Code signing flaw in macOS

```
> whoami

Thomas Reed
Director of
Mac & Mobile
@ Malwarebytes

@thomasareed
```

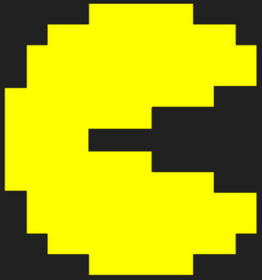
Not rocket science

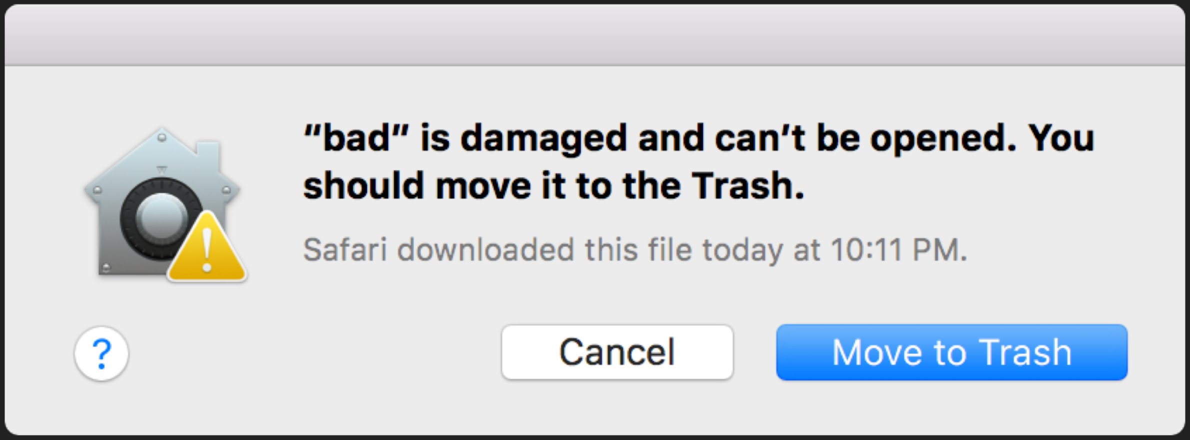
..but why should it be when we have threats like this?

```
    <key>ProgramArguments</key>
    <array>
        <string>osascript</string>
        <string>-e</string>
        <string>do shell script "osascript
~/Library/LaunchAgents/com.apple.Yahoo.plist"</string>
    </array>
```

Code signing on Mac

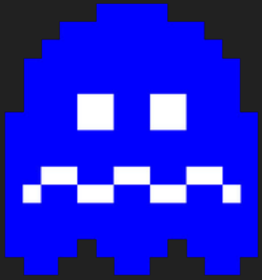
- Most apps code signed today
- Unsigned apps not allowed by default
- macOS verifies code signature before running downloaded apps





"bad" is damaged and can't be opened. You should move it to the Trash.

Safari downloaded this file today at 10:11 PM.



