DMG, it will not appear in the trojaned DMG