Online Tracking and Privacy

NWI-IMC074

Lecture 9

24 Apr 2024

Güneş Acar - Digital Security group
Radboud University

Agenda

- IoT security and privacy
- DoH, DoT, eSNI
- Wireshark

IoT privacy and security

IoT Security and Privacy

- 25 billion connected devices by 2025 (Ericsson)
- security is not the highest priority for most IoT vendors
- massive DDoS attacks due to insecure IoT devices (e.g. Mirai)
- limited privacy and security countermeasures

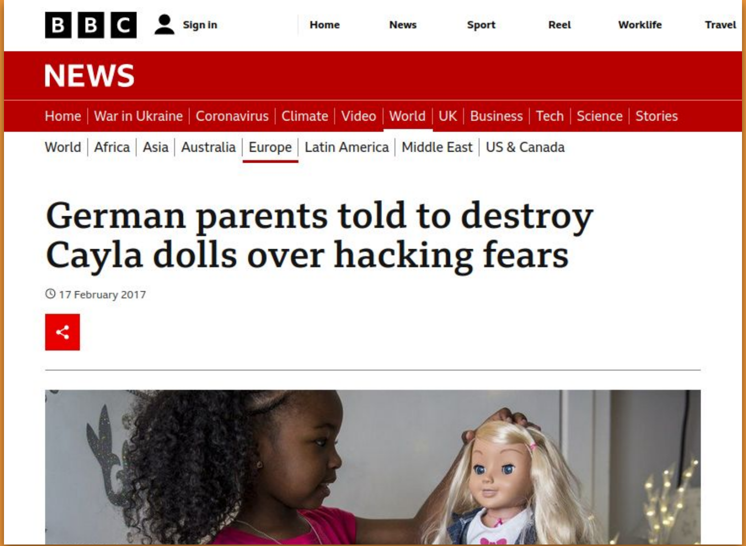
My Friend Cayla

- Unauthenticated Bluetooth pairing
  - speak through the doll
- Voice sent to company servers
  - can be used for targeted ads
  - shared with 3rd parties

https://www.youtube.com/watch?v=lAOj0H5c6Yc

My Friend Cayla

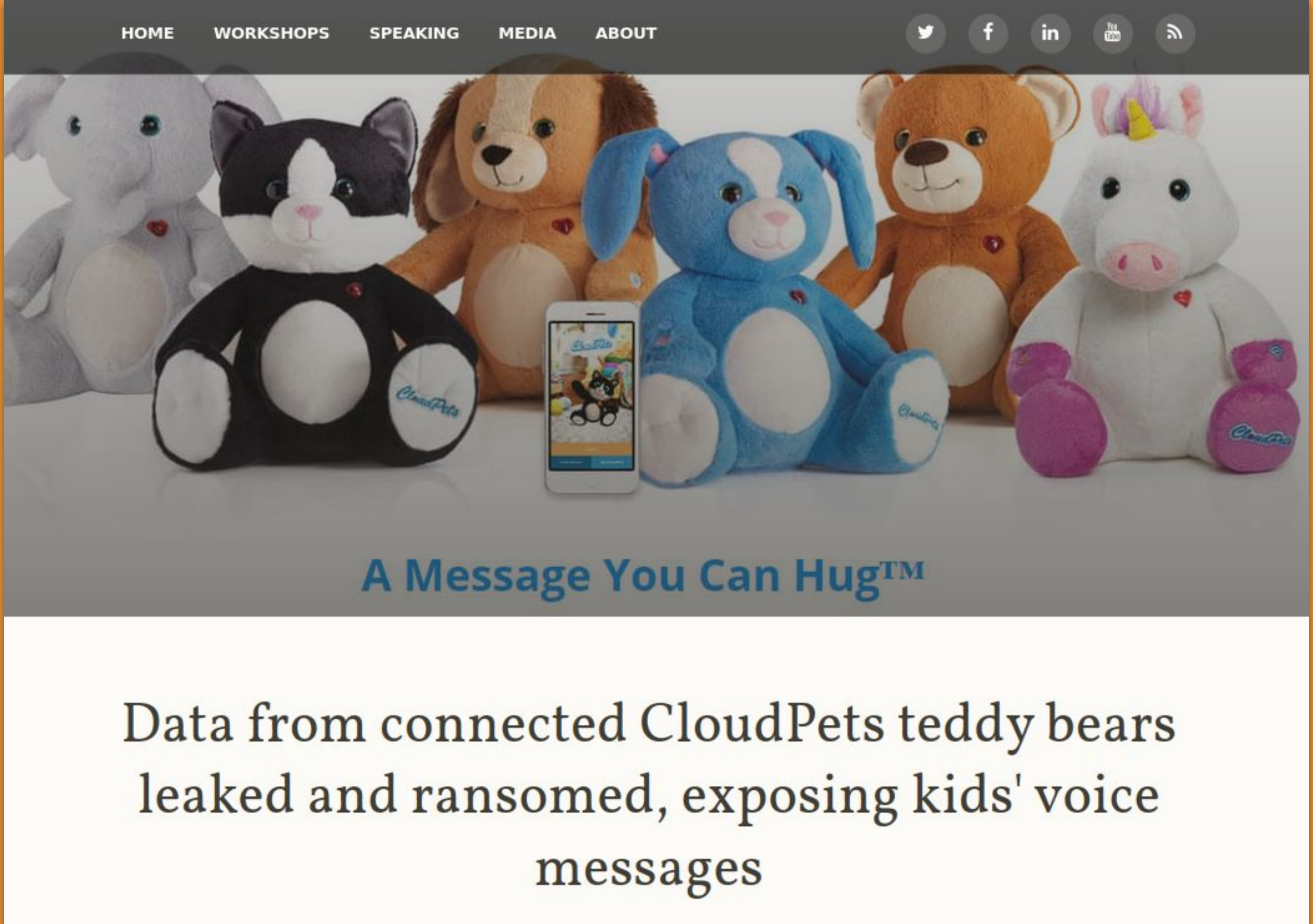
*In February 2017 the German Federal Network Agency notified parents that **they were obliged to "destroy"** any Cayla in their possession as **it constitutes a concealed espionage device** violating the German Telecommunications Act. (Wikipedia)*


BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
NEWS
Home | War in Ukraine | Coronavirus | Climate | Video | World | UK | Business | Tech | Science | Stories
World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