Code signing on Mac

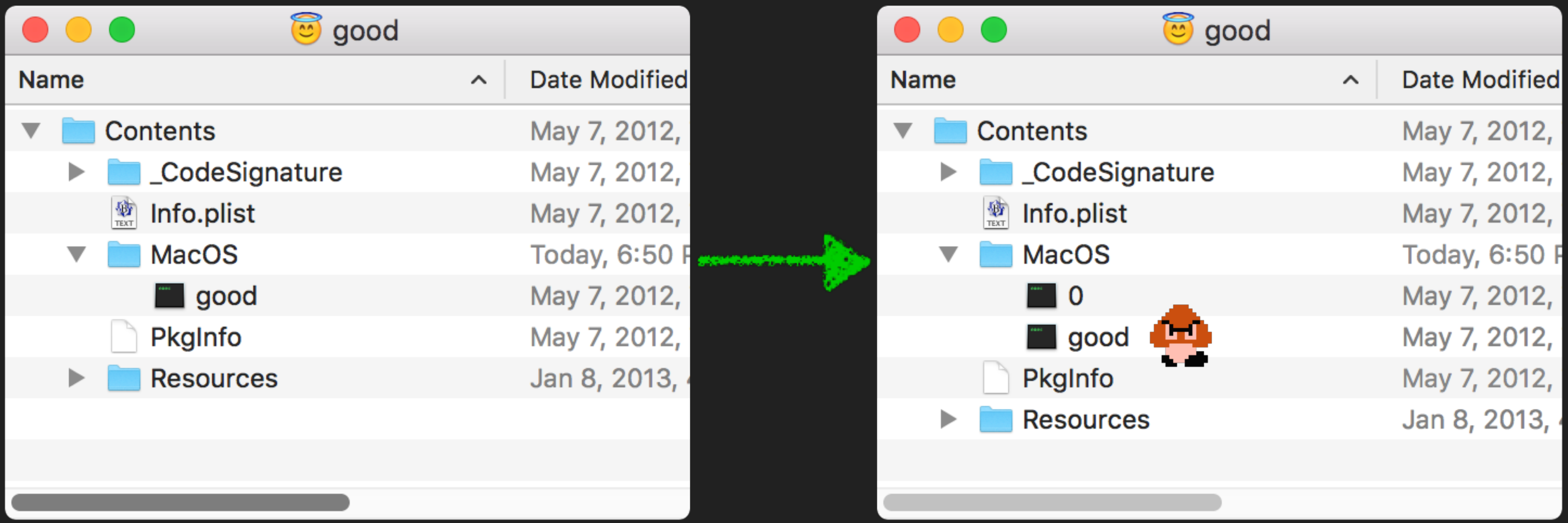
- Apps are "quarantined" when downloaded
- Gatekeeper only checks code signature for quarantined apps
- After opening, quarantine flag is removed
- Code signature is never checked again!

Infecting an app

> Rename "good" to something else - like "0"

> Add malicious executable named "good"

