nordic
INNOVATION LABS

Presentation Title Goes Here

nordic
INNOVATION LABS

Threat models and the tools of the industry
→ From an attacker's point of view

Harri Hursti

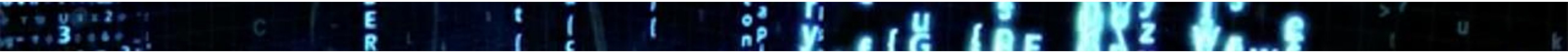
Is our threat model up to date?

… actually it's the wrong threat model

- People outside of the cyber realm have traditionally considered the threat to be a dishonest candidate cheating to win
  - Nation-state attacker motivations are harder to predict than that
  - If the motivation is just to cause distrust and chaos, it opens new attack vectors

- Thinking that hackers cannot do wholesale attacks without the Internet is wrong
  - There are many ways to attack the system on a wholesale basis from the Internet *without* real-time Internet connectivity
  - Even computer viruses infecting consumer computers outdate availability of Internet to the consumers

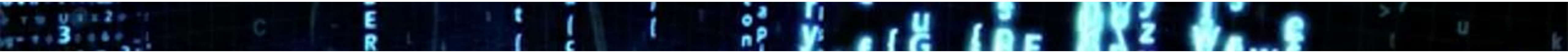
- The tools are cheap and available to all



Some attack surfaces

… and sample tools

- USB
  - Central tabulator computers, voting machines and epollbooks all have these
  - Also many voting vendors rely on USB devices in their designs
- WiFi
  - Attacker may be able to leverage personal devices present in sensitive locations as the point to leverage access
- Barcodes
  - Barcodes are used in ballots, and epollbooks can read driving licenses etc



USB is everywhere

USB is everywhere

… and sometimes hiding in a plain sight

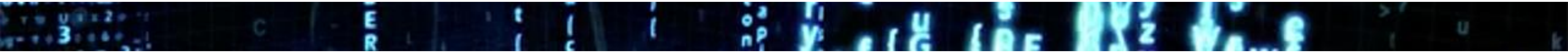
- USB is basically integrated into every device you use
  - Computers
  - USB memory sticks
  - Printers
  - (Video)cameras
  - Mobile phones

- In voting technology they’re used to :
  - Store encryption keys
  - Transfer election results from the central tabulator to the reporting system
  - Read and program election information cartridges etc

USB is everywhere

… and it is never ‘just a cable or disk’

- USB device are always controlled by a miniature computer
  - A USB memory stick is an active computer, which responds to the computer’s requests to read / write data
  - Even your USB charger is an ‘intelligent’ device which talks with the device to be charged
  - If the programming of the USB device cannot be trusted, nothing the device communicates can be trusted
    - … but about half of the devices are reprogrammable
    - … and the computers like to trust them
    - … and the standard has serious flaws, the issues are not bugs
    - … and the devices are unidentifiable from each other
      - the serial number is optional and usually non-existent on many of the devices



USB is everywhere

… and it can bring many things to the table

- USB device can be from many classes
  - Storage
  - Printer
  - Display
  - Camera
  - Keyboard
  - Mouse
  - Network adaptor (wireless, Ethernet, Bluetooth, whatever)
  - TV/Radio
  - Etc etc etc

USB is everywhere

… and it is flexible

- It can have many identities and described functionalities
  - I am your Disk and Keyboard with Mouse
- It can change its mind any time
  - USB device can register and de-register itself and the services it provides
    - Become a keyboard only 12 hours after been plugged in, and only for 20 seconds
- USB can register to be a display
  - … and ask to be a mirror display of the primary screen
  - Now it can see everything you see, and either use it for autonomous attacks or send it to the Master
  - … and it has enough horsepower to OCR the content for attack directing