German parents told to destroy Cayla dolls over hacking fears

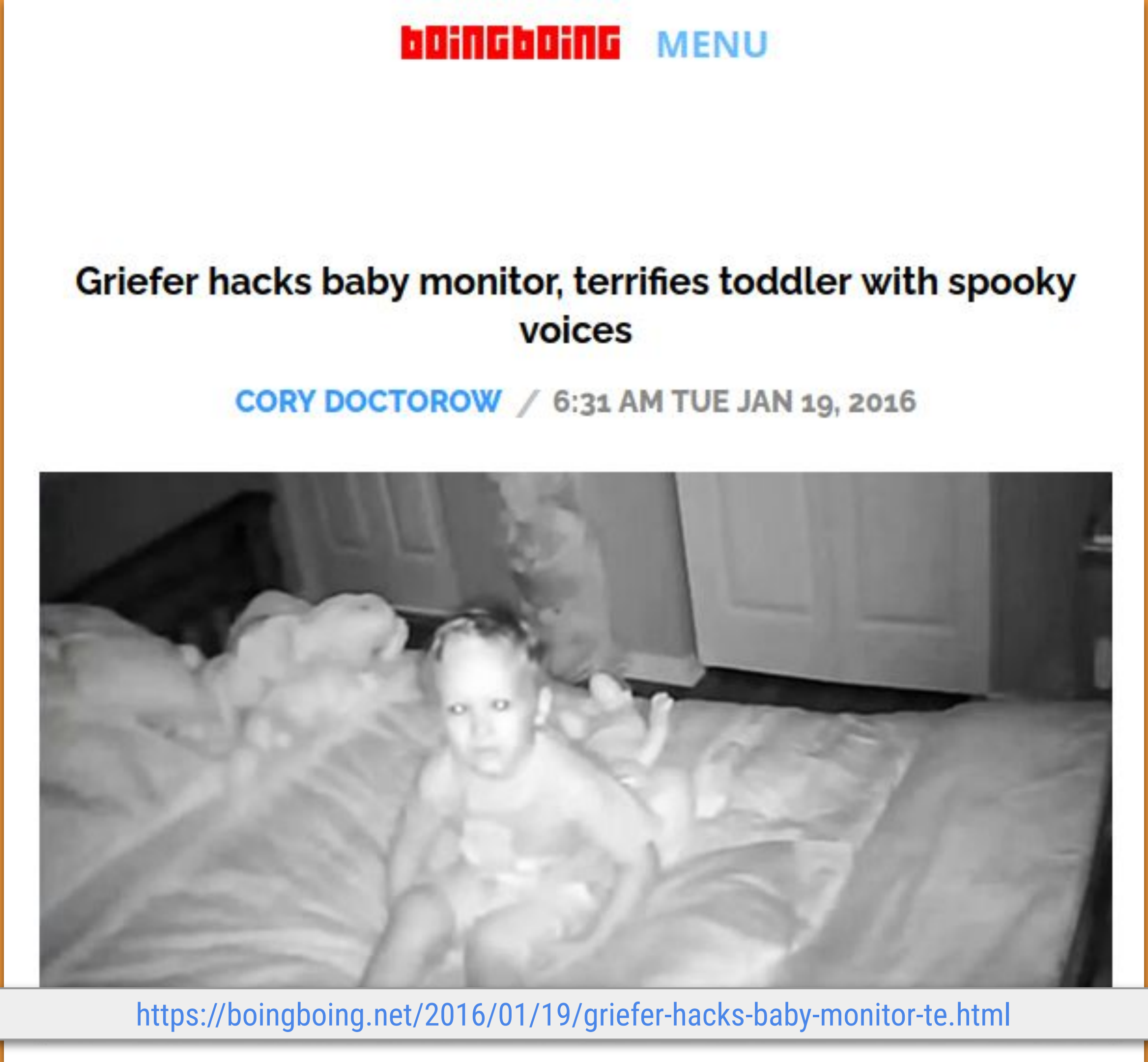
17 February 2017

https://www.bbc.com/news/world-europe-39002142



Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages

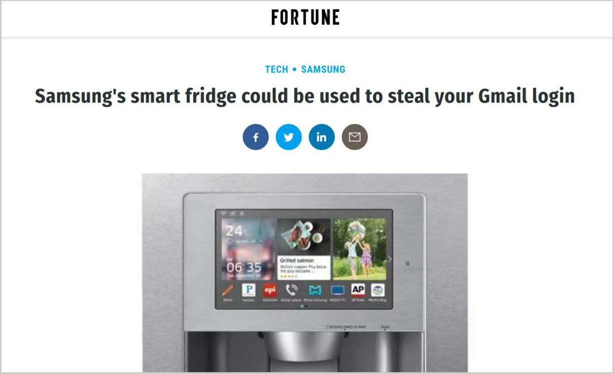
https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/



Griefer hacks baby monitor, terrifies toddler with spooky voices

CORY DOCTOROW / 6:31 AM TUE JAN 19, 2016

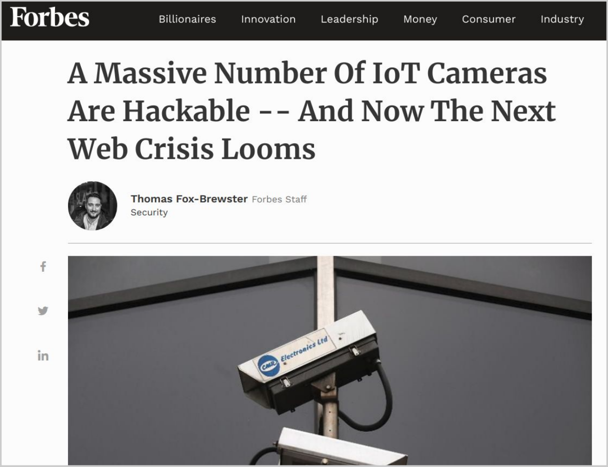
https://boingboing.net/2016/01/19/griefer-hacks-baby-monitor-te.html



FORTUNE

TECH • SAMSUNG

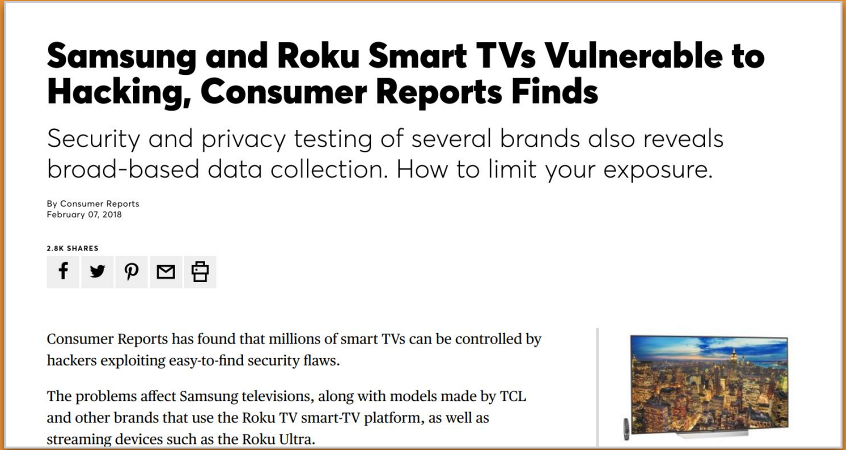
Samsung's smart fridge could be used to steal your Gmail login



Forbes Billionaires Innovation Leadership Money Consumer Industry

A Massive Number Of IoT Cameras Are Hackable -- And Now The Next Web Crisis Looms

Thomas Fox-Brewster Forbes Staff
Security



Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

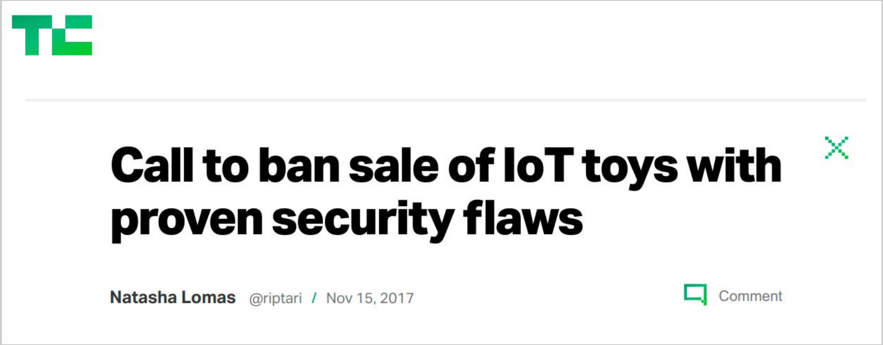
Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.