> "good" executable loads "0" to make the app seem normal



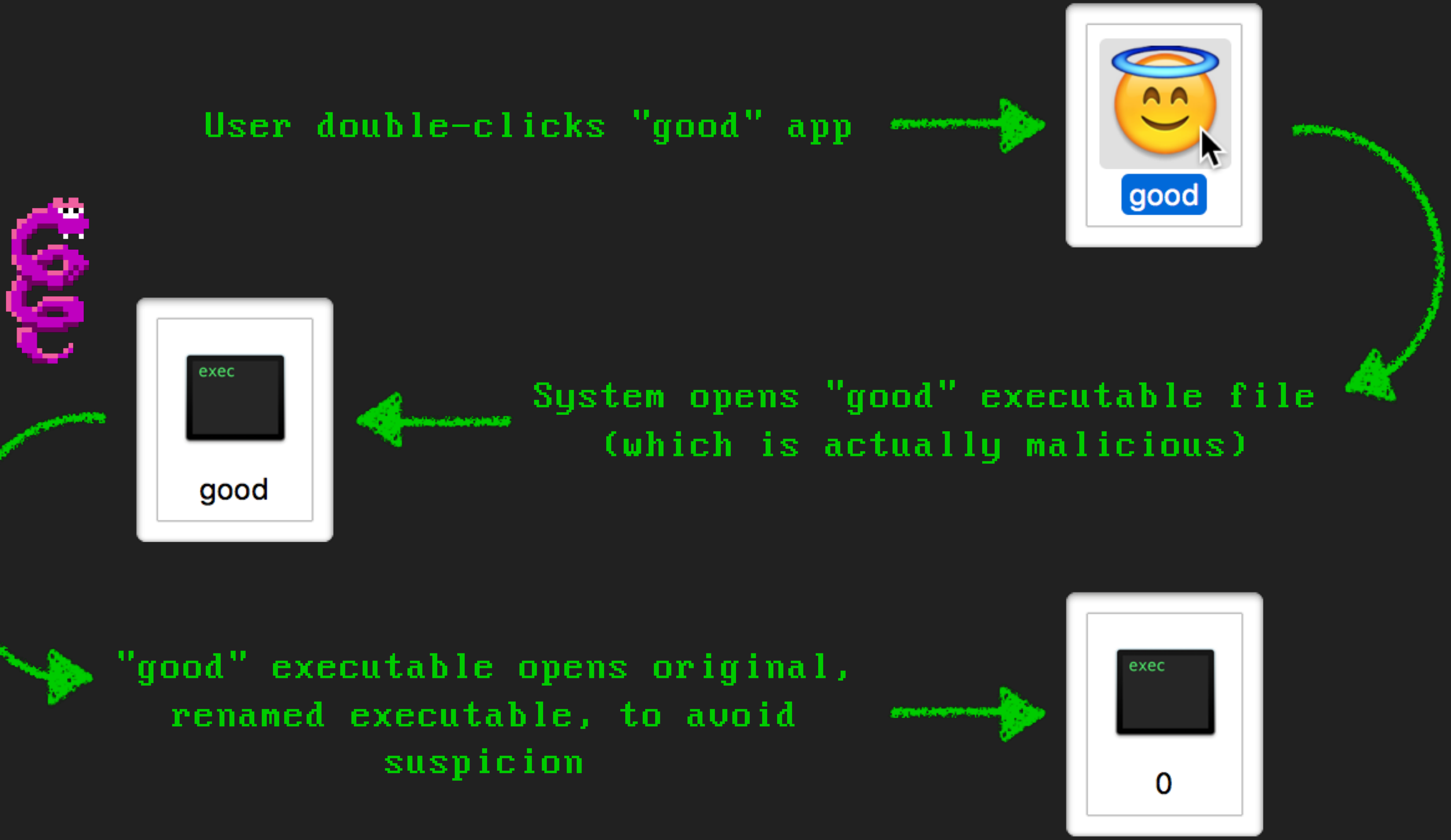
good

Name	Date Modified
Contents	May 7, 2012,
_CodeSignature	May 7, 2012,
Info.plist	May 7, 2012,
MacOS	Today, 6:50
good	May 7, 2012,
PkgInfo	May 7, 2012,
Resources	Jan 8, 2013,

good

Name	Date Modified
Contents	May 7, 2012,
_CodeSignature	May 7, 2012,
Info.plist	May 7, 2012,
MacOS	Today, 6:50
0	May 7, 2012,
good	May 7, 2012,
PkgInfo	May 7, 2012,
Resources	Jan 8, 2013,