USB is everywhere

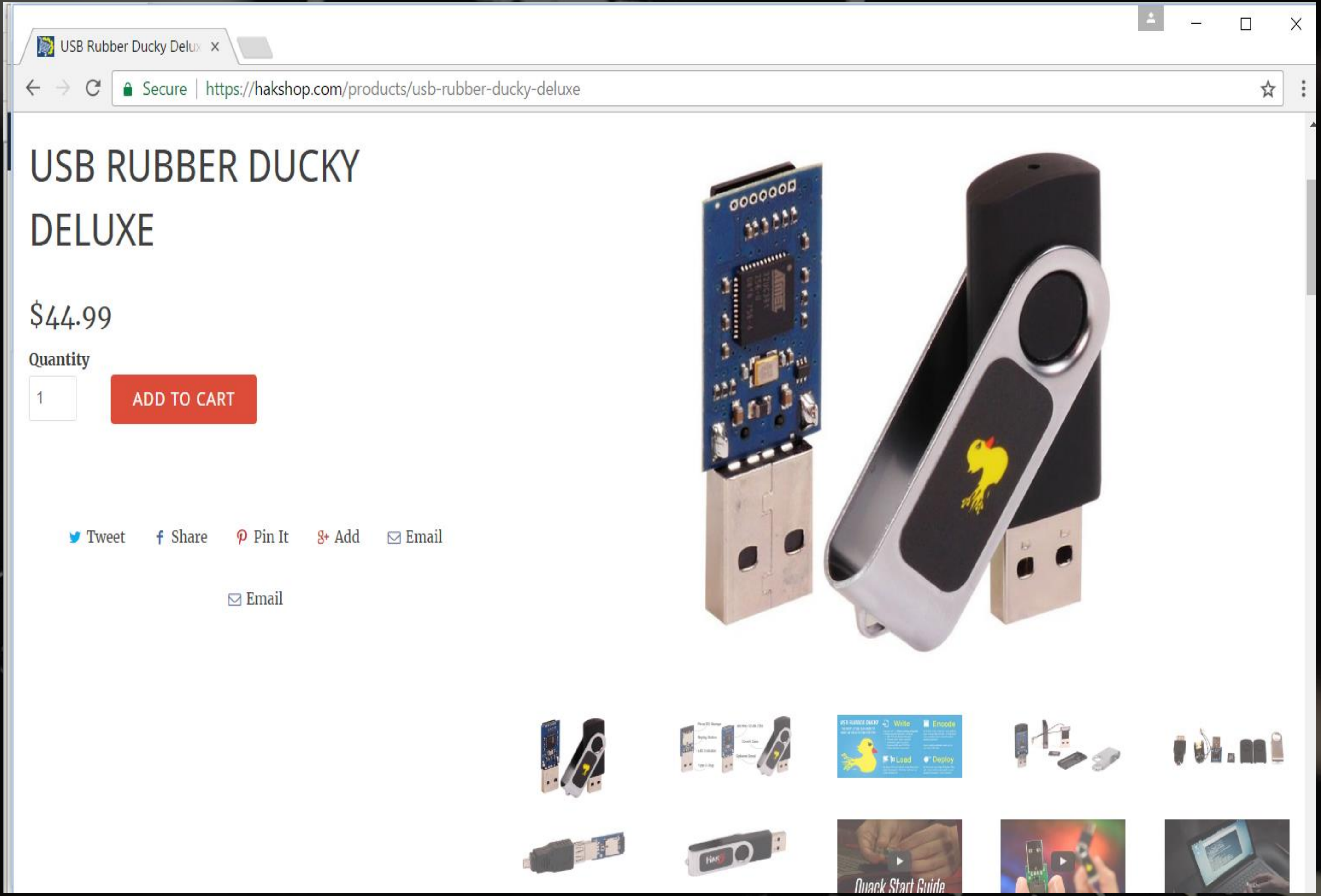
… and it can easily take the control to seriously undermine network security

- As a programmable device, USB device is intelligent
  - malicious features only after trigger activity observed
- USB device can announce itself to be a network device
  - Windows will prefer wireline network connection over wireless
  - … and then some good old Ethernet spoofing and other fun stuff
- Scenario : USB device spoofs Ethernet adapter
  - USB device replies to DHCP query with DNS evil server on the Internet, but without default gateway
  - Internet traffic is still routed through the normal WiFi connection
    - DNS queries are sent to the evil server, enabling a redirection attack

USB is everywhere

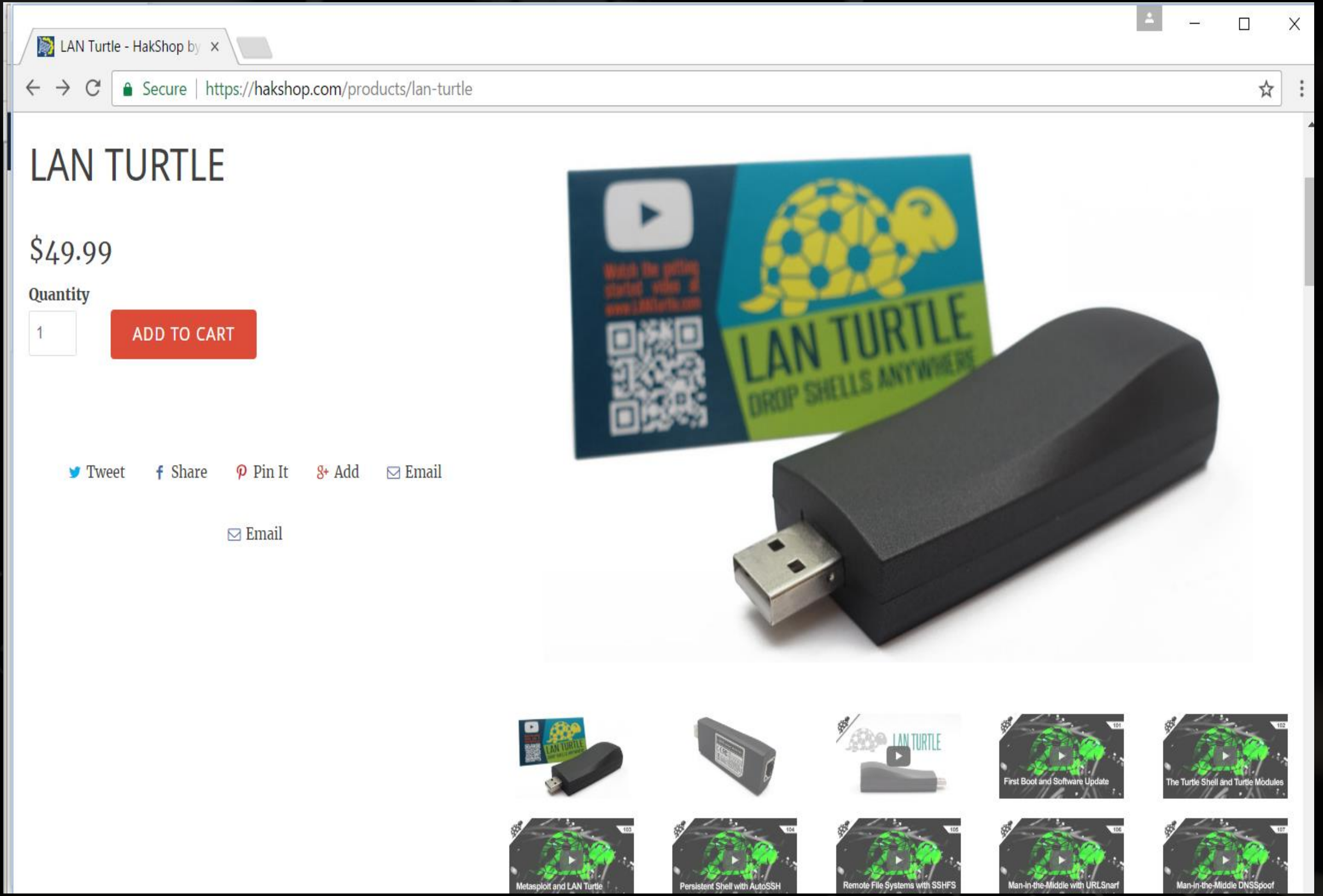
… and it can easily take the control to seriously undermine network security

