Boutique Kit

Playing WarGames with expensive rootkits and malware

Josh “m0nk” Thomas

display(eratta_dc21.drink);

This is Ricky…

Ricky likes to drink…

Drink when you see Ricky…

display(eratta_dc21.abuse);

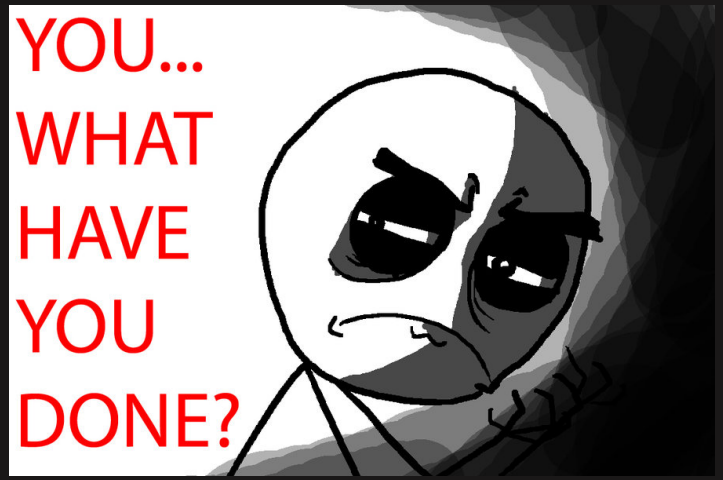
Opening Question

- 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

preso.start()

<header>

- @m0nk_dot
- Why?
  - Because… logic



- My opinions != Accuvant Labs
  - … blah blah blah blah blah
- This is about understanding a problem so we can fix it

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

But...

DO NOT CARE

Not really 0-Day

- Just iterative, boring, annoying crap
- Capitalism trumps innovation
- Disposable
- Non Targeted
- zzz……

Don’t listen to me

- Just go find the slides from damn near any recent talk from Mudge.

