Mac OS X Hacks

hack value: n.

Often adduced as the reason or motivation for expending effort toward a seemingly useless goal, [...] but this cannot really be explained, only experienced. As Louis Armstrong once said when asked to explain jazz: "Man, if you gotta ask you'll never know."

http://www.catb.org/~esr/jargon/html/H/hack-value.html

GUI Mods und versteckte Optionen

- NIB Files, Localizations
  - System/Library/CoreServices/loginwindow.app/Contents/Resources/German.lproj/AboutThisMac.strings
  - ABOUT_BOX_SINGLE_PROCESSOR_FIELD_FORMAT
  - Addressbook, ImageCapture
- defaults, plists
  - ~/Library/Preferences/com.apple.finder.plist
  - defaults write com.apple.finder AppleShowAllFiles ON
  - AppleShowAllFiles
  - QuitMenuItem

Hinter den Kulissen

- lsof, ioreg
  - ioreg -l | grep -A 5 -B 5 temperatu
  - sudo lsof | grep LISTENING
- eastereggs
  - Mail.app/Contents/Resources/senders.tiff
  - good old times
- /usr/libexec/WaitingForLoginWindow

Tiefer im System

- class-dump
  - Mail.app, Apple802.framework, SystemUIPlugin.framework
  - http://elliotth.blogspot.com/2005/05/mac-os-104-slideshows-from-java.html
- iTMS Movie Ripping
  - sudo tcpflow -c | grep -E 'GET|Host'

Niemand mag ObjC

- PyObjC
  - http://developer.apple.com/cocoa/pyobjc.html
  - /Developer/Python/PyObjC/Examples
- PyInject
- MACH Injections....

MACH Injections

- Ein “Feature” von ObjC
- Bekannt seit MacHack 2003
  - http://rentzsch.com/papers/overridingMacOSX
- mach_*, SIMBL, APE, InputManager, (..?)
- mailHack, Taboo

Das ewige Thema

- Klassische Viren für Mac OS X
  - MP3Concept
  - rsrc_hook, mach-cat
- Trojaner natürlich auch
  - iWork ReadMe

FunStuff

- killall Dock.app während Genie
- Slow Motion Effekt durch Shift key
- Firewall stealth mode
- Watchdogimplementierung -> pistole am kopf
- Safari Art Bug
  - http://rentzsch.com/bugs/modernArtWithSafariCanvasBug

Kryptoecken

- CDSA
  - CardServices (Lustige Bildresourcen)
  - VM
  - FileVault
  - Keychain
- QuickTime/iTunes
- OpenSSH/OpenSSL

Script Kiddies

- Rootkits
  - Opener
  - Metasploit
- Datensparsamkeit
  - rendezvous

Bonusspiele

- FireWire DMA
- OpenFirmware
  - Pong Game
- http://docs.info.apple.com/article.html?artnum=61798