By Consumer Reports
February 07, 2018

2.8K SHARES

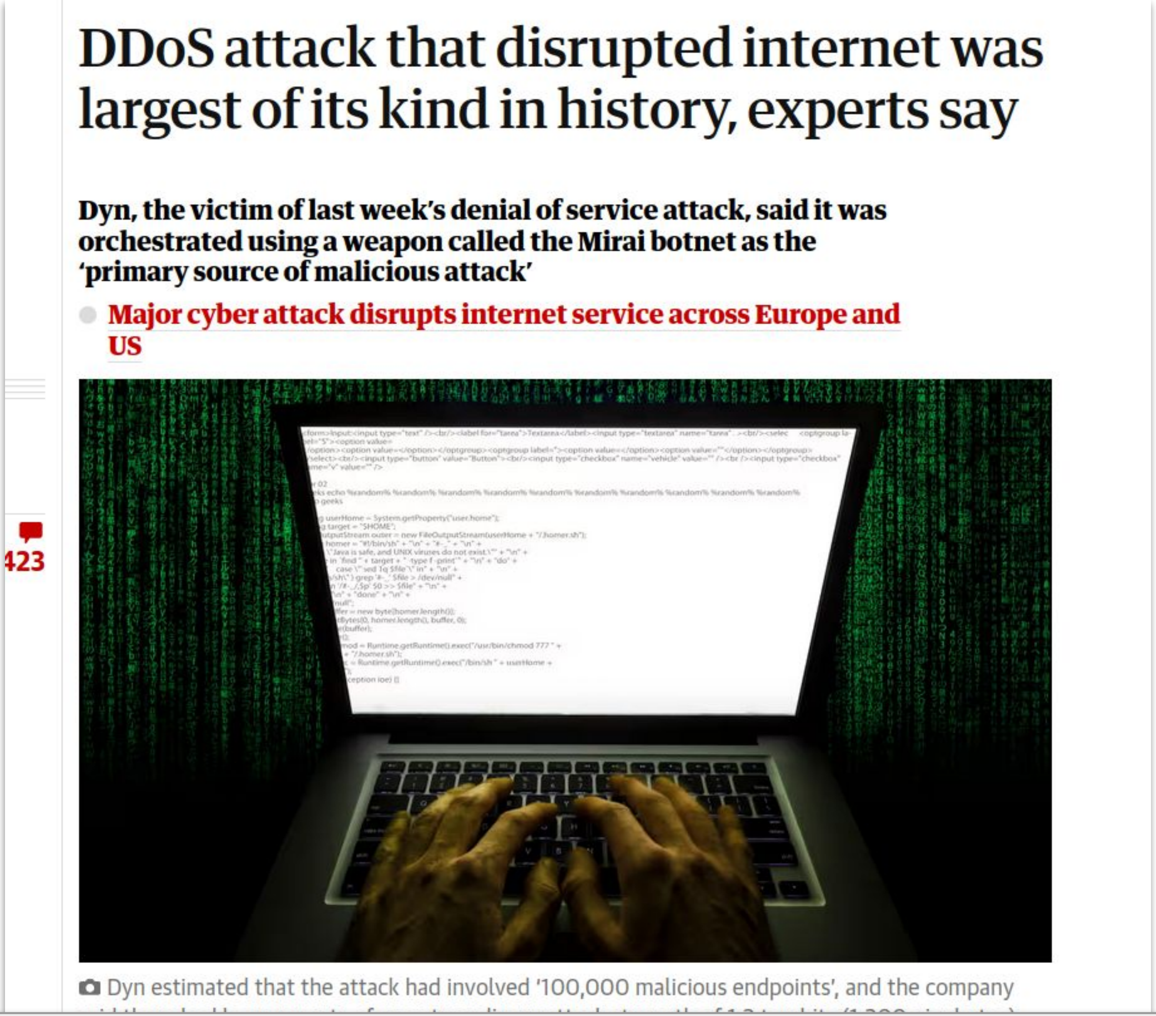
Consumer Reports has found that millions of smart TVs can be controlled by hackers exploiting easy-to-find security flaws.

The problems affect Samsung televisions, along with models made by TCL and other brands that use the Roku TV smart-TV platform, as well as streaming devices such as the Roku Ultra.



Call to ban sale of IoT toys with proven security flaws

Natasha Lomas @riptari / Nov 15, 2017 Comment



DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

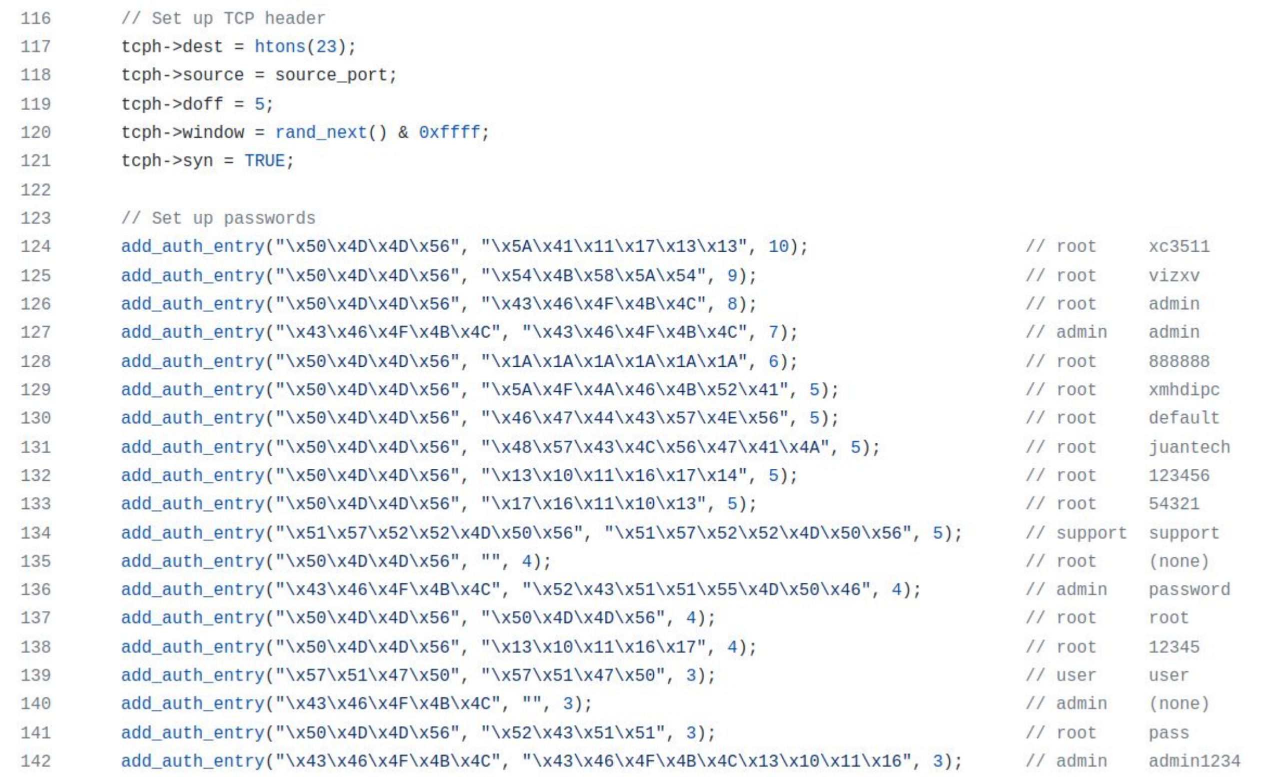
- Major cyber attack disrupts internet service across Europe and US

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Mirai attack

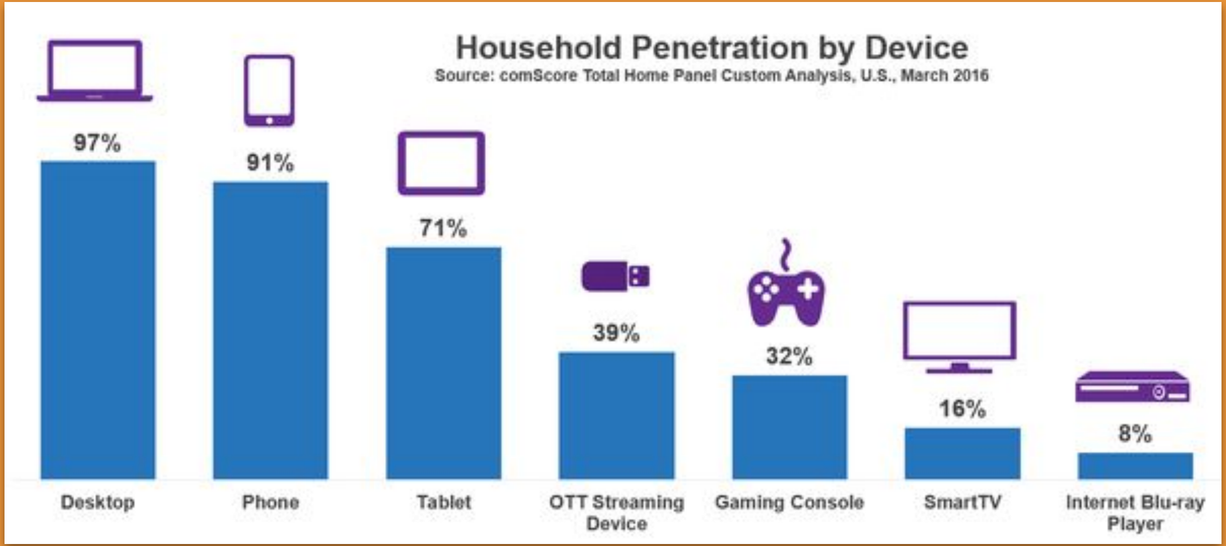
- Used IP cameras, routers to launch massive DDoS attacks
- Source code
- Understanding the Mirai Botnet



```
    // Set up TCP header
    tcph->dest = htons(23);
    tcph->source = source_port;
    tcph->doff = 5;
    tcph->window = rand_next() & 0xffff;
    tcph->syn = TRUE;

    // Set up passwords
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                      // root     xc3511
    add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                           // root     vizxv
    add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                           // root     admin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                       // admin    admin
    add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                       // root     888888
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                   // root     xmhdipc
    add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                   // root     default
    add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);               // root     juantech
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                       // root     123456
    add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                           // root     54321
    add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);       // support  support
    add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                               // root     (none)
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);           // admin    password
    add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                               // root     root
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                           // root     12345
    add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                               // user     user
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                           // admin    (none)
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                               // root     pass
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);       // admin    admin1234
```