- As a programmable device, a USB device is intelligent
  - malicious features only after trigger activity observed
- USB device can present itself tas a network device
  - Windows will prefer wireline network connection over wireless
  - … and then some good old Ethernet spoofing and other fun stuff
- Scenario : USB device spoofs Ethernet adapter
  - USB device replies to DHCP query with DNS evil server on the Internet, but without the default gateway
  - Internet traffic is still routed through the normal WiFi connection
    - DNS queries are sent to the evil server, enabling a redirection attack



USB RUBBER DUCKY DELUXE

$44.99



LAN Turtle - HakShop by

Secure | https://hakshop.com/products/lan-turtle

LAN TURTLE

$49.99

Quantity

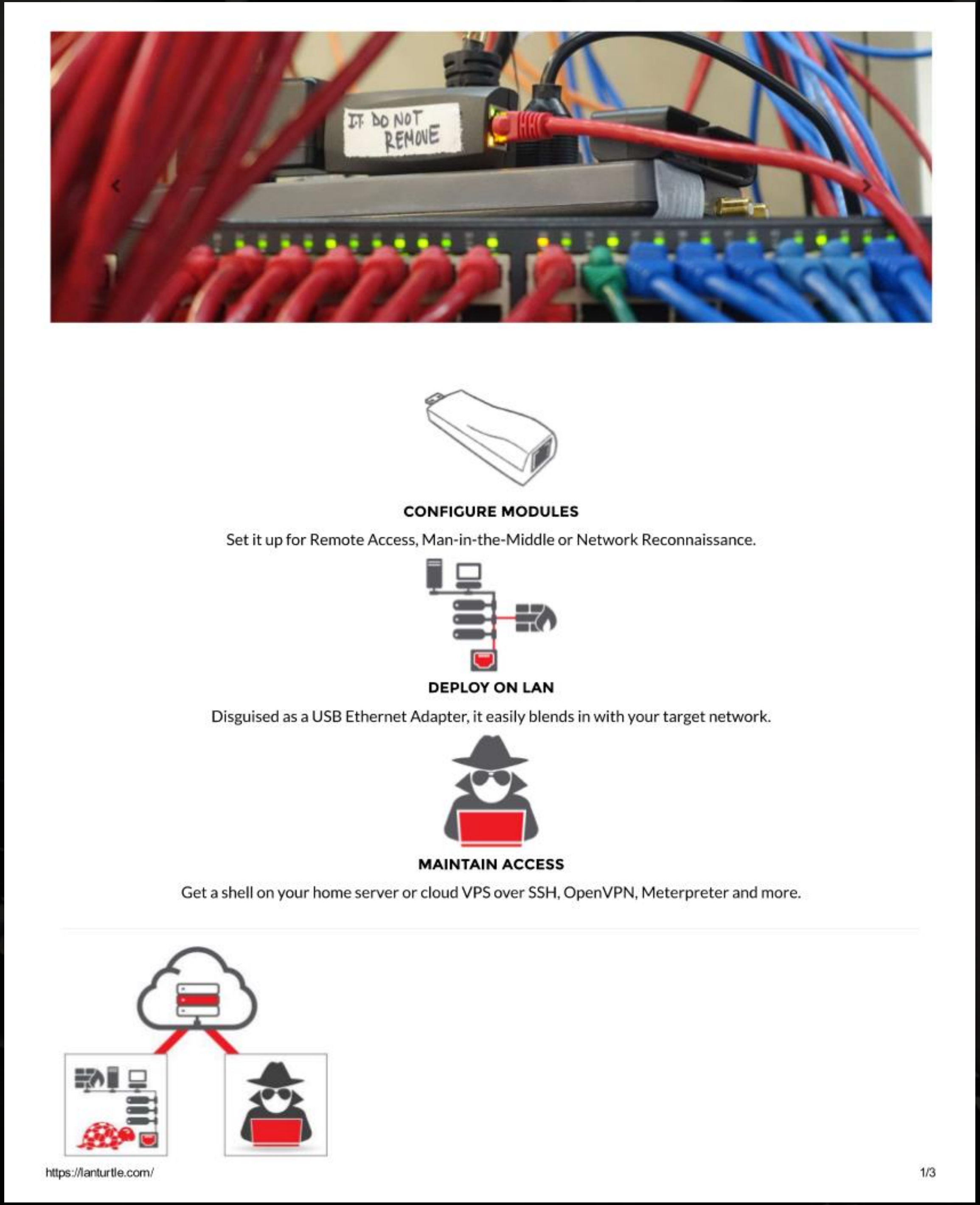
1

ADD TO CART

Tweet Share Pin It Add Email

Email

LAN TURTLE
DROP SHELLS ANYWHERE
First Boot and Software Update
The Turtle Shell and Turtle Modules
Metasploit and LAN Turtle
Persistent Shell with AutoSSH
Remote File Systems with SSHFS
Man-in-the-Middle with URLSnarf
Man-in-the-Middle DNSSpoof



CONFIGURE MODULES

Set it up for Remote Access, Man-in-the-Middle or Network Reconnaissance.

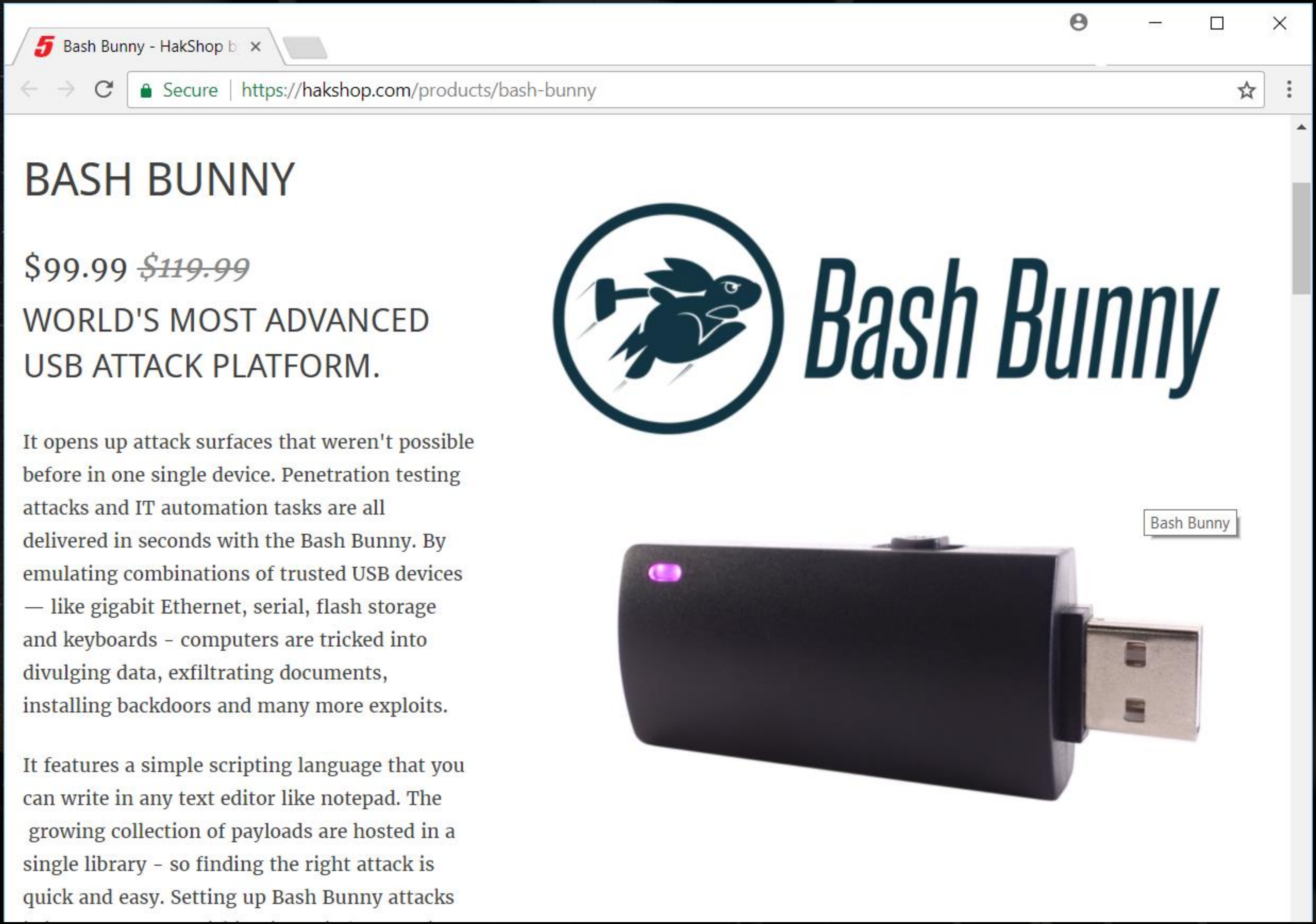
DEPLOY ON LAN

Disguised as a USB Ethernet Adapter, it easily blends in with your target network.

