Popping shells with your cereal box

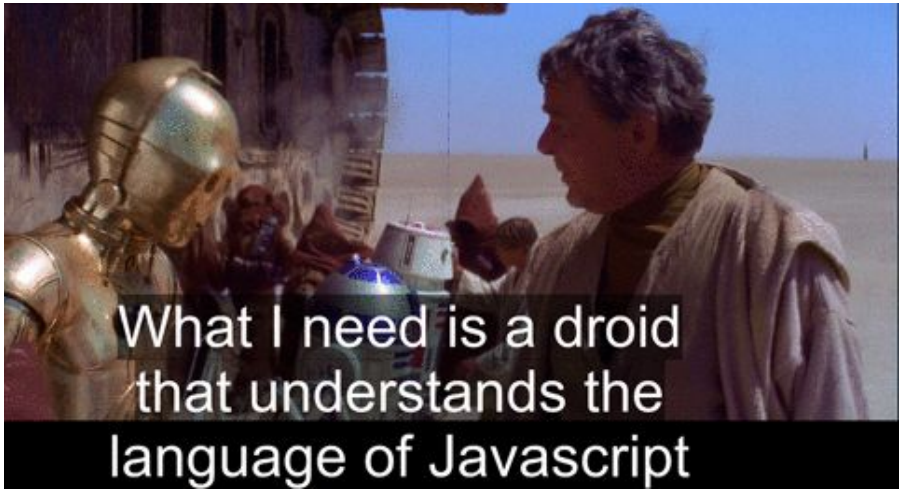
Michael West
T3h Ub3r K1tten

Colin Campbell
magicspacekiwi

humans.txt

Michael West

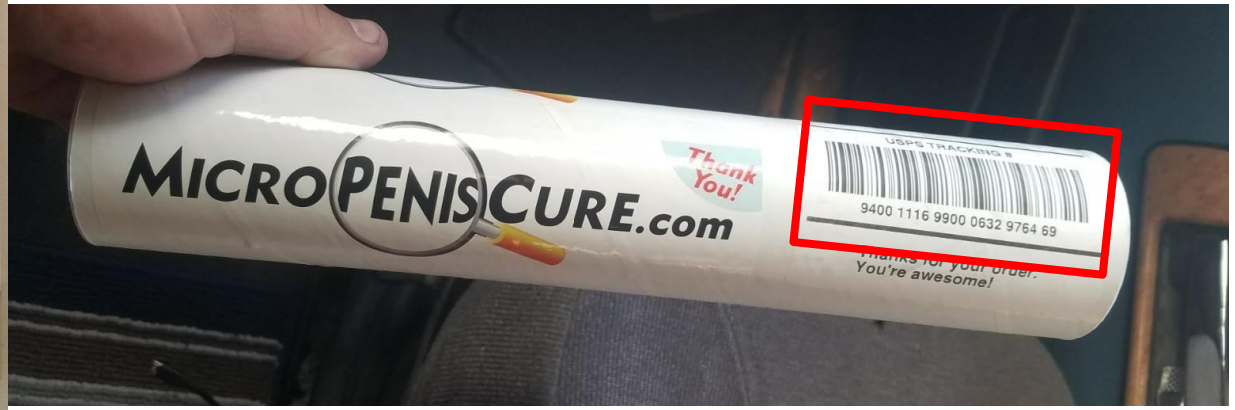
Enjoys scanning long barcodes on the beach