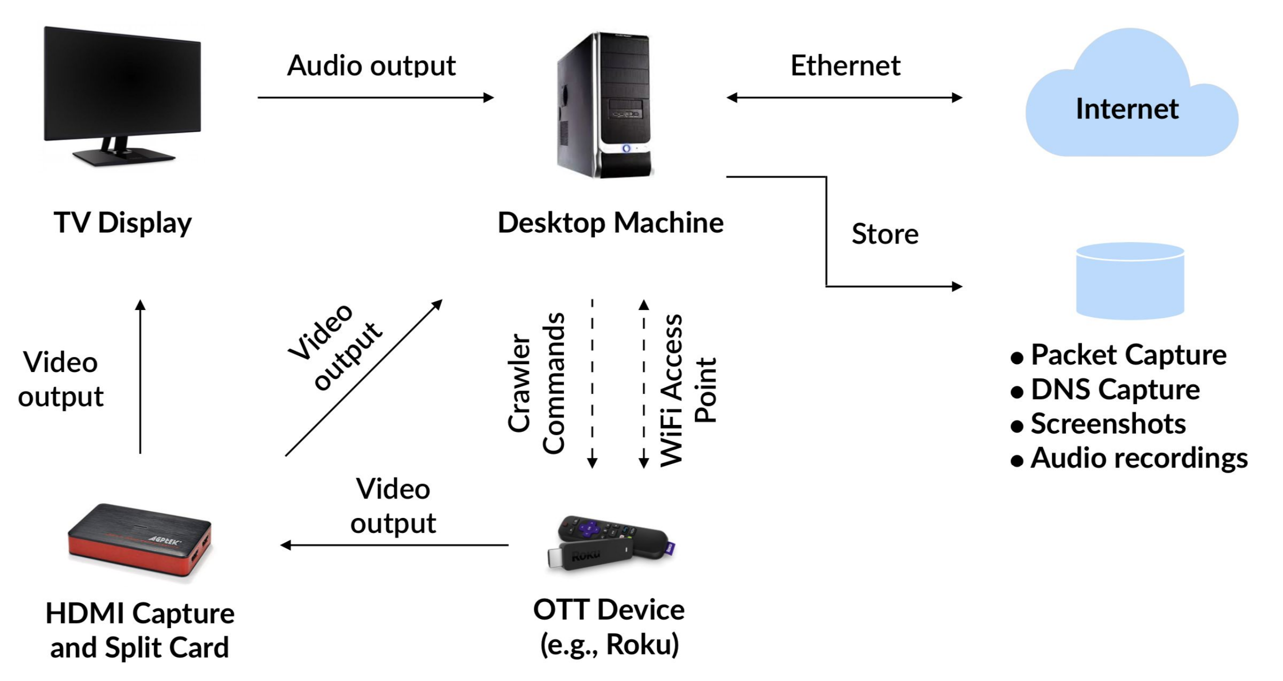
Over-the-Top TV Streaming Devices



Amazon FireTV

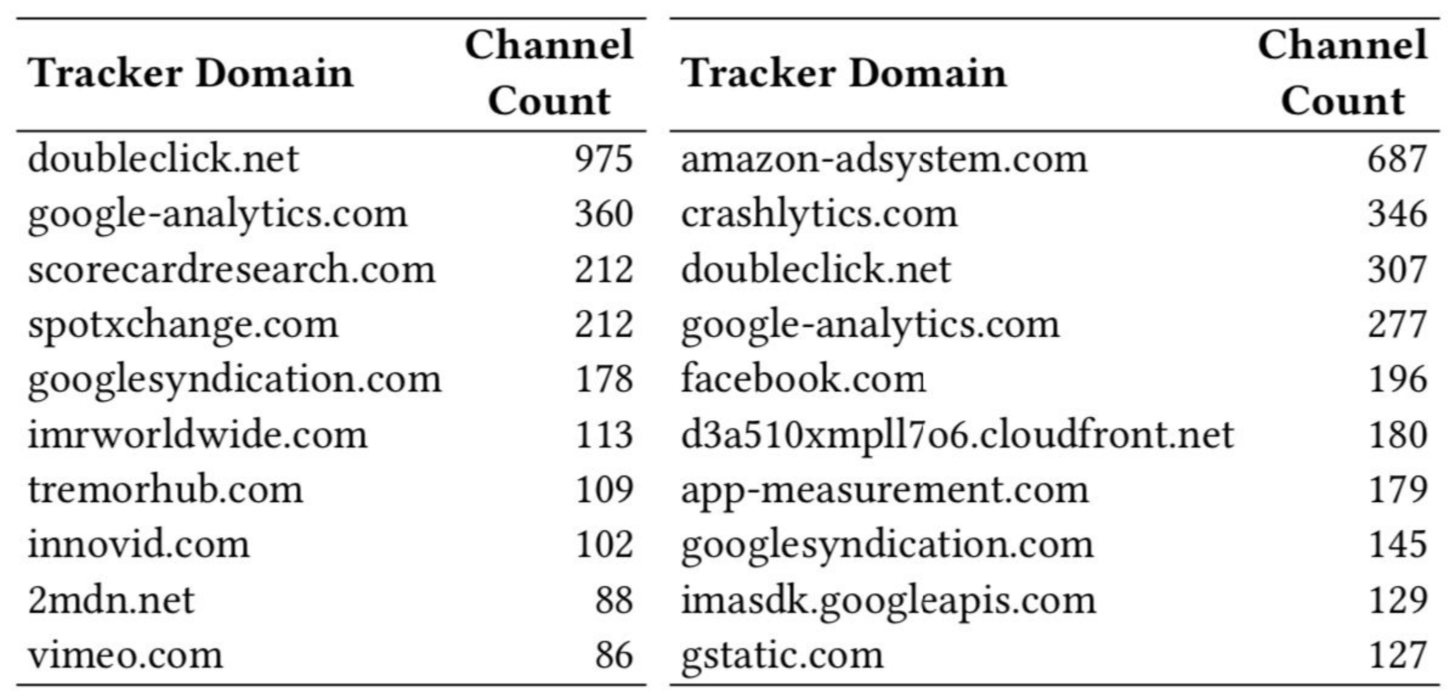
Roku

Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices (Moghaddam et al. ,CCS'19)



- Packet Capture
- DNS Capture
- Screenshots
- Audio recordings

3rd-party trackers



Roku

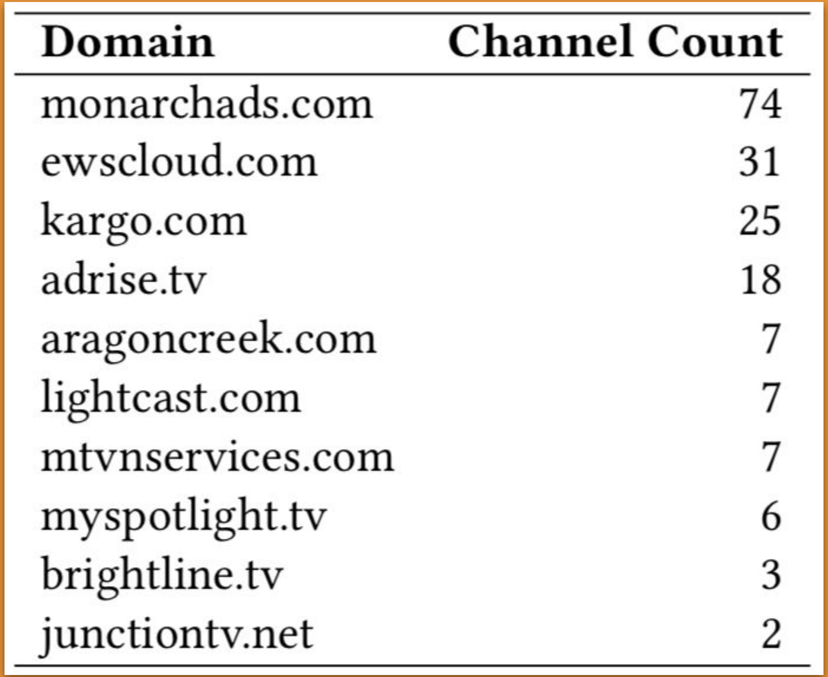
Tracker Domain	Channel Count
doubleclick.net	975
google-analytics.com	360
scorecardresearch.com	212
spotxchange.com	212
googlesyndication.com	178
imrworldwide.com	113
tremorhub.com	109
innovid.com	102
2mdn.net	88
vimeo.com	86