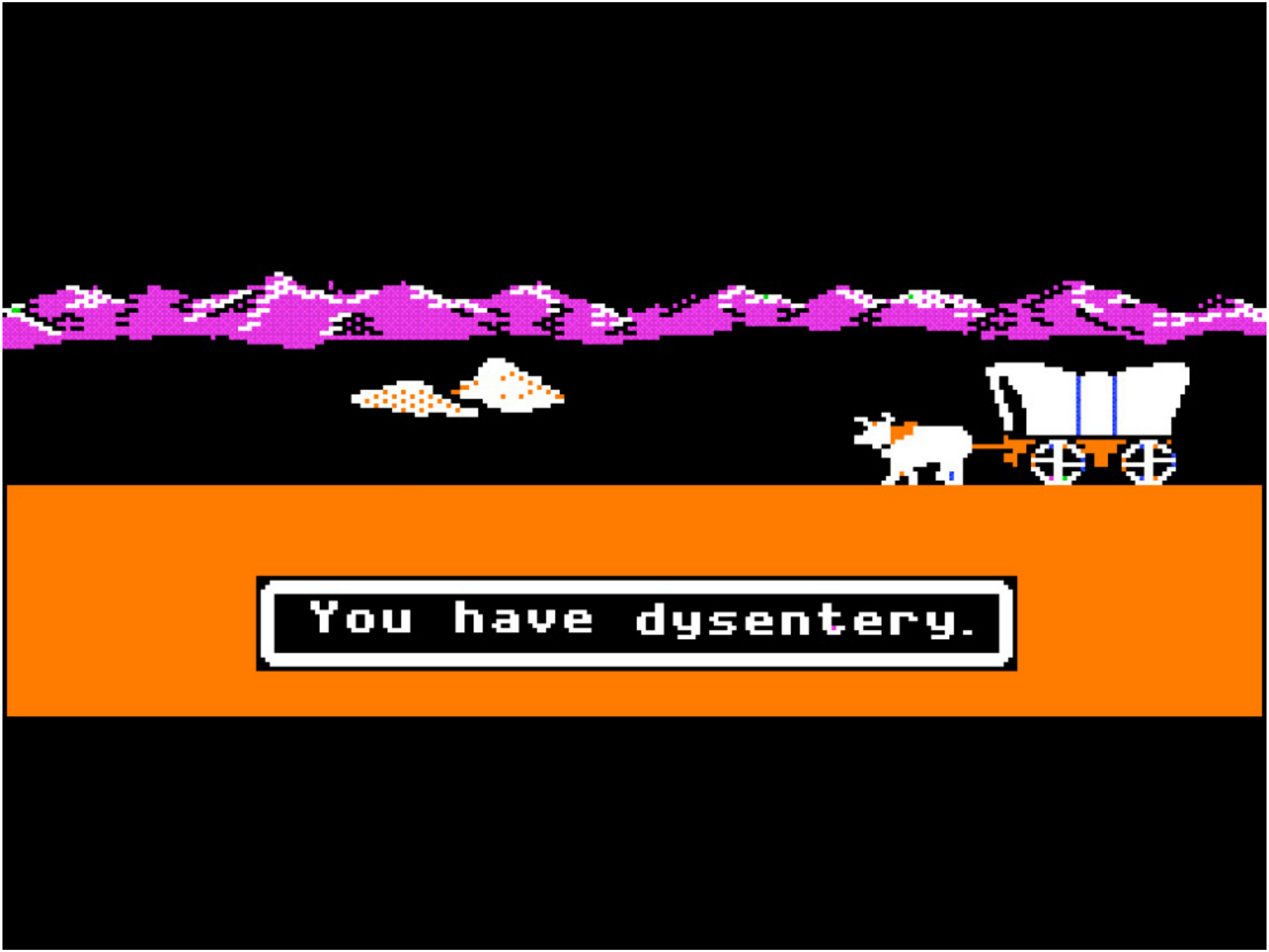
Infecting an app



User double-clicks "good" app

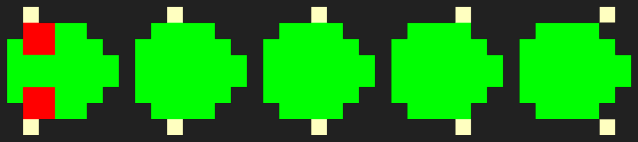
System opens "good" executable file (which is actually malicious)

"good" executable opens original, renamed executable, to avoid suspicion



You have dysentery.

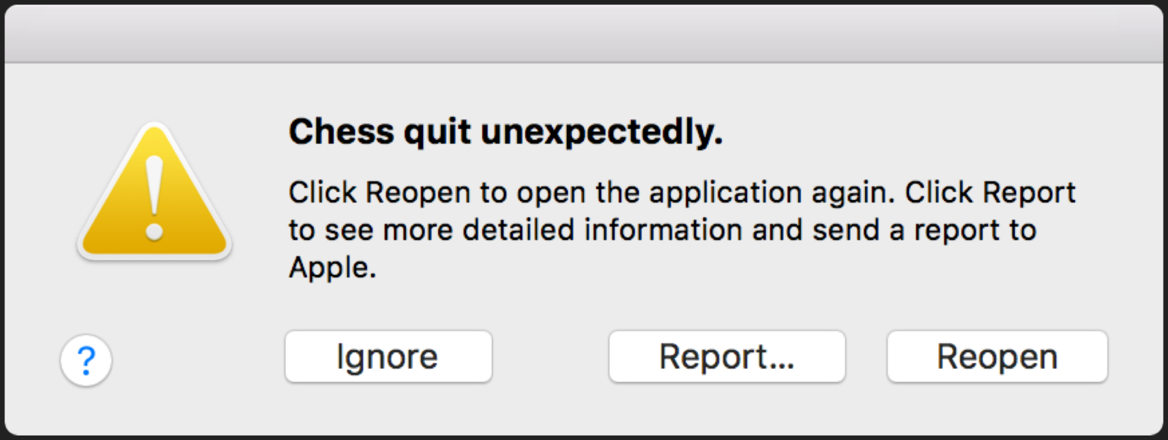
How hard is this?



- Not very!
- 22 lines of Swift code - malicious executable
- 18 lines of AppleScript - dropper part 1
- 16 lines of shell script - dropper part 2

Exceptions

- Apple's apps can't be modified
- If you try it, they crash
- Malicious code still runs!