MAINTAIN ACCESS

Get a shell on your home server or cloud VPS over SSH, OpenVPN, Meterpreter and more.

nordic INNOVATION LABS



BASH BUNNY

$99.99 ~~$119.99~~

WORLD'S MOST ADVANCED USB ATTACK PLATFORM.

It opens up attack surfaces that weren't possible before in one single device. Penetration testing attacks and IT automation tasks are all delivered in seconds with the Bash Bunny. By emulating combinations of trusted USB devices — like gigabit Ethernet, serial, flash storage and keyboards - computers are tricked into divulging data, exfiltrating documents, installing backdoors and many more exploits.

It features a simple scripting language that you can write in any text editor like notepad. The growing collection of payloads are hosted in a single library - so finding the right attack is quick and easy. Setting up Bash Bunny attacks

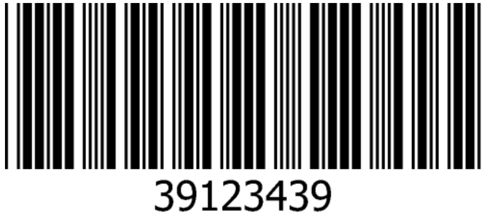
About barcodes

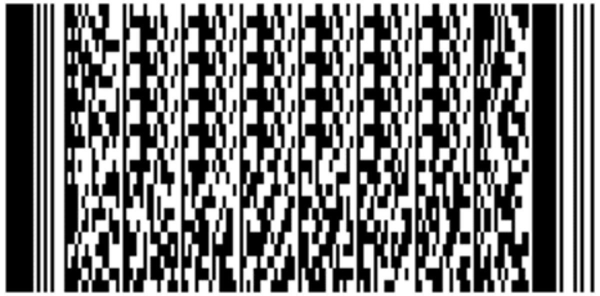
… can barcodes assist in a jailbreak?

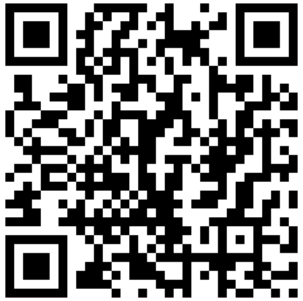
About barcodes

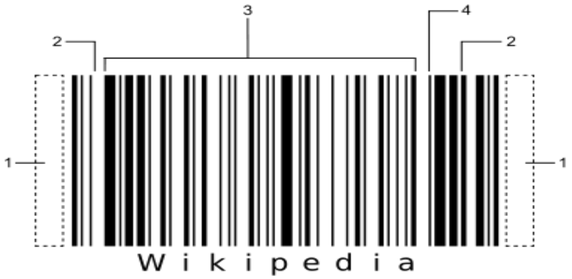
… What is a barcode?

- A barcode is an optical machine-readable representation of data relating to the object to which it is attached;
- Originally barcodes (1D) systematically represented data by varying the widths and spacings of parallel
  - Common misconseption : 1D barcodes are safe and limited compared to 2D barcodes









About barcodes

… What is a barcode?

- A barcode is an optical machine-readable representation of data relating to the object to which it is attached;
- Originally barcodes(1D) systematically represented data by varying the widths and spacings of parallel
- Many barcode scanners are keyboard emulation device
- Some barcode protocols, like Code 128, supports ASCII control characters
  - Almost every barcode scanner supports Code 128 by default
- Almost every barcode scanner has its own additional keyboard emulation features
- Common Hotkeys registered by many programs, like: CTRL+O, CTRL+P can be sent directly
- ADF (Advanced Data Formatting) makes it possible to also send GUI+ keys and for example "right shift"

- Very often reading a barcode is the equivalent of letting something unknown be typed with the keyboard!

Crash into the WiFi world

WiFi is everywhere

- WiFi is extremely convenient
- One can set their devices to automatically pair with the office network and other networks frequently visited
  - The devices automatically connect into paired networks

- WiFi is an attack surface almost always
  - If the target system does not have WiFi, the people around the system do have wireless devices which may be useful for the attacker to gain intelligence and/or a beachhead to carry out an attack

Crash into the WiFi world

WiFi management is not secure

- Management frames :
  - Define network SSID, crypto (beacons)
  - Control client access (probe request, response)
- *Not authenticated*
- *Not encrypted*
- New standards seek to address this in the future

Crash into the WiFi world

How does it connect?

- Finding a WiFi network is really easy
- Networks are really noisy (radios are noisy by design)
  - Access point beacon talks all the time, up to 10x a second
  - Even 'hidden' networks make noise when someone talks to it
- No way to really hide