Amazon

Tracker Domain	Channel Count
amazon-adsystem.com	687
crashlytics.com	346
doubleclick.net	307
google-analytics.com	277
facebook.com	196
d3a510xmpll7o6.cloudfront.net	180
app-measurement.com	179
googlesyndication.com	145
imasdk.googleapis.com	129
gstatic.com	127

Previously unknown trackers

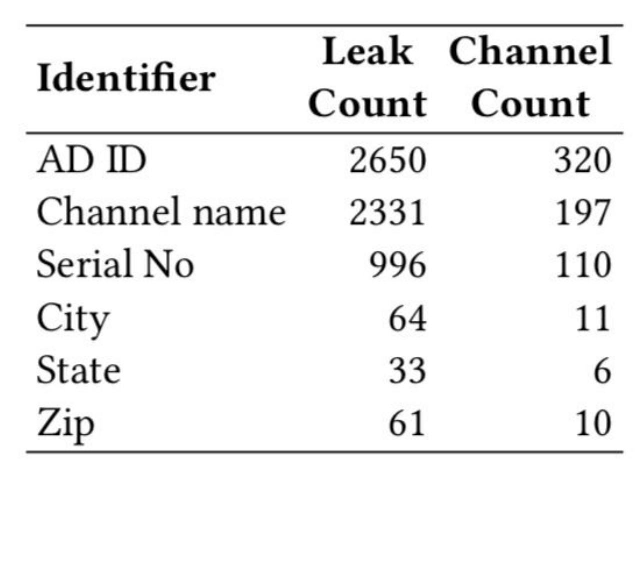
Roku



Domain	Channel Count
monarchads.com	74
ewscloud.com	31
kargo.com	25
adrise.tv	18
aragoncreek.com	7
lightcast.com	7
mtvnservices.com	7
myspotlight.tv	6
brightline.tv	3
junctiontv.net	2

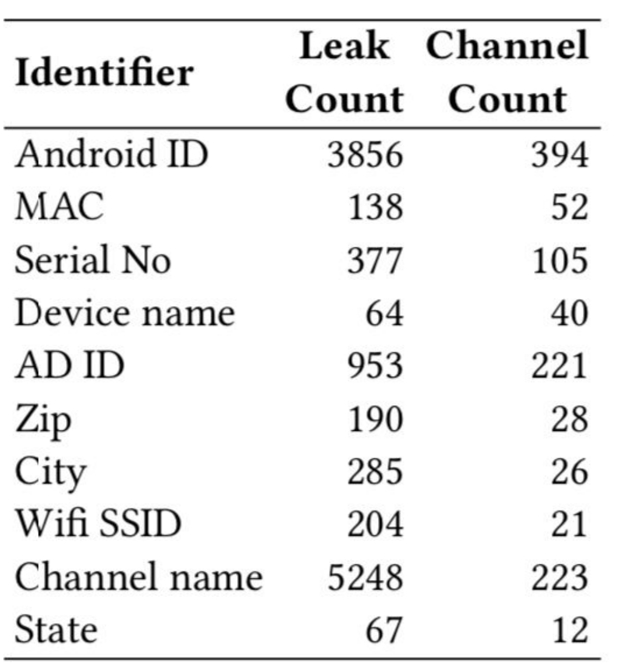
Device and location identifiers (found in the traffic)

Roku



Identifier	Leak	Channel
	Count	Count
AD ID	2650	320
Channel name	2331	197
Serial No	996	110
City	64	11
State	33	6
Zip	61	10

Amazon



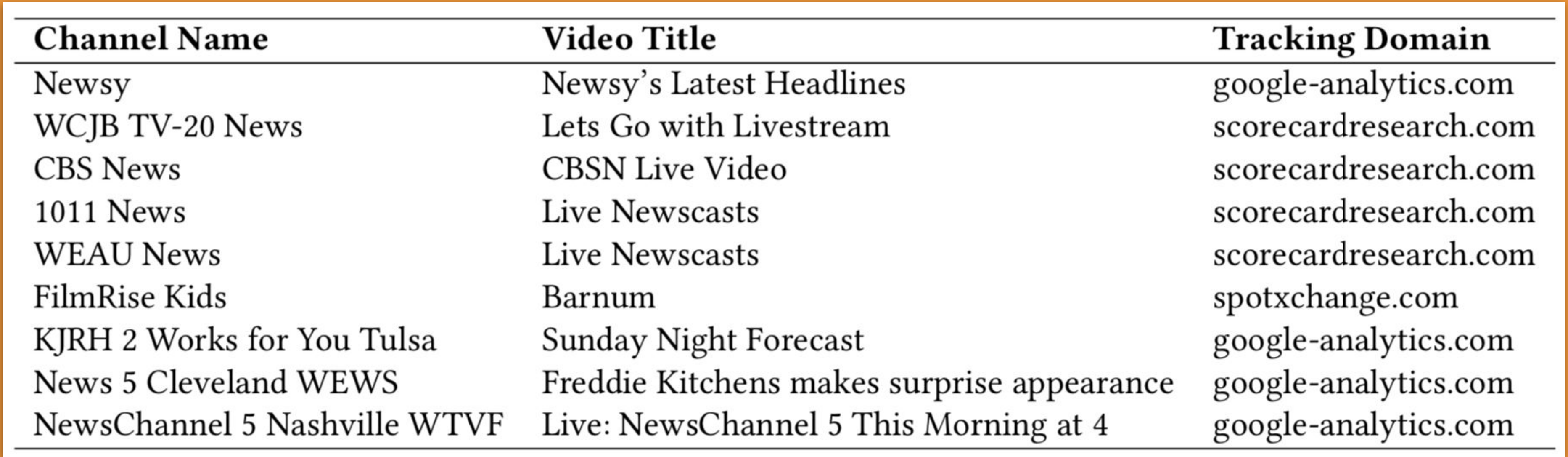
Identifier	Leak	Channel
	Count	Count
Android ID	3856	394
MAC	138	52
Serial No	377	105
Device name	64	40
AD ID	953	221
Zip	190	28
City	285	26
Wifi SSID	204	21
Channel name	5248	223
State	67	12

Analyzing packet captures

- Compile list of search terms (e.g. potential identifiers)
  - encodings, hashes
- Search in PCAP files
  - Use **Wireshark** to manually explore and analyze
  - Use **tshark** to automatically parse and extract protocol fields