NO NAME GIVEN

Non Public Players and the new rules

RTFM: Generic Game Rules

- 2+ players
- Game Play Mechanics
- Goals

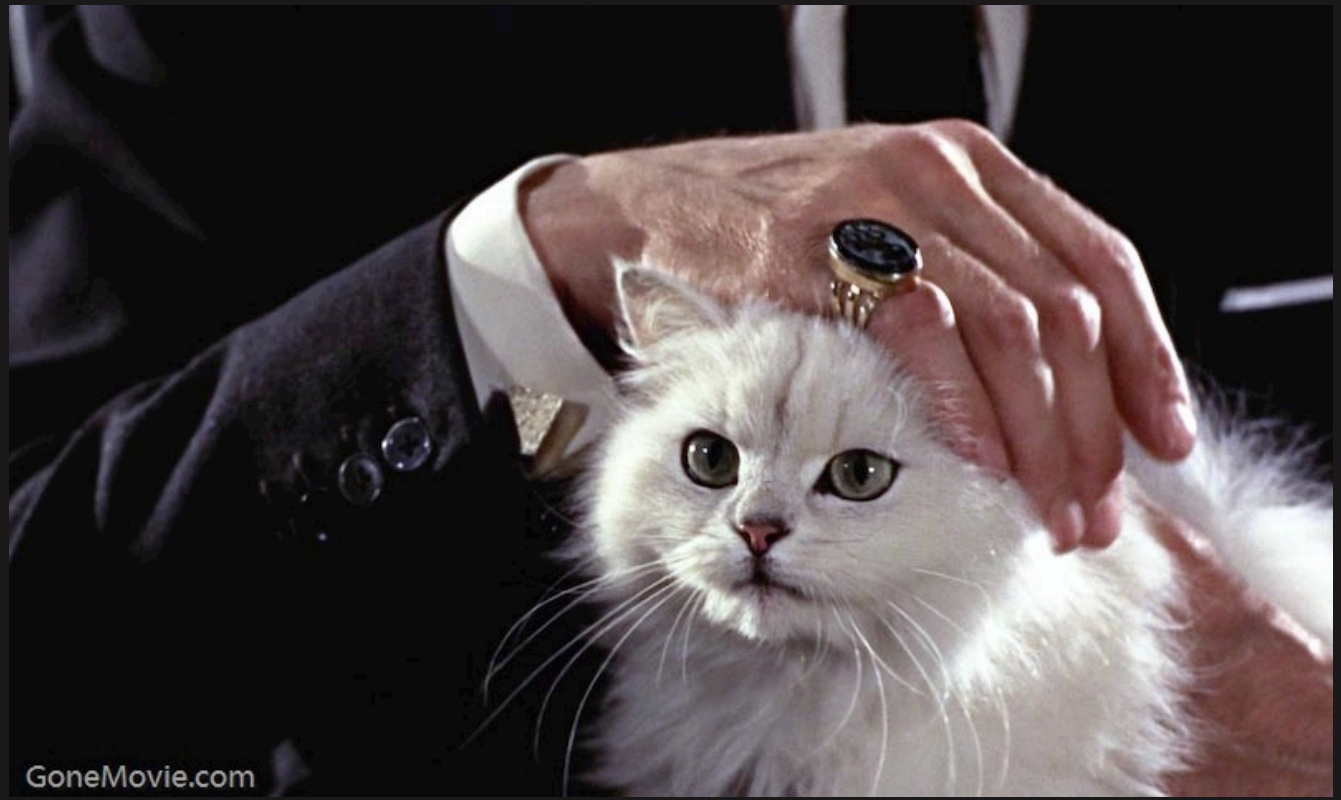

PLAYER 1

Nameless people doing interesting things

Define: Player 1

- <insert generic government / state sponsored image here>
- <insert generic large multinational corporation image here>

You know… “those people”



Maybe Even…

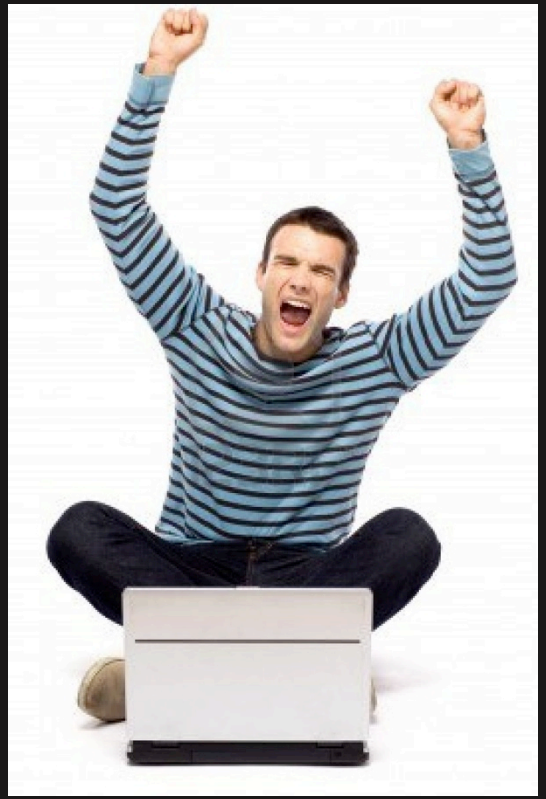
Or even:


PLAYER 2

Define: Player 2

Define: Player 2

Define: Player 2



Define: Player 2

Game Mechanics

- We need all teh 0-Days -> gift wrap
- We need all teh Devices -> package

All teh 0-Dayz!!!!!

- Still kind of boring
- Not the real point
- Disposable...