Crash into the WiFi world

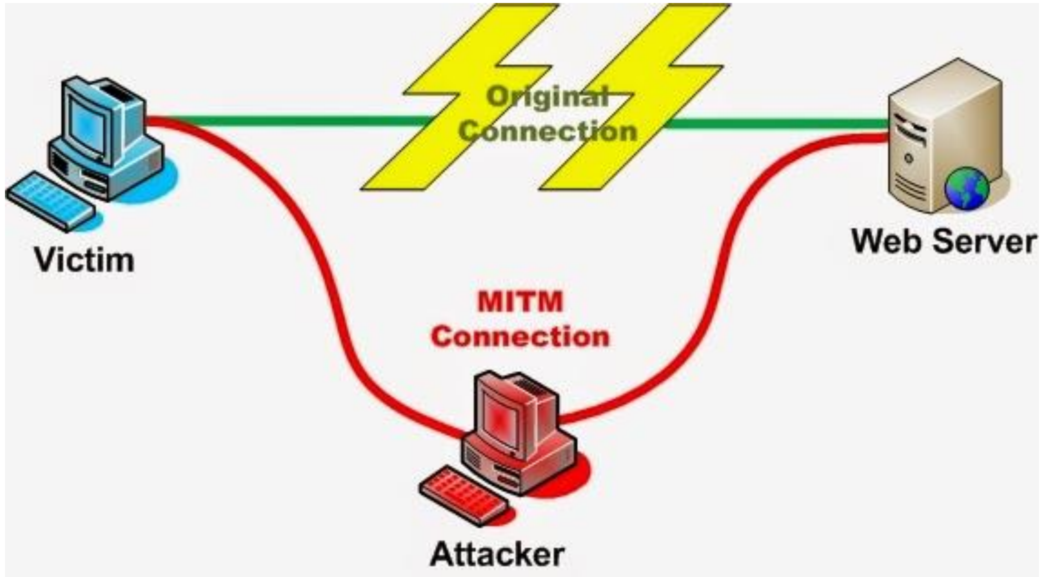
How does it connect?

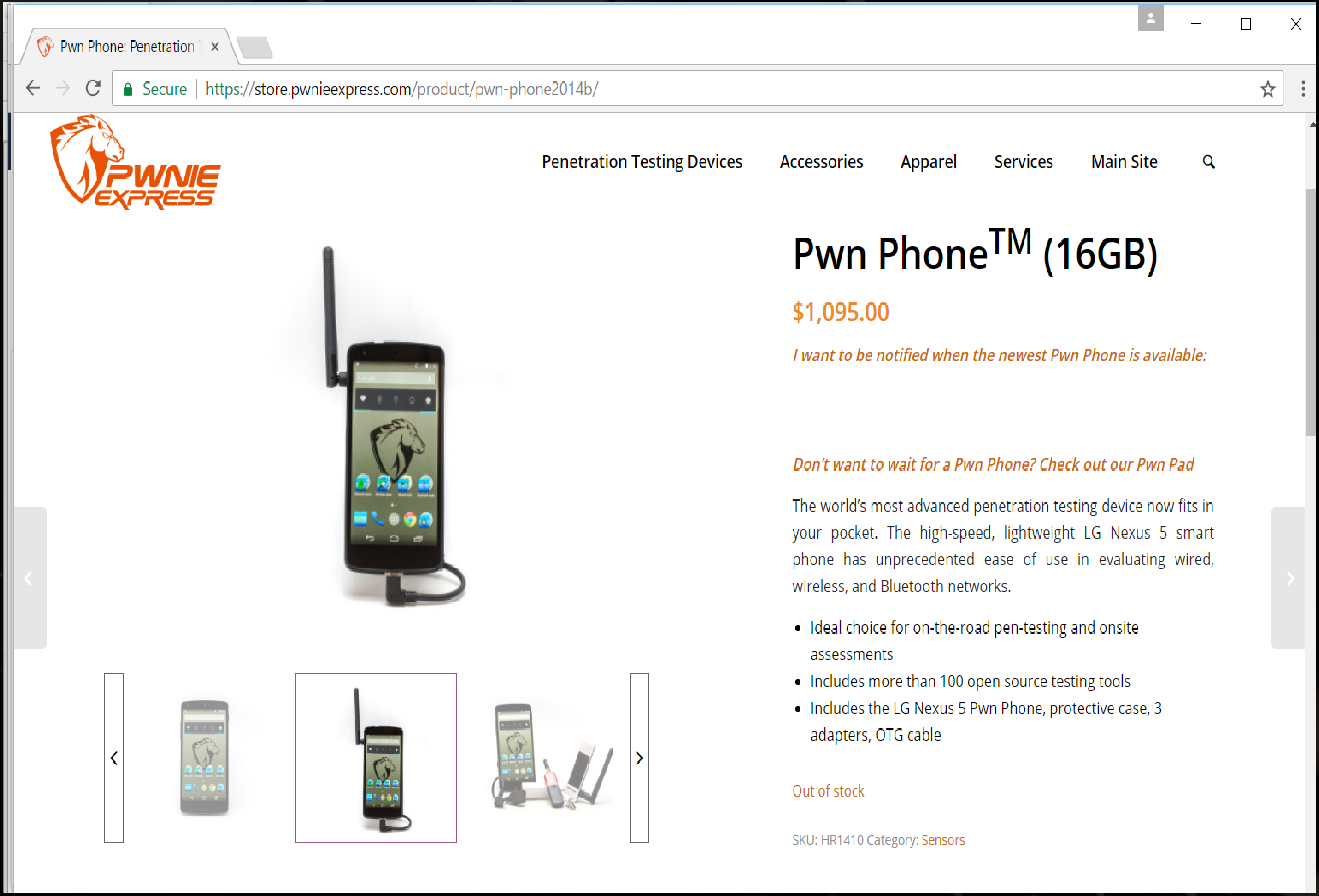
- Clients constantly look for networks to join
- And often tell us every network they'd like to see (every network they are paired with)
  - Just as easy to find as networks
  - … and they get very noisy when they cannot find a network to join
- Also they are very trusting, way too trusting
  - If network answers 'I am foo', it must be foo. Right?
    - So if an attacker has a stronger radio than your real Access Point
      - You may not be talking to who you think you're talking to
- EvilAP also called as Evil Twin or Bad Karma
  - Answer ALL probe requests as the ultimate Yes Man
    - Are you “Free Public Wifi”? Sure am.
    - Are you “My Secure Corporate Network”? Yup!