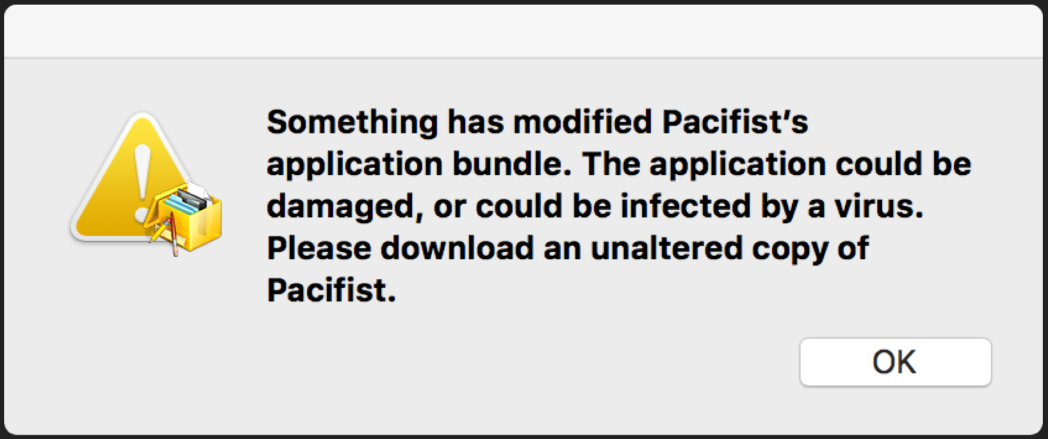


Chess quit unexpectedly.

Click Reopen to open the application again. Click Report to see more detailed information and send a report to Apple.

Exceptions

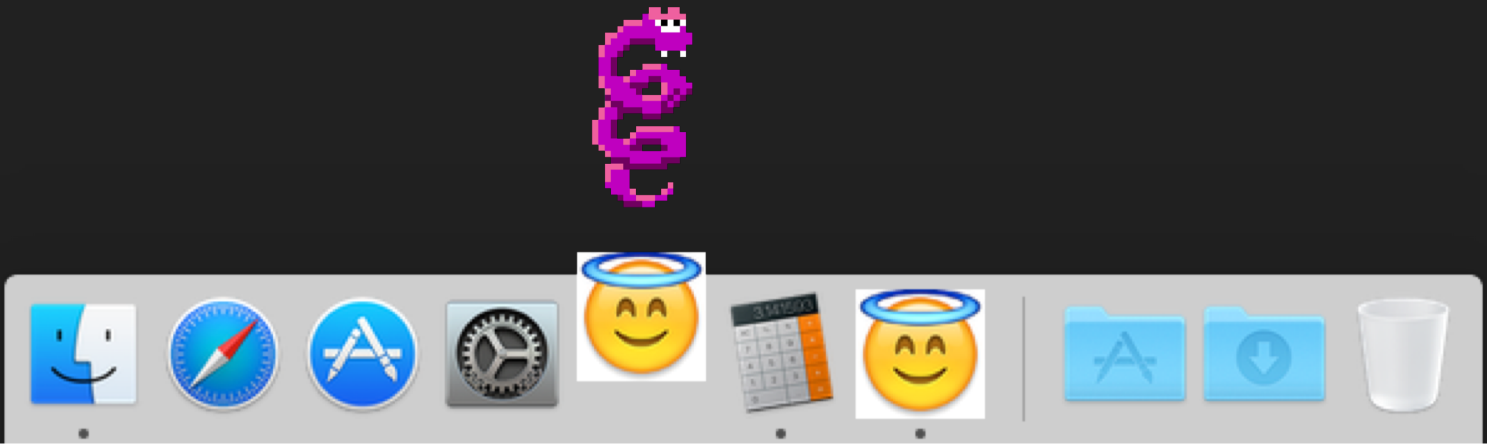
- Some third-party apps have self-protection
- If you change them, they'll let the user know
- Malicious code still runs!



Something has modified Pacifist's application bundle. The application could be damaged, or could be infected by a virus. Please download an unaltered copy of Pacifist.