Video titles shared with 3rd-party trackers

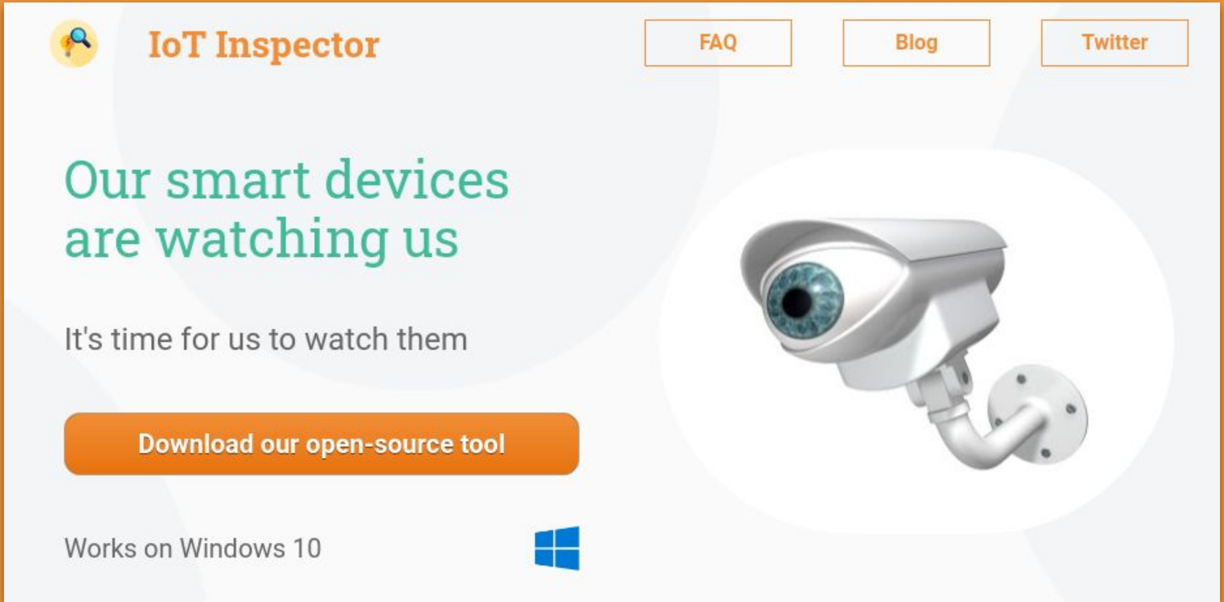
Roku



Channel Name	Video Title	Tracking Domain
Newsy	Newsy's Latest Headlines	google-analytics.com
WCJB TV-20 News	Lets Go with Livestream	scorecardresearch.com
CBS News	CBSN Live Video	scorecardresearch.com
1011 News	Live Newscasts	scorecardresearch.com
WEAU News	Live Newscasts	scorecardresearch.com
FilmRise Kids	Barnum	spotxchange.com
KJRH 2 Works for You Tulsa	Sunday Night Forecast	google-analytics.com
News 5 Cleveland WEWS	Freddie Kitchens makes surprise appearance	google-analytics.com
NewsChannel 5 Nashville WTVF	Live: NewsChannel 5 This Morning at 4	google-analytics.com

IoT Security and Privacy Studies: Lab vs Crowdsourcing

- IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale (Huang et al., IMWUT’20).



IoT Inspector

FAQ

Blog

Twitter

Our smart devices are watching us

It's time for us to watch them

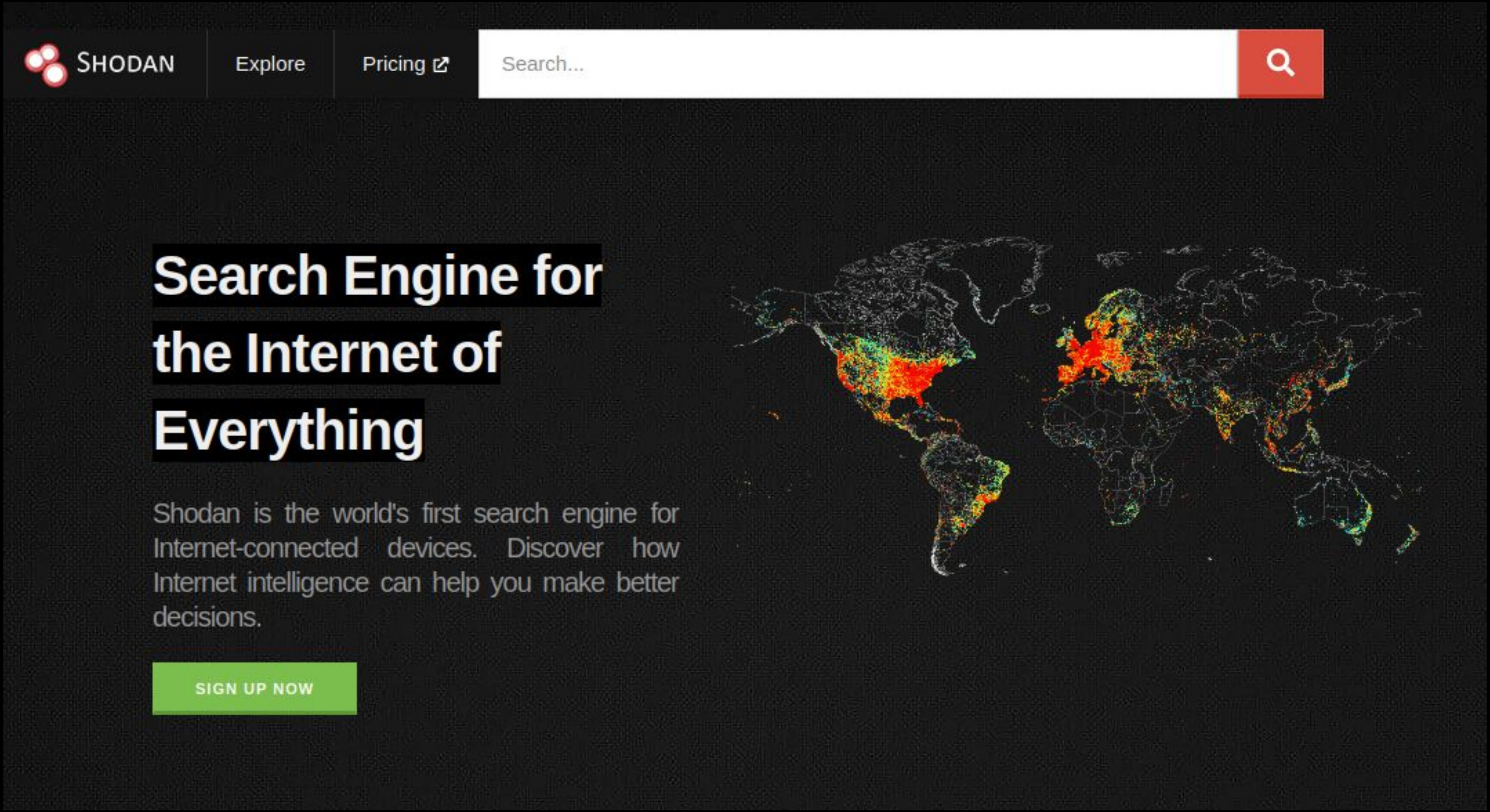
Download our open-source tool

Works on Windows 10

Other IoT attack surfaces

How to reach local IoT devices?

- **Public facing devices** (e.g., port forwarding)
  - reachable, under more risk
  - Shodan!
- Local malware
- Web-based attacks



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

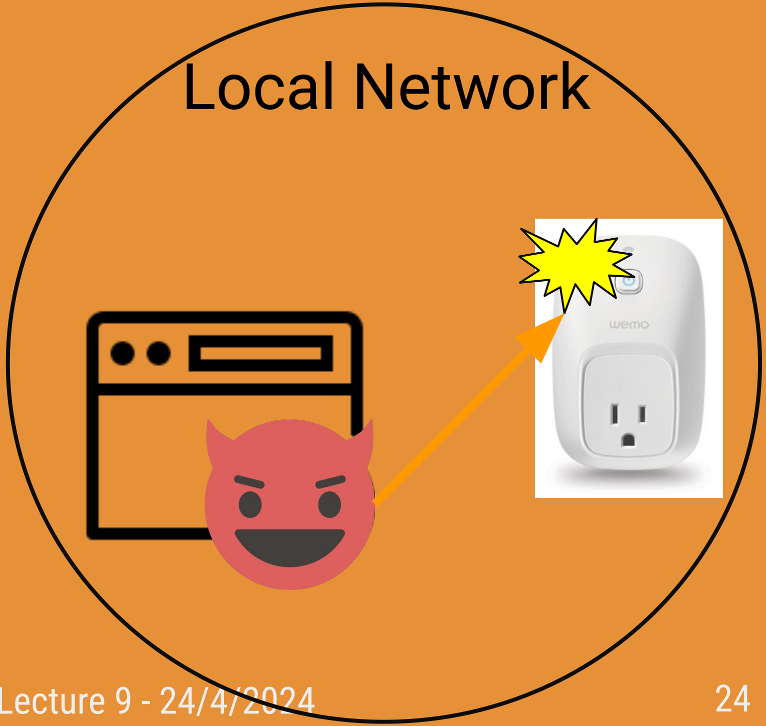
https://www.shodan.io/

How to reach local IoT devices?

- Public devices (e.g., port forwarding)
- Local malware
- **Web-based attacks**

How to reach local IoT devices?