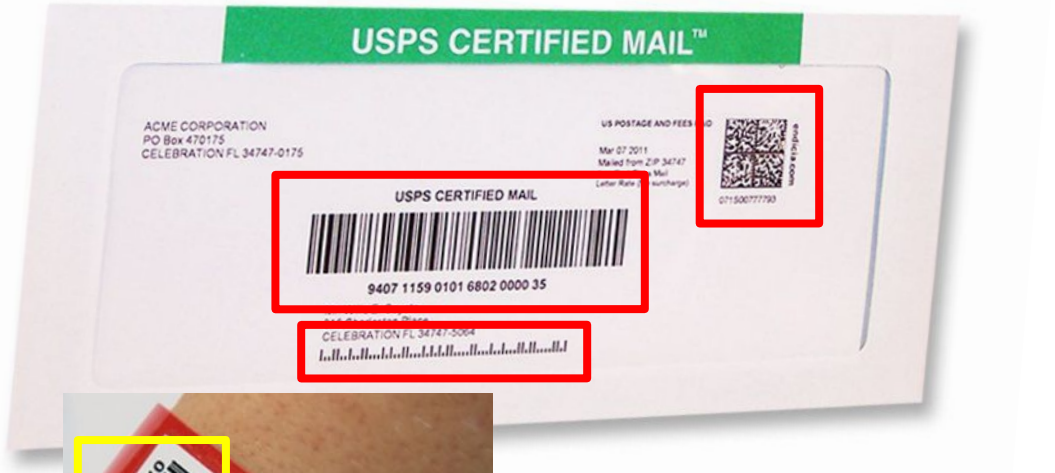
magicspacekiwi

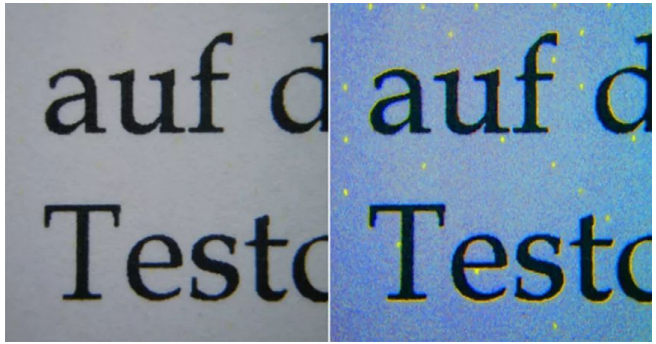
Professional internet tube filler
"Master of the web"