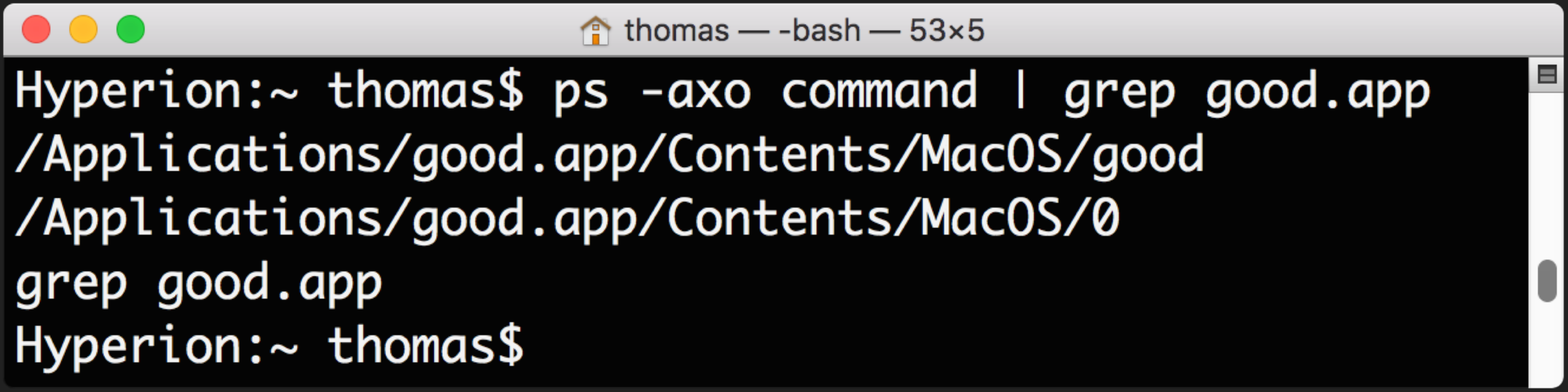
Potential giveaways

- Doubled Dock icons
- Malicious process shows as bouncing icon
- Original process appears normally
- Can be prevented



Potential giveaways

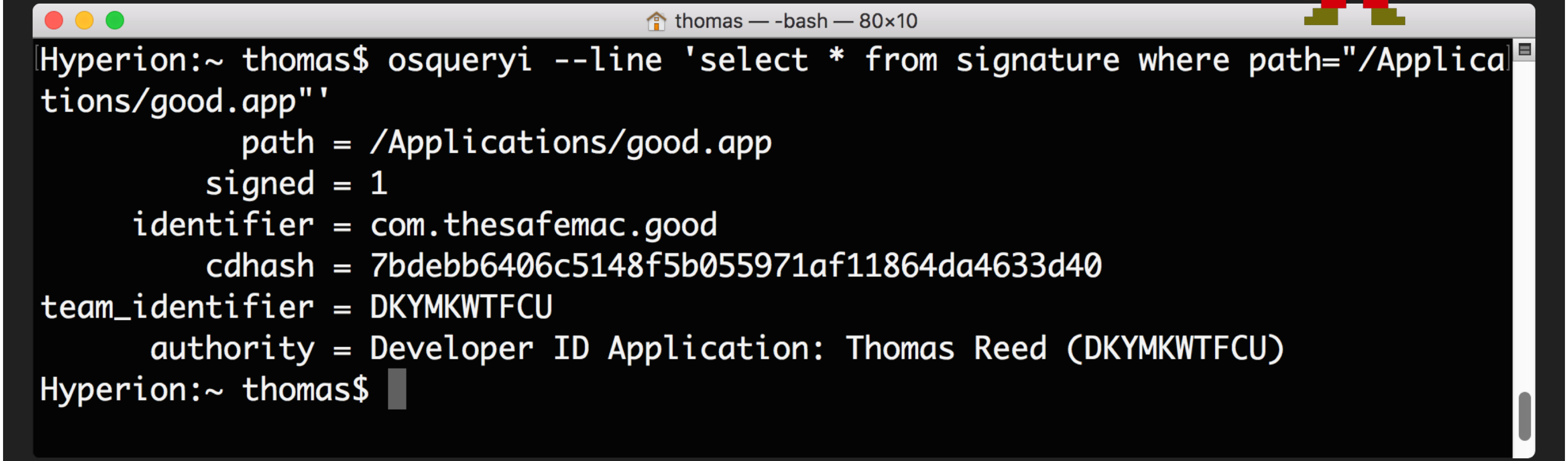
- Two processes in Activity Monitor
- Two processes in ps output
- Could make this less suspicious fairly easily



```
Hyperion:~ thomas$ ps -axo command | grep good.app
/Applications/good.app/Contents/MacOS/good
/Applications/good.app/Contents/MacOS/0
grep good.app
Hyperion:~ thomas$
```