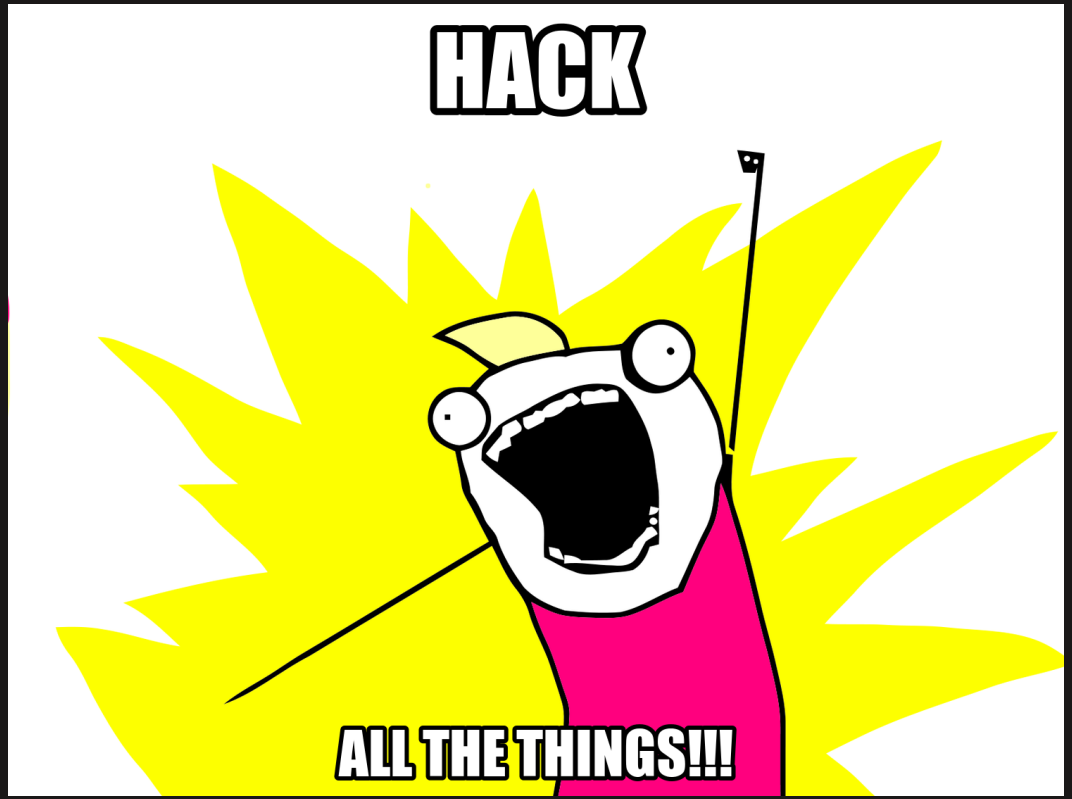
Cost of the 0-Day?

Need moar!

No, MOAR!!!!

ok, that's better

All teh Devices!



I need a new computer

Moar computer

Computer!

But I run Android, I’m special?

Sure…

Unless I had….

ok, that's better

Game mechanics

- Kit / Implant is not an 0-Day
- Actually costs real money
- Actually takes real time to dev
- But… Drudgery != Sexy

Dev time ☹

Moar dev time ☹ / Real Job ☹ ☹

Years to Dev = $$$$$

Years to Dev = $$$$$






Years to Dev = $$$$$

Well… it's something

Goals

Ok, we have a game!

Didn’t take long…

And the winner is….

Whatever… “jerks”

Protecting the real investment

Protecting the real investment

But wait, I want to know more!

Getting popped and burned

Don’t do that to poor Ricky, OK?