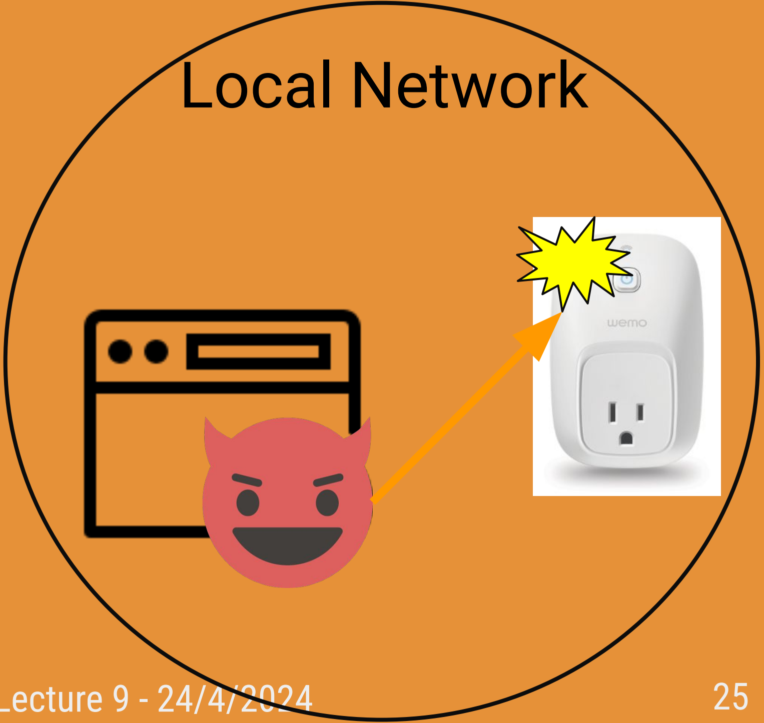
- Public devices (e.g., port forwarding)
- Local malware
- **Web-based attacks**

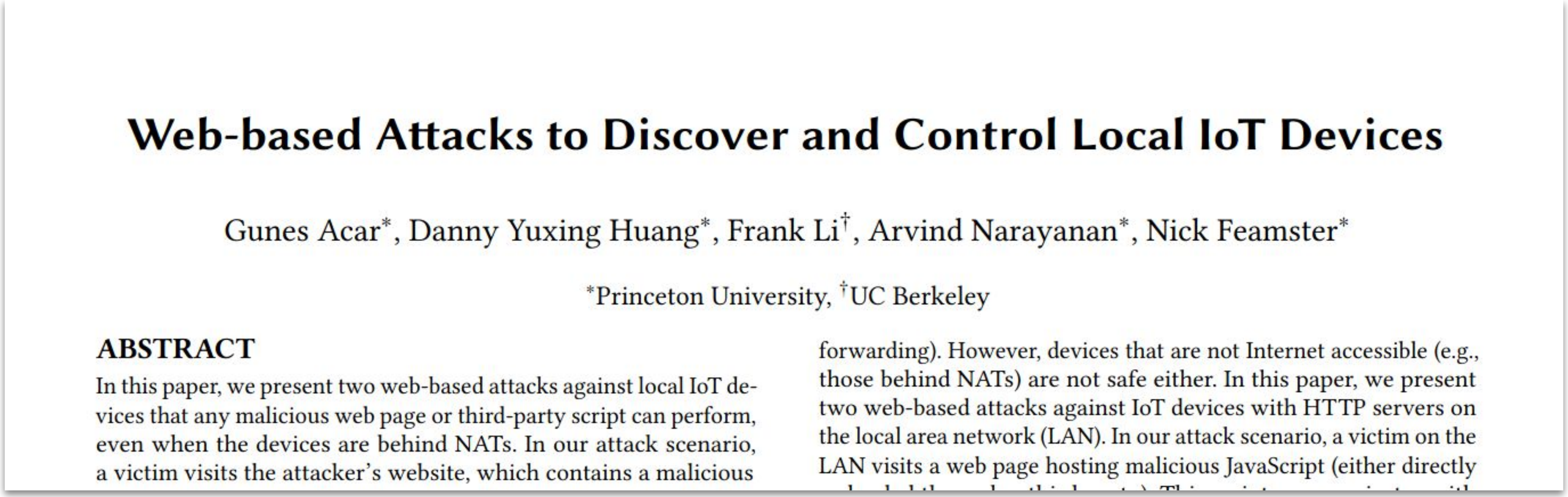


How to reach local IoT devices?

- Public devices (e.g., port forwarding)
- Local malware
- **Web-based attacks**

1. Discover certain IoT devices
2. Access & control IoT devices





Web-based Attacks to Discover and Control Local IoT Devices

Gunes Acar*, Danny Yuxing Huang*, Frank Li†, Arvind Narayanan*, Nick Feamster*

*Princeton University, †UC Berkeley

ABSTRACT

In this paper, we present two web-based attacks against local IoT devices that any malicious web page or third-party script can perform, even when the devices are behind NATs. In our attack scenario, a victim visits the attacker's website, which contains a malicious

forwarding). However, devices that are not Internet accessible (e.g., those behind NATs) are not safe either. In this paper, we present two web-based attacks against IoT devices with HTTP servers on the local area network (LAN). In our attack scenario, a victim on the LAN visits a web page hosting malicious JavaScript (either directly

Paper (IoT S&P'18) / Blog post

Attack overview

- Find HTTP endpoints by interacting with the devices
- Use DNS rebinding to bypass origin-based restrictions

Attack 1:

Identify Local IoT Devices

Attack on Devices - Google Home/Chromecast

- Play arbitrary Youtube videos on Chromecast
- Reboot Chromecast/Home
- Scan for WiFi networks and return information

Attack Demo

https://www.youtube.com/watch?v=KsleJlj4XB8

Implications

- Attacker control of IoT device actions
- Exploiting IoT device vulnerabilities for full compromise
- Privacy leaks (e.g., extensive device fingerprinting or user profiling)

Attack on Devices: Google Home/Chromecast

Access:

- Unique device ID
- Build/firmware version
- SSID of connected WiFi network
- Device schedules/alarms (Home)

Attack on Devices: Google Home/Chromecast

Control:

- Reboot device
- Play any video (Chromecast)
- Scan for WiFi networks and return SSIDs detected

Responsible Disclosure

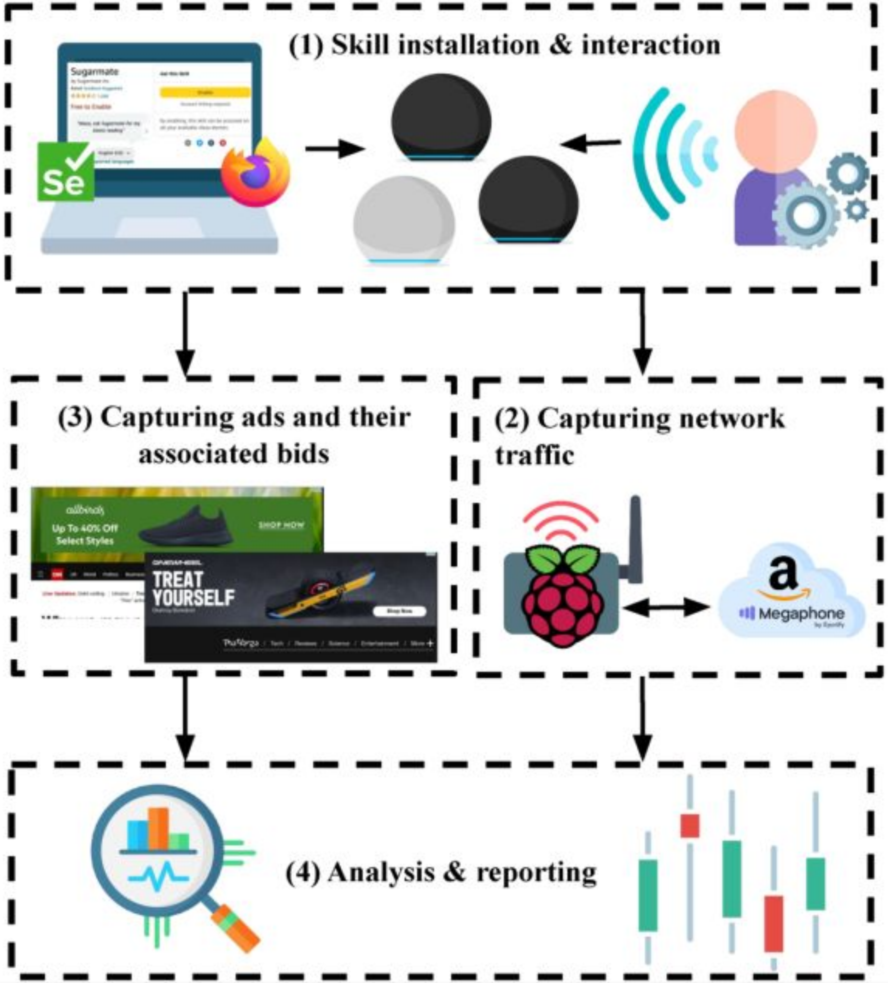
- Reported the vulnerabilities to...
  - Browser vendors: Chromium (Google), Mozilla
  - IoT vendors: Google, Samsung, D-Link, Belkin
- Both Chromium and Mozilla offered bug bounty of $500
  - Fixed, released
- Google Home: known issue
- Belkin promised to release a patch in August
- Ack from Samsung
- No response from D-Link

