Boutique Kit

Playing WarGames with expensive rootkits and malware

Josh “m0nk” Thomas

Opening Question

- Hands up if you run Android
- Keep ‘em up if you run a custom ROM / Kernel
- Down if you actually compiled it
- Back up if you didn’t look at the source
- Back up if you didn’t do a FULL source audit
- Don’t lie, Santa Claus and the NSA already know the answer

./whoami

- Josh “m0nk” Thomas
- @m0nk_dot

- Paid by the epic people @ Accuvant Labs
- Used to get paid by other folk in a prior life

- Q: Why listen to me?
- A: TBH, Not a damn clue

- Current slides can always be found here:
  - https://github.com/monk-dot/David-Byrne.git

echo $AGENDA

- Boring Kit – The public space of rootkits and malware
- No Name Given: Non Public Players and the new rules
- War Game 1: Hide deep, hide long
- War Game 2: Run off the processing grid
- War Game 3: Is it cold in here?
- Revisiting Tic-tac-toe: The fun we can have

BORING KIT

The public space of rootkits and malware

I’m sure its fascinating but…

Uber 1337 h4x0r <3 teh Malwarez

NO NAME GIVEN

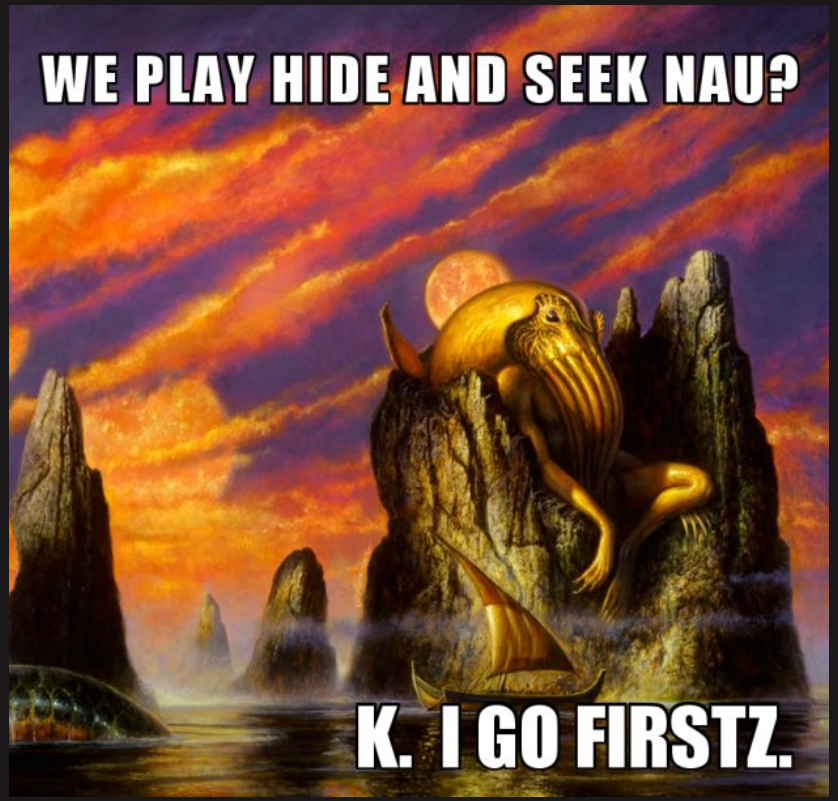
Non Public Players and the new rules

Nameless people doing interesting things

Out come the Androids

Cost of the game

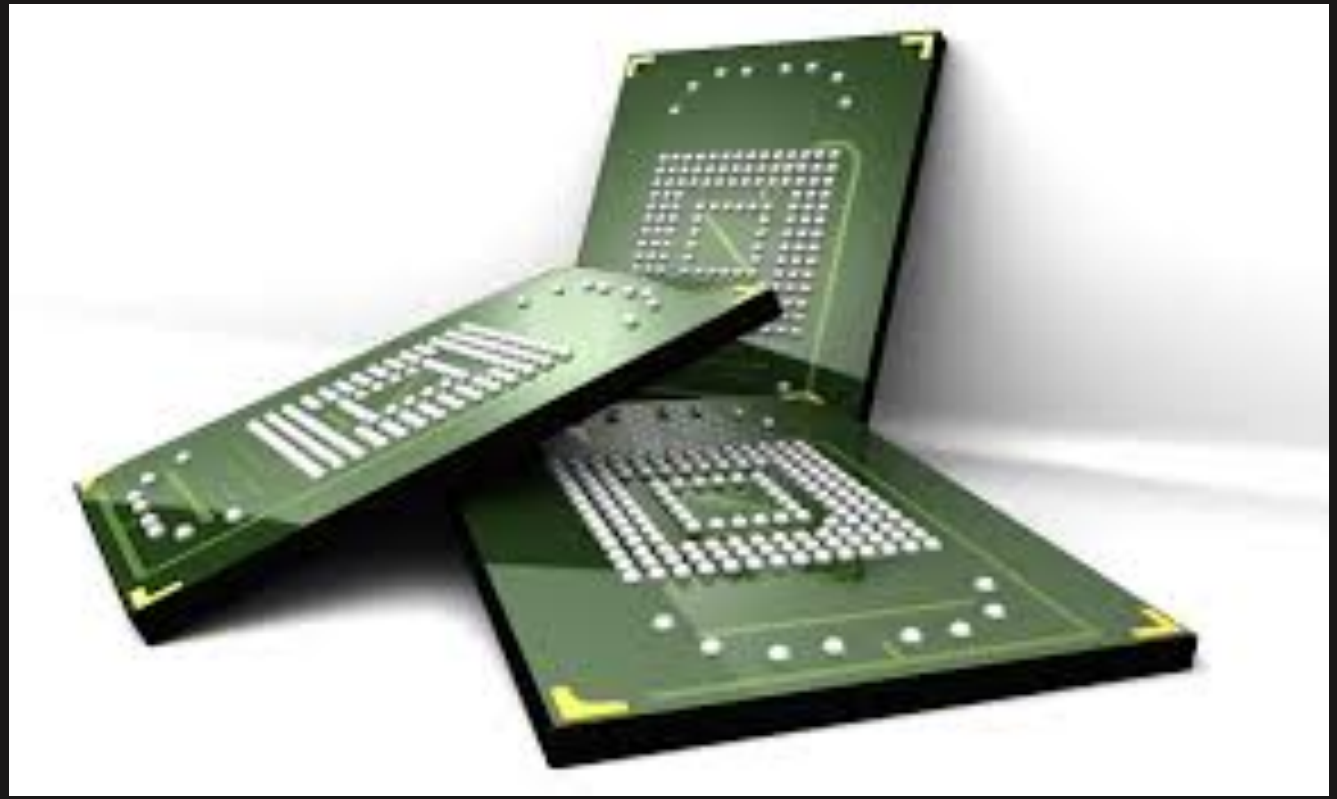
Rules of the game



WAR GAME 1

Hide deep, hide long

NandX



Content goes here

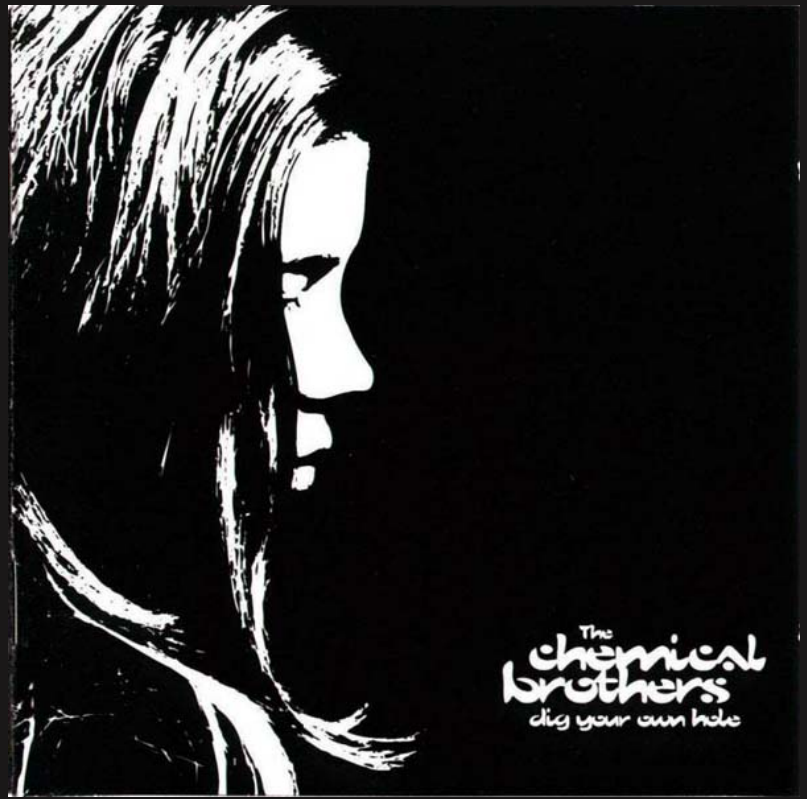
- OMG - Text

Stop – Demo Time!

WAR GAME 2

Run off the processing grid

Clock Locking Beats



WAR GAME 3

Is it cold in here?

Project Burner

REVISITING TIC-TAC-TOE

The fun we can have

Stuff Goes here

- And here!

Whatever…

Questions?

https://github.com/monk-dot/David-Byrne.git

Josh Thomas
@m0nk_dot
jthomas@accuvant.com

fin

1125 17th Street, Suite 1700, Denver, CO 80202
800.574.0896
sales@accuvant.com
www.accuvant.com