Final Rules of the game

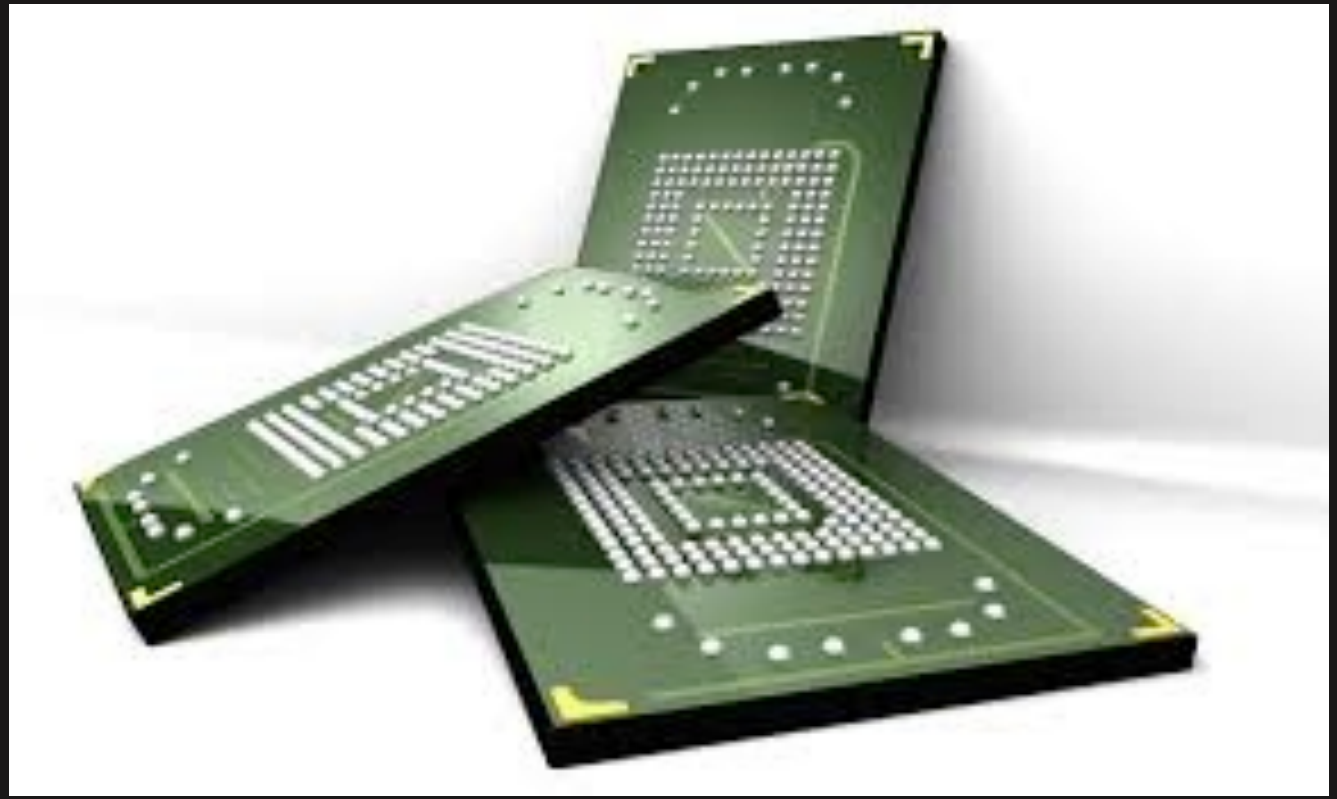
define

- “Air to Glass”
  - Playing with remote code execution that never touches data storage.

WAR GAME 1

Hide deep, hide long

NandX



Stop – Demo Time!

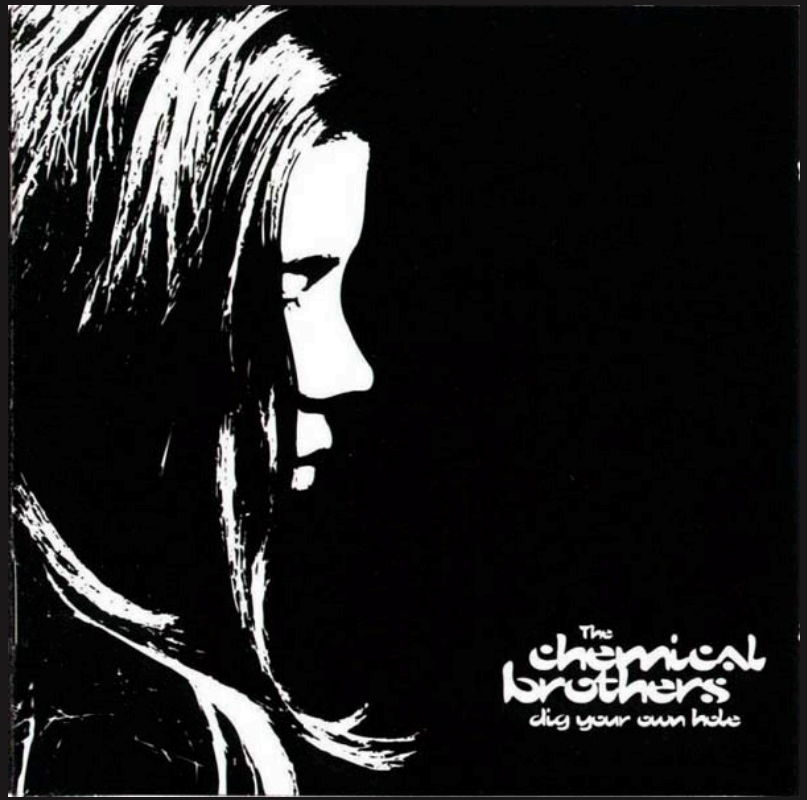
find

- https://github.com/monk-dot/NandX

WAR GAME 2

Run off the processing grid

Clock Locking Beats



find

- https://github.com/monk-dot/ClockLockingBeats

WAR GAME 3

Is it cold in here?

Project Burner

Random fire pic from google

Coming to a github near you!

find

- https://github.com/monk-dot/ProjectBurner

REVISITING TIC-TAC-TOE

The fun we can have

Stuff Goes here

- Open source all the things
- Burn all the tricks
- Sadden all the Rick Ross
- Harder you must try

fatality()

#CharlieSheenWinning?

Whatever…

Questions?

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

Josh Thomas
@m0nk_dot
m0nk.omg.pwnies@gmail.com

jthomas@accuvant.com

fin

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