Gathering data from IoT devices

- More difficult compared to browsers
- No automation libraries
- No way to get a feedback about the state of the device

Gathering data from IoT devices

- Set up fake wireless access point (e.g., via **hostapd**)
  - bridge to an I/F with an Internet connection
  - capture packets
  - *optional*: **mitm**
- What can we do when mitm attacks against TLS is not possible?
  - e.g. due to cert pinning



(1) Skill installation & interaction

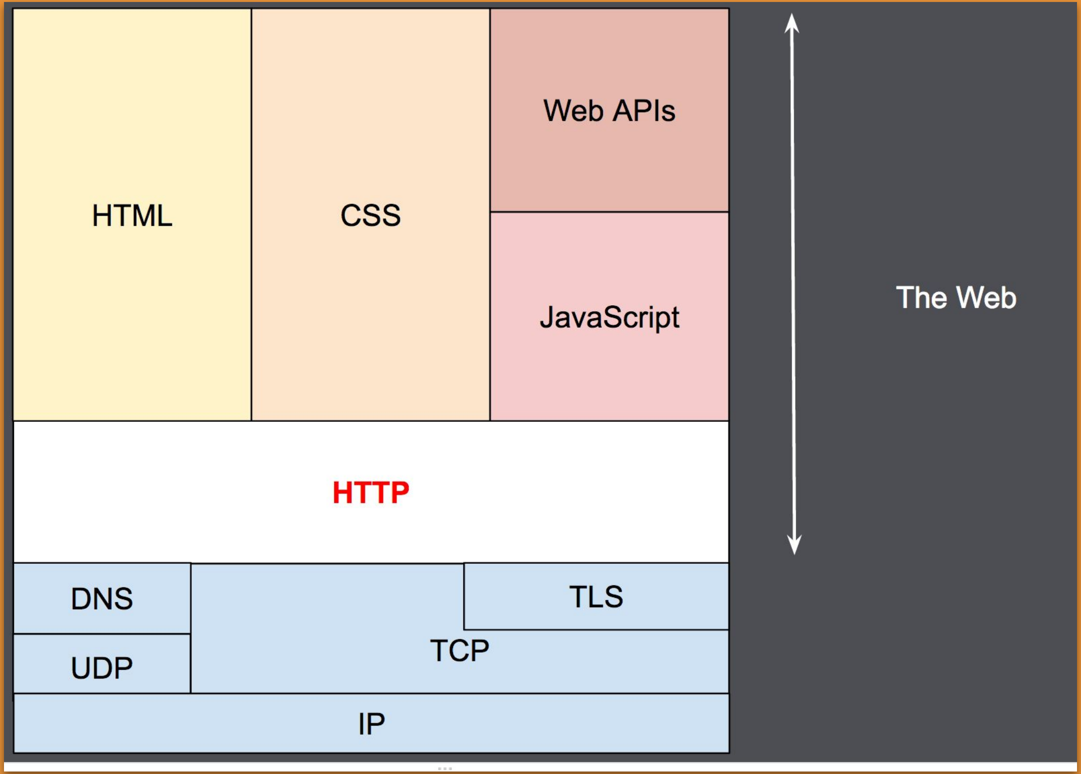
(2) Capturing network traffic

(3) Capturing ads and their associated bids

(4) Analysis & reporting

Iqbal et al. Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem (IMC'23)

HTTP and below (MDN)



HTTP

- Unencrypted HTTP, used to be default
- Very uncommon thanks to
  - Let’s encrypt
  - Downranking by Google
  - Many new web features are only available on HTTPS

DNS leaks

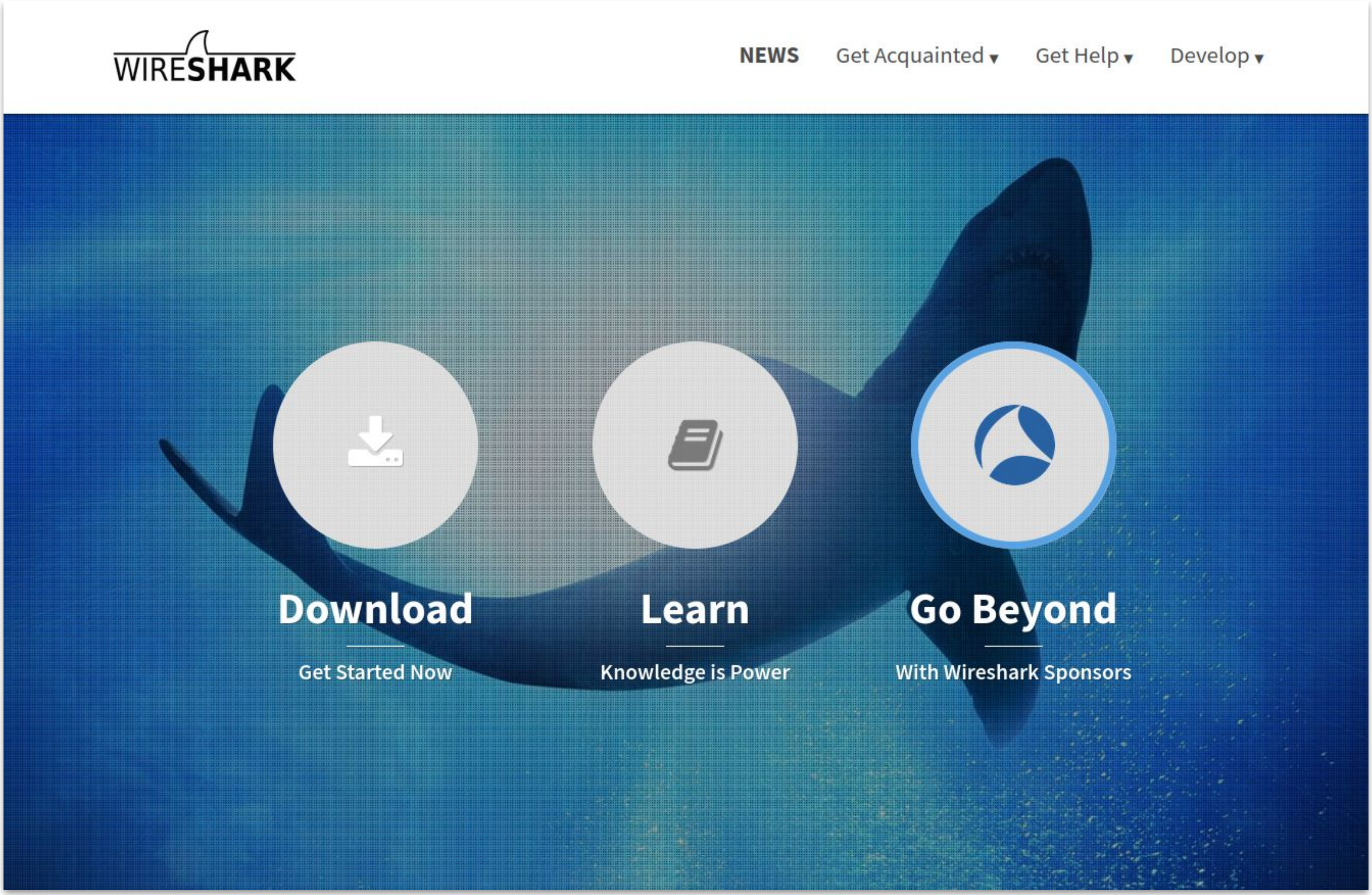
- Queries sent unencrypted unless DoH & DoT
- DoH: DNS-over-HTTPS
- DoT: DNS-over-TLS

SNI leaks

- Server Name Indication
  - reveals the hostname you are connecting to
- Enables serving multiple sites on one IP (e.g. CDNs)
- Contains the visited website address (*not the page URL*)
- ECH: Encrypted Client Hello
  - eSNI: encrypted SNI

Wireshark

- packet capture with GUI
- filter by protocol, field names and values
- command line alternatives: **tcpdump, dumpcap**
- **tshark:** scripted parsing of pcaps from the cmd line



WIRESHARK

NEWS Get Acquainted ▾ Get Help ▾ Develop ▾

Download

