Unpacking bird’s eye view

Ero Carrera
Sabre Security GmbH
The idea

• Thought it would be cool to be able to see how unpacking goes

• as easy as tracing all memory writes and EIP location as the unpacker goes on its way

• i’m a slacker and lame, don’t wanna worry about anti-db g tricks and the like... then... have write my own tool

• cool thing is, I already had it :)


Gather data

- Run some packers through my black ‘bochs’
Plot data

- I plotted most of the packer’s data with Mathematica
- EIP = blue
- Memory writes = green
Questions?