How to detect

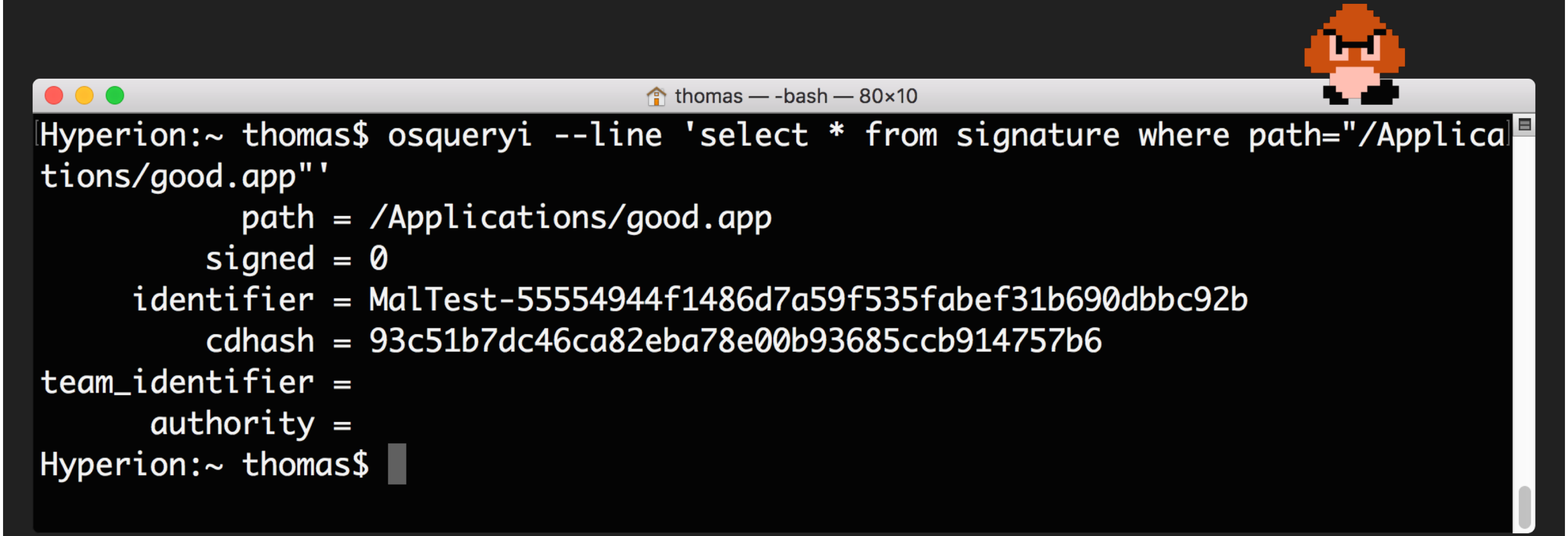
> Use osquery to check signature



```
Hyperion:~ thomas$ osqueryi --line 'select * from signature where path="/Applica
tions/good.app"'
           path = /Applications/good.app
         signed = 1
     identifier = com.thesafemac.good
         cdhash = 7bdebb6406c5148f5b055971af11864da4633d40
team_identifier = DKYMKWTFCU
      authority = Developer ID Application: Thomas Reed (DKYMKWTFCU)
Hyperion:~ thomas$ 
```

