```
mly@morocco:~$ cat presentation.txt
```

```
$ whoami
```

MOHAMMED AMINE MOULAY

Security Engineer @ Oracle |Surfer|Writer & Poet| Solutions Builder :)

```
$ cat cool-topics/topic-defcon-group-casa.txt
```

IoT Security 101:How Cybercriminals Turn Your Smart Devices Into Weapons

DefCon Group Casablanca | Feb 13, 2026

Press ENTER to continue...

```
$ cat security_foundations.md
```

# THREE CORE PRINCIPLES

1. **EVERYTHING IS VULNERABLE**
   Not 'can be' - IS vulnerable

2. **SECURITY = ADVERSARIAL THINKING**
   Think like attacker climbing walls

3. **COMPLEXITY IS THE ENEMY**
   Best security: Code you didn't write

I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, I DO IT IN PRODUCTION
makeameme.org

```
$ cat iot_reality.md
```

# THE IoT DISASTER

THE MATH:
IoT: 512KB RAM
Security agent: 200MB
Gap: 400x

DEFCON STATS:
300+ vulnerabilities
47 vulns / 23 devices (2019)
ALL hacked

```
$ cat coffee_weaponization.md
```

# WEAPONIZING COFFEE MACHINES

AVAST RESEARCH (2020):

✓ Ransomware machine
✓ Gateway to home network
✓ Fire hazard (burner overheat)
✓ Scalding water attack

```
$ shodan search --demo
```

# LIVE DEMO: SHODAN HUNT

Shodan.io - 'Google for Hackers'
3+ million users | Created 2009

Country X IOT EXPOSURE:

```
1. SEARCH:
port:23 country:X
   Result: Telnet servers in X
   Risk: Default credentials, no encryption

2. SEARCH: "webcamxp" country:X
   Result: Unprotected webcams
   Risk: Live video feeds, no auth

3. SEARCH: "default password" country:X
   Result: Devices with factory settings
   Risk: admin/admin, immediate access
```

A Threat Visit to your Smart Home

IMPORTANT: We're VIEWING, not ATTACKING. That's illegal.

MOIRAGUARD Eye O Tea Scanner Link

ATTACK SURFACE: 4 LAYERS

LAYER	WHAT ATTACKERS GET
NETWORK	Pivot point, credentials, firmware, MitM updates
PHYSICAL (UART/JTAG)	Root filesystem, hardcoded creds, API keys, crypto keys
SOFTWARE	CVE exploits, command injection, buffer overflows
CLOUD	ALL machines globally, cloud infra, customer data

Source: Daniel Miessler 'IoT Attack Surfaces' (DEF CON 23)

REAL-WORLD ATTACK SCENARIOS:

TrendMicro Research: Smart Home Threats & Attack Patterns

‣ Network infiltration via smart devices ‣ Data exfiltration through IoT gateways ‣ Persistent access via compromised hubs

WEAPONIZATION: 4 SCENARIOS

1. BOTNET BARISTA

→ Mirai: 600K devices (2016)

Your espresso helps DDoS X ~~Twitter~~

2. NETWORK PIVOT

→ Avast 2020 research

Corporate VPN via kitchen

3. CRYPTOMINER CAPPUCCINO

→ DefCon: Smart bulbs mining

You pay electric for their Bitcoin

4. RANSOMWARE ROAST

→ Negotiate before coffee

Irony: MAXIMUM

[MEME] 'Your coffee machine works a second job you don't know about'

DEFCON: Baby monitors, smart bulbs, thermostats, doorbells, refrigerators, Ecovacs robots

```
$ cat why_this_matters.md
```

THIS ISN'T ABOUT COFFEE. It's about THE PATTERN.

Daniel Miessler (DefCon 23):

"Enough with junk hacking and being amazed when people hack their junk..."

The coffee machine is a METAPHOR for every IoT device.

The Disconnected IoT Club
So ... we're just not going to talk to each other?
When your IoT security is so tight, even the devices think they are on a need-to-know basis.

WHAT ACTUALLY WORKS

FOR USERS:

✓ Change defaults
✓ Segment network
✓ **Best IoT = no IoT**

FOR DEVELOPERS:

✓ Secure by default
✓ Regular OTA updates
✓ **Test adversarially**

FOR RESEARCHERS:

✓ Document (IoT Village model) ✓ Build tools ✓ Reverse engineer ✓ Write about it ✓ **Break responsibly**

Chris Valasek (DefCon): 'Stop saying things are unhackable'

```
$ cat takeaways.txt
```

# KEY TAKEAWAYS

1. **EVERYTHING IS VULNERABLE**
   Not 'can be' - IS. Accept it. Find flaws first.

2. **IOT SECURITY IS A PATTERN PROBLEM**
   300+ DefCon vulnerabilities prove it. Default creds, no updates, exposed debug ports - same pattern.

3. **SHODAN IS YOUR WAKE-UP CALL**
   If I can find your devices in 30 seconds, so can attackers. Check your exposure: shodan.io

4. **SOLUTIONS EXIST, BUT REQUIRE ACTION**
   Users: Change defaults, segment networks
   Devs: Secure by default, actual OTA updates
   Researchers: Document, build, break responsibly

5. **YOUR COFFEE MACHINE IS PROBABLY COMPROMISED**
   But at least the espresso tastes good. 😏

MOIRAGUARD Eye O Tea Scanner

$ cat next_chapter.txt

# COOKING THE NEXT ATTACK (Make sure you have needed legal permission :)   )

On going RESEARCH:

Hardware hacking methodology

THE PLAN:

1. Browse the (Morocco's Amazon)
2. Find most popular IoT device:
   - Smart cameras?
   - WiFi routers?
   - Smart doorbells?
3. Buy it
4. Hardware hack it:
   - UART extraction
   - Firmware analysis
   - Find vulnerabilities
5. Demonstrate exploitation
6. Publish findings
7. **Present at DefCon Group Casablanca**

Goal: Live hardware hacking demo

From store shelf → root shell → propagation

4G modem
UART extraction

CP2102 adapter
Logic analyzer
Firmware dump

TEASER:
This is what's coming next...

DEFCON
GROUP CASABLANCA

```
mly@morocco:~$ cat closing.txt
```

# THANKS + REFERENCES

Life is a continuous debug cycle.
Patch what you can. Surf when waves are good.

Your coffee machine is probably compromised.
But at least the espresso tastes good.

REFERENCES:

- Avast: Smart Coffee Maker (2020)
- Miessler: IoT Attack Surfaces (DC23)
- Giese: Having Fun With IoT (DC26)
- IoT Village: 300+ vulns (2013-2024)
- Valasek: Jeep hack (BH2015)
- TrendMicro: Smart Home Threats
- Shodan.io: Device exposure research

CONTACT:

Email: aminepa8+defcongroupcasa@gmail.com
LinkedIn: linkedin.com/medmly
Medium: [OSINT IT :)]

```
$ # Questions?
$ EOF
```

DEFCON
GROUP CASABLANCA