Crash into WiFi world

Disruption can a step on the way

- If one first sets up Evil AP
  - … and then spoofs real AP asking clients to disconnect
  - … and then the clients automatically reconnect




Pwn Phone: Penetration
Secure
https://store.pwnieexpress.com/product/pwn-phone2014b/
PWNIE EXPRESS
Penetration Testing Devices
Accessories
Apparel
Services
Main Site

Pwn Phone^{TM} (16GB)

$1,095.00

I want to be notified when the newest Pwn Phone is available:

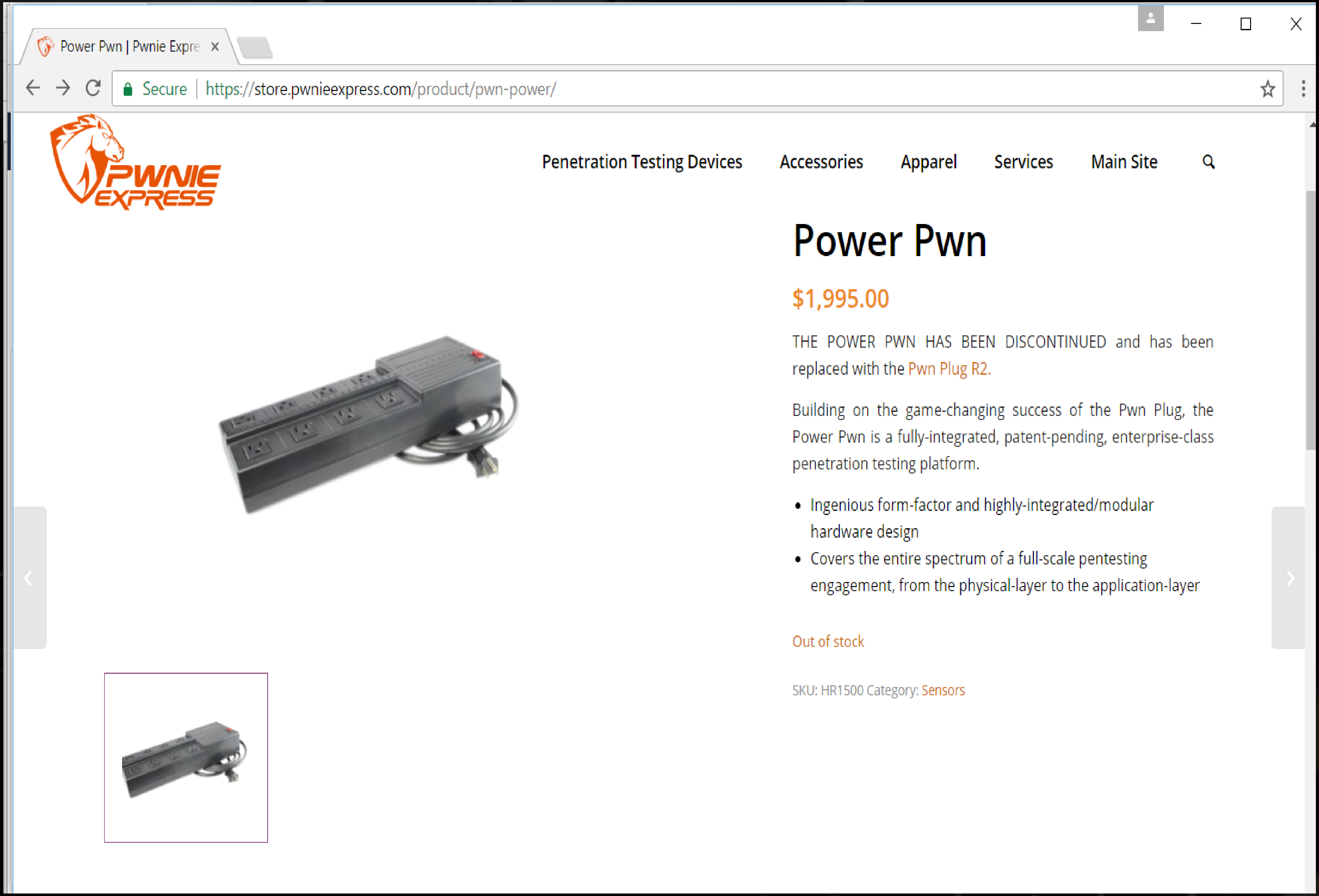
Don't want to wait for a Pwn Phone? Check out our Pwn Pad

The world's most advanced penetration testing device now fits in your pocket. The high-speed, lightweight LG Nexus 5 smart phone has unprecedented ease of use in evaluating wired, wireless, and Bluetooth networks.