How to detect

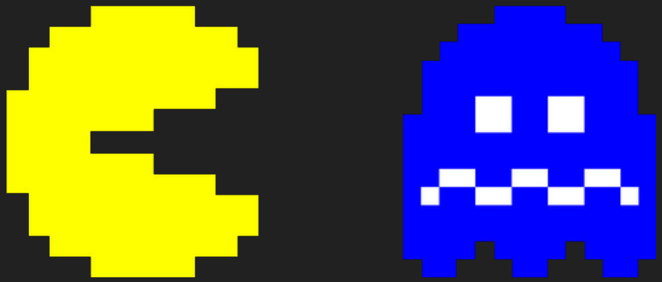
> Use osquery to check signature



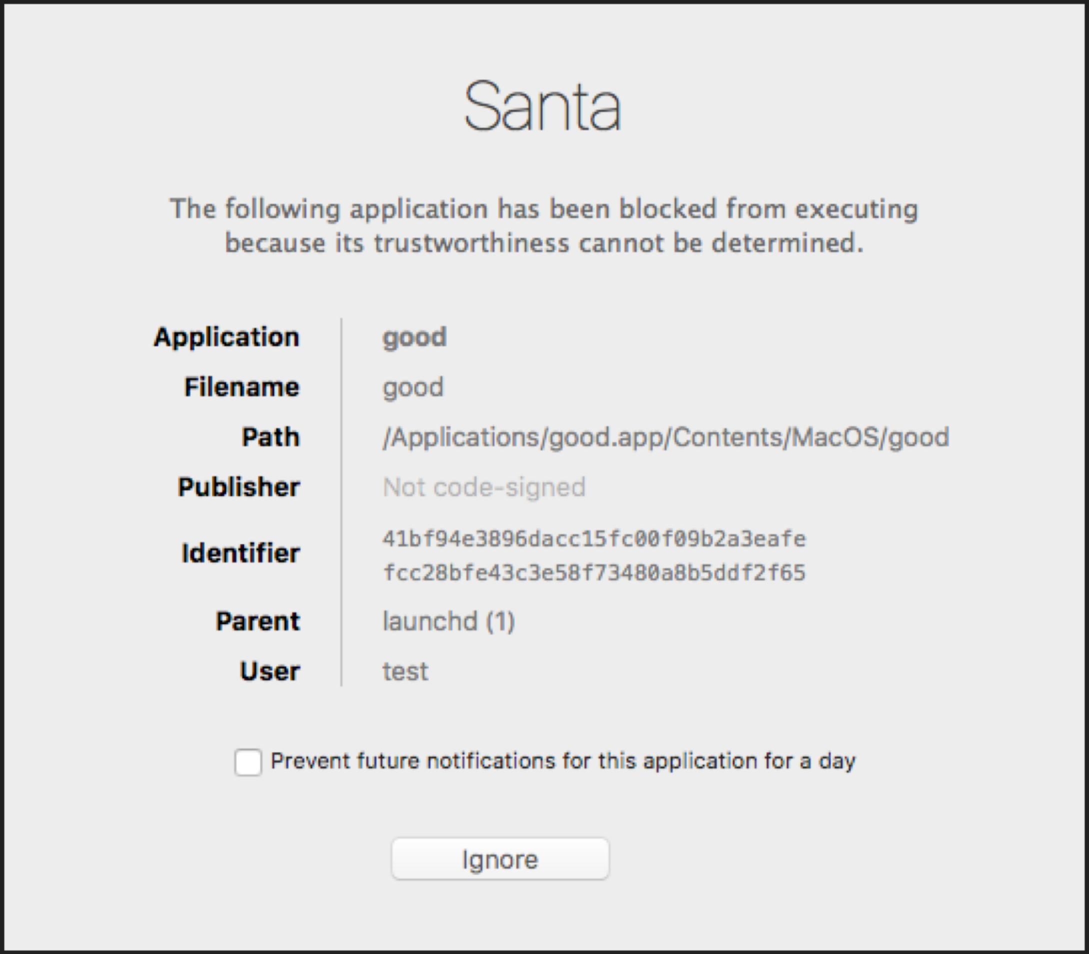
```
Hyperion:~ thomas$ osqueryi --line 'select * from signature where path="/Applica
tions/good.app"'
           path = /Applications/good.app
         signed = 0
     identifier = MalTest-55554944f1486d7a59f535fabef31b690dbbc92b
         cdhash = 93c51b7dc46ca82eba78e00b93685ccb914757b6
team_identifier =
      authority =
Hyperion:~ thomas$
```

Naughty or nice?

- Possible solution: Santa
  https://github.com/google/santa
- Use in lockdown mode to allow only whitelisted apps to run
- Modified apps will be blocked



Naughty or nice?



Santa

The following application has been blocked from executing because its trustworthiness cannot be determined.

Application	good
Filename	good
Path	/Applications/good.app/Contents/MacOS/good
Publisher	Not code-signed
Identifier	41bf94e3896dacc15fc00f09b2a3eafe fcc28bfe43c3e58f73480a8b5ddf2f65
Parent	launchd (1)
User	test

☐ Prevent future notifications for this application for a day

Naughty or nice?

- Pros:
  - Difficult to bypass
- Cons:
  - Whitelisting will keep you jumping with user requests!
  - Unrealistic for certain users (eg, developers)

Solutions?

- Apple could check signatures more often
  - Potentially resource-heavy
- Developers need to check their own signatures

Bonus points

............Space Invaders.....10 points

.........................Blinky (PAC-MAN).....15 points

.......................Centipede.....20 points

.............Pooka & Fygar (Dig-Dug).....50 points

.....................Goomba (Super Mario).....75 points

....................Spider (Centipede).....100 points

........snake & scorpion (Pitfall).....200 points

...........................Coily (Q*bert).....500 points