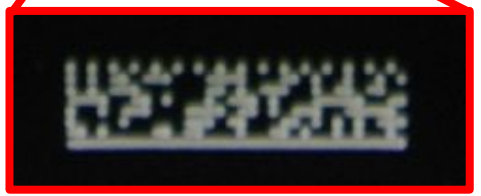
Barcodes are everywhere



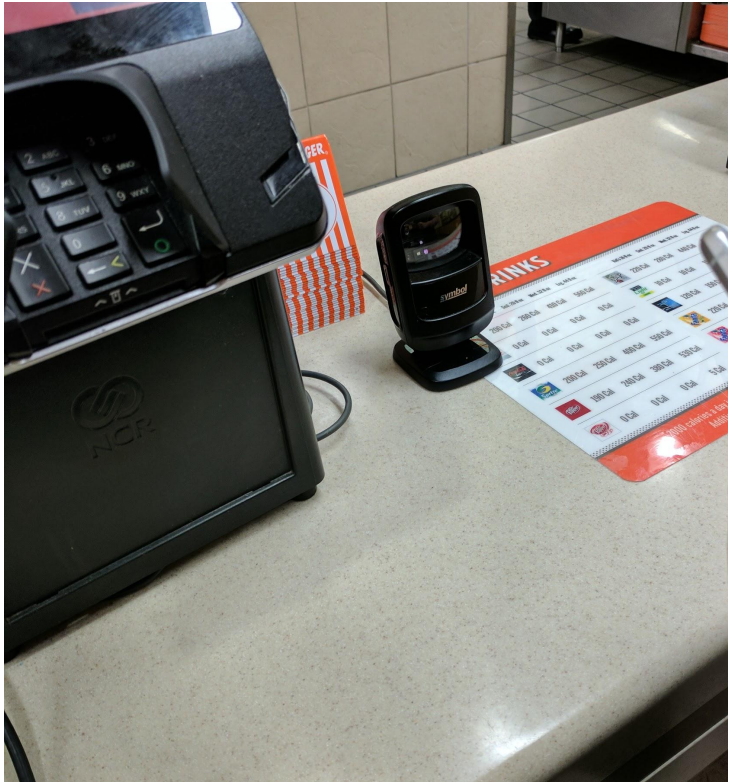
Barcodes are *everywhere*

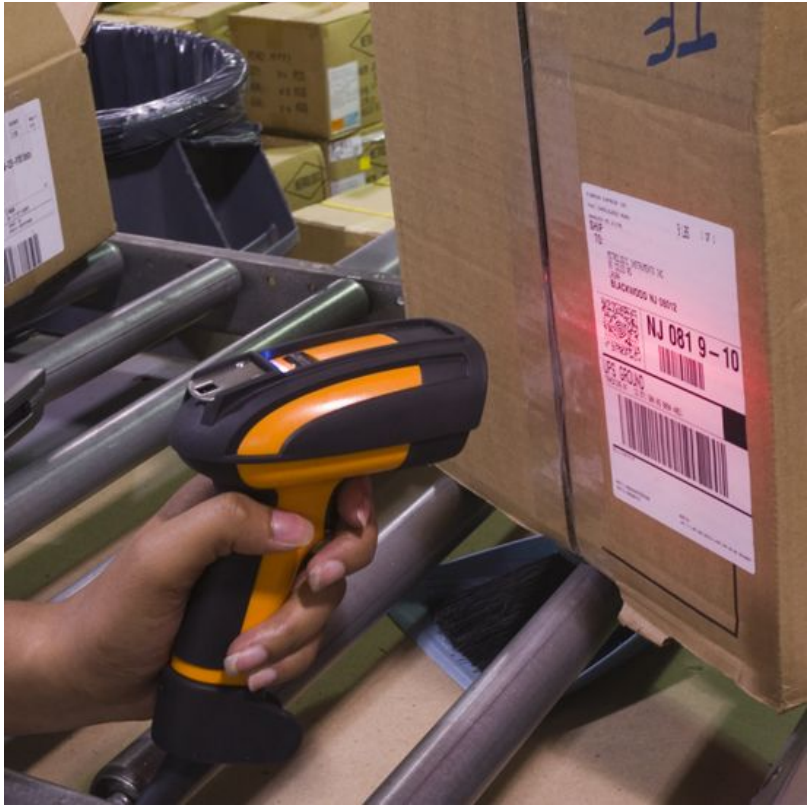






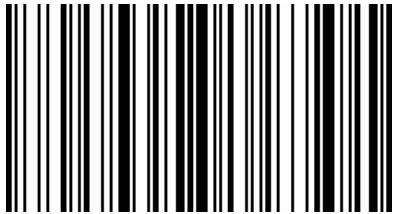
Barcode scanners are everywhere





Barcodes usually decode to text

Code 128



barcOwned

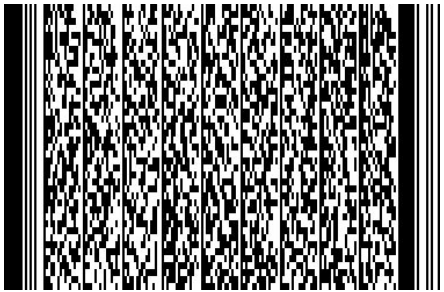
QR

https://038000144158.pw/

Aztec

barcOwned

PDF417



Did you ever hear the tragedy of Darth Plagueis "the wise"? I thought not. It's not a story the Jedi would tell you. It's a Sith legend. Darth Plagueis was a Dark Lord of the Sith, so powerful and so wise he could use the Force to influence the midichlorians to create life... He had such a knowledge of the dark side that he could even keep the ones he cared about from dying. The dark side of the Force is a pathway to many abilities some consider to be unnatural.

UPC

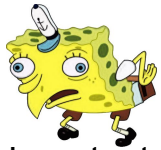
02626260

Scanner soliloquy

- Scanners are mostly the same
- Most common (default) mode:
  - Act as HID keyboard
  - Type buffer key by key
- What could we do if we could
  - Change the text on the fly?
  - Send arbitrary keystrokes?
  - Win + R?

To scan, or not to scan...

What could we do?*



*with proper permission in the scope of a legal, sanctioned pentest

It's not a bug!™

- Some symbologies add control chars
- Code 128:
  - 107 possible characters
  - 0 - 95: portions of ASCII
  - 96-106: control chars
- Control chars trigger programming
- Majority of scanners support this
  - Manufacturer specific

FNC3

10111100010

Index: 96

Yes, it's in-band signaling

What can programming do?

- Exists for legacy systems
- "We use Cyberdyne to track and herd our cats."
- "It's too expensive to replace or modify."
- "Make it faster!"
- Real (fake) example

No, not THAT type of cat...

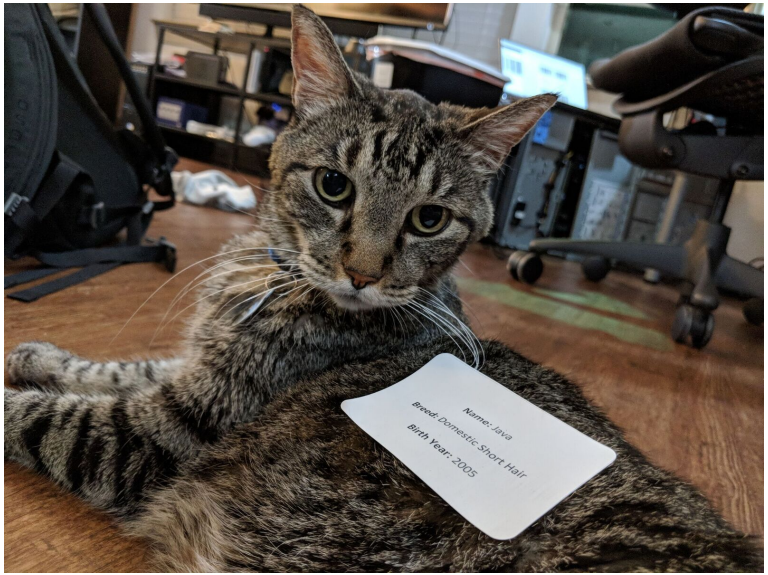
Herding cats

```
CAT DATA PROCESSING ERP
(c) 1984 Cyberdyne Systems

NAME:

BREED:

BIRTH YEAR:

PRESS F12 TO SAVE
```

Name: Java

Breed: Domestic Short Hair

Birth Year: 2005



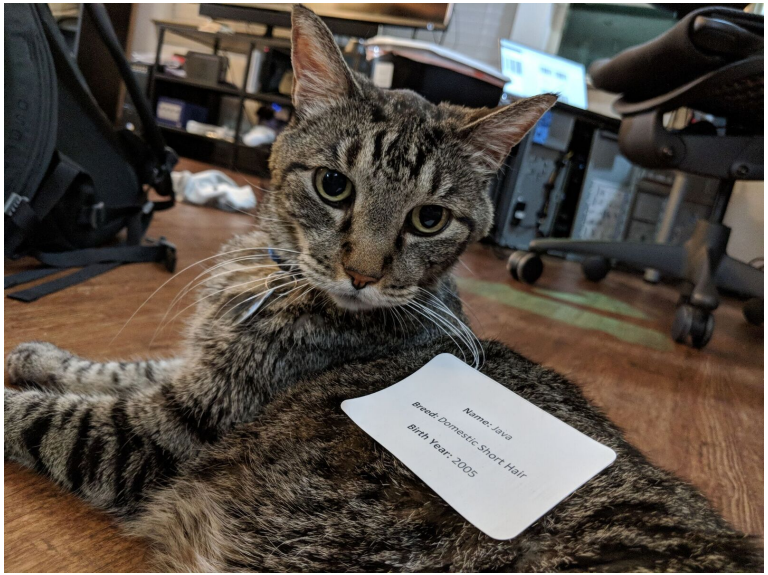
Herding cats

```
CAT DATA PROCESSING ERP
(c) 1984 Cyberdyne Systems

NAME:

BREED:

BIRTH YEAR:

PRESS F12 TO SAVE
```

Name: Java

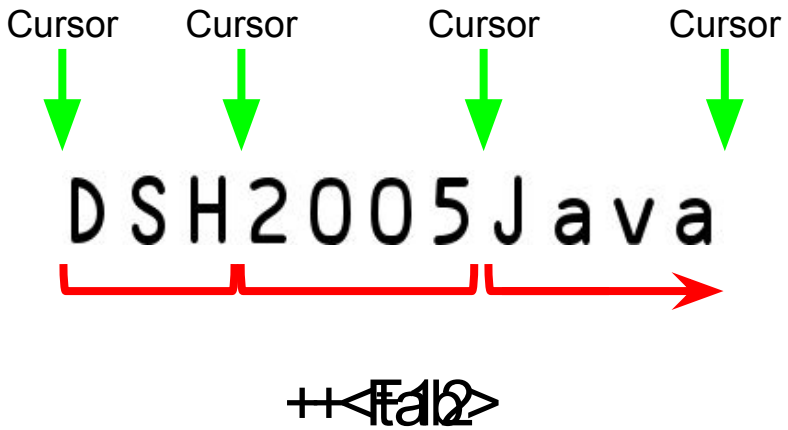
Breed: Domestic Short Hair

Birth Year: 2005



Barcoding cats

```
CAT DATA PROCESSING ERP
(c) 1984 Cyberdyne Systems

NAME: Java

BREED: DSH

BIRTH YEAR: 2005

PRESS F12 TO SAVE
```



Scanning cats

```
CAT DATA PROCESSING ERP
(c) 1984 Cyberdyne Systems

NAME:

BREED:

BIRTH YEAR:

PRESS F12 TO SAVE
```

Scanning cats

```
CAT DATA PROCESSING ERP
(c) 1984 Cyberdyne Systems

NAME:

BREED:

BIRTH YEAR:

PRESS F12 TO SAVE
```

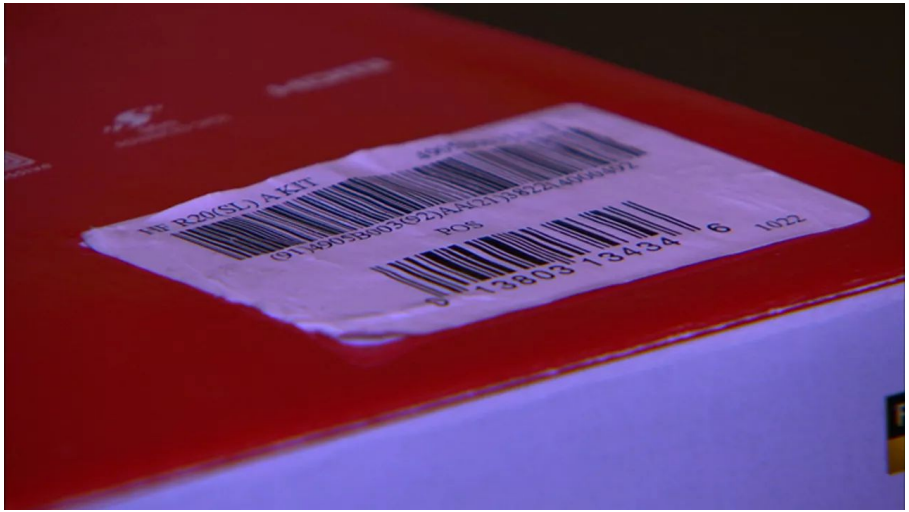
Programming is stupid simple

- Specify criteria
  - All barcodes (no criteria)
  - Barcodes that start with 9
  - Barcodes that contain "cat"
  - All UPC barcodes
- Specify actions when rule is triggered
- Can store multiple rules
  - Model-specific limits on size

"CatERP"

Actions we can do with rules

- Modify/replace text
- Ignore text
- Add extra characters
- Add special keys
  - Ctrl or Alt key combos
  - Windows/super key too!
- "Brick" scanners
  - Do nothing!



barcOwned (finally)

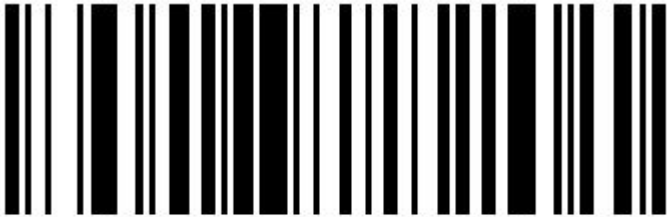
- Payload design IDE
  - Payloads in JSON
  - Rapidly develop and test
- Abstracts most complexity
  - No deciphering manuals
- Supports Motorola Symbol
  - Send us scanners?
- Open source

```
{
  "name": "Hello World",
  "description": "Scan hello, get a bonus world!

  "setup": {
    "options": [],
    "rules": [
      {
        "criteria": [
          ["stringatstart", "hello"]
        ],
        "actions": [
          ["sendremaining"],
          ["sendtext", "world"]
        ]
      }
    ]
  },

  "payload": [
    "hello"
  ]
}
```

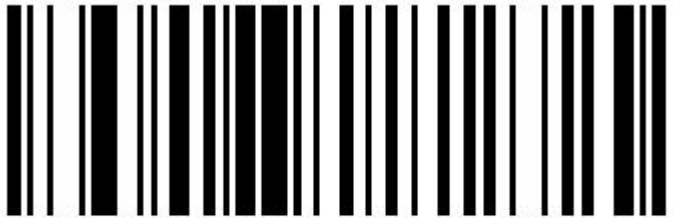
Harder Than Ducky Script™

Demo

Can you turn it off?



Disable Parameter Scanning
(00h)



*Enable Parameter Scanning
(01h)

Red team considerations

- Find beeper hole and cover it if possible
- Successful attacks take significant recon, planning
- BYOS - Bring Your Own Scanner
  - Detach scanner with screwdriver, plug your own in
- Even when systems are off, scanners may be powered
- Laser scanners will only work with paper or a Kindle
- Trick others into delivering barcodes

Let someone else do the dirty work

Blue team considerations

- No way to secure scanners from programming
  - Some models may not support it
- Assume scanners are hostile keyboards
  - Remove local admin
  - Use endpoint protection + app control
  - Limit PowerShell, cmd, run dialog, etc
- Filter malicious keys at OS-level
  - Or enforce non-HID modes

Related talks

- BadBarcode - Yang Yu
  - PacSec 2015 in Tokyo
  - Demoed attack, no paper/code released
- Toying with Barcodes - Felix Lindner
  - DEF CON 16 in 2008
  - General overview of barcodes as input vectors

Special thanks

- Terry Burton - BWIPP
- Mark Warren - bwip-js
- Hermit Hacker - shirts
- Dallas Hackers Association
- CyberArk - travel + support

barcowned.com

github.com/t3hub3rk1tten/barcowned

Michael West
@t3hub3rk1tten
mwe.st

Colin Campbell
@magicspacekiwi