- Ideal choice for on-the-road pen-testing and onsite assessments
- Includes more than 100 open source testing tools
- Includes the LG Nexus 5 Pwn Phone, protective case, 3 adapters, OTG cable

Out of stock

SKU: HR1410 Category: Sensors


Power Pwn | Pwnie Expre
Secure
https://store.pwnieexpress.com/product/pwn-power/
Penetration Testing Devices
Accessories
Apparel
Services
Main Site

Power Pwn

$1,995.00

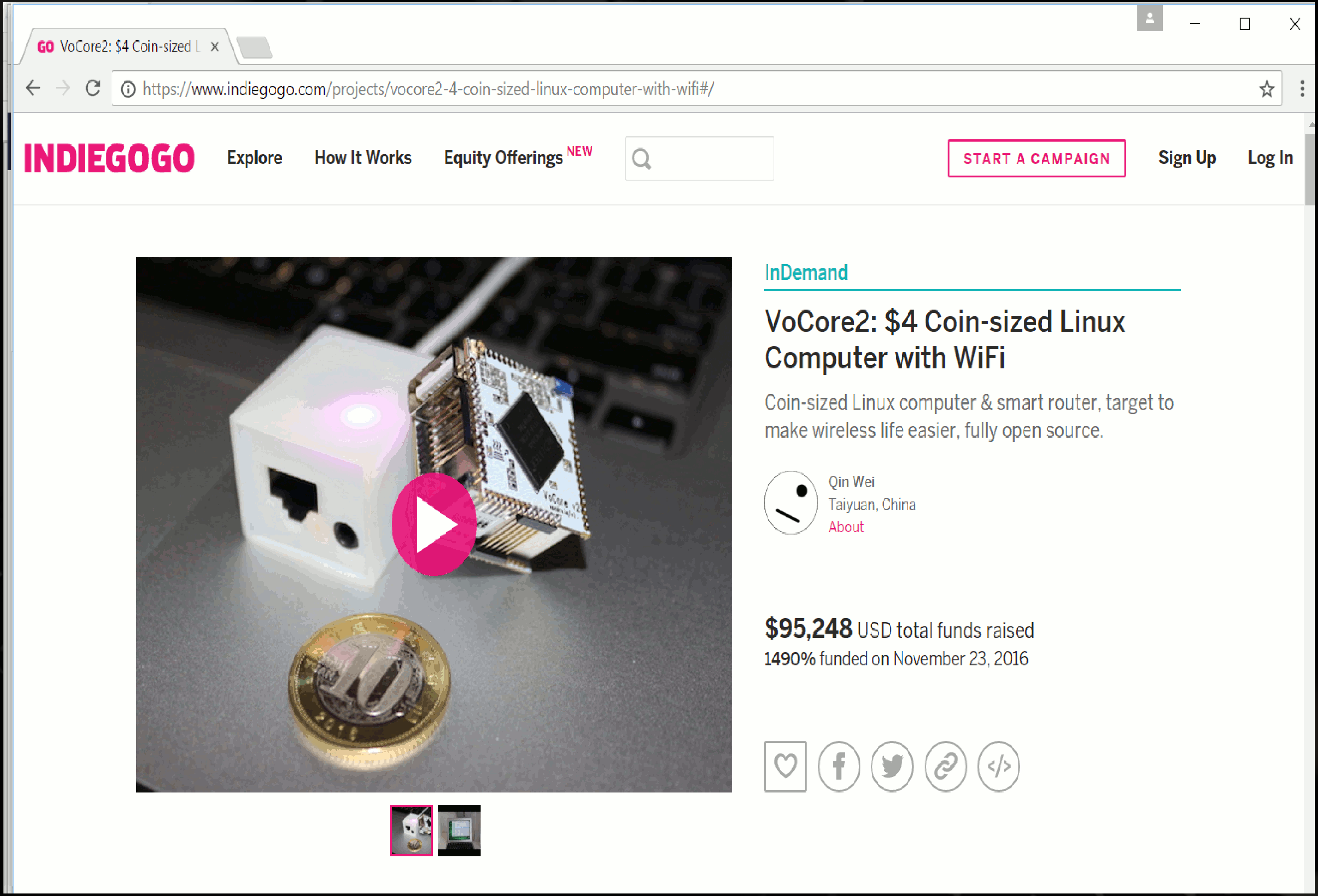
THE POWER PWN HAS BEEN DISCONTINUED and has been replaced with the Pwn Plug R2.

Building on the game-changing success of the Pwn Plug, the Power Pwn is a fully-integrated, patent-pending, enterprise-class penetration testing platform.

- Ingenious form-factor and highly-integrated/modular hardware design
- Covers the entire spectrum of a full-scale pentesting engagement, from the physical-layer to the application-layer

Out of stock

SKU: HR1500 Category: Sensors



GO VoCore2: $4 Coin-sized L
https://www.indiegogo.com/projects/vocore2-4-coin-sized-linux-computer-with-wifi#/
INDIEGOGO
Explore
How It Works
Equity Offerings NEW
START A CAMPAIGN
Sign Up
Log In

InDemand

VoCore2: $4 Coin-sized Linux Computer with WiFi

Coin-sized Linux computer & smart router, target to make wireless life easier, fully open source.

Qin Wei
Taiyuan, China
About

$95,248 USD total funds raised
1490% funded on November 23, 2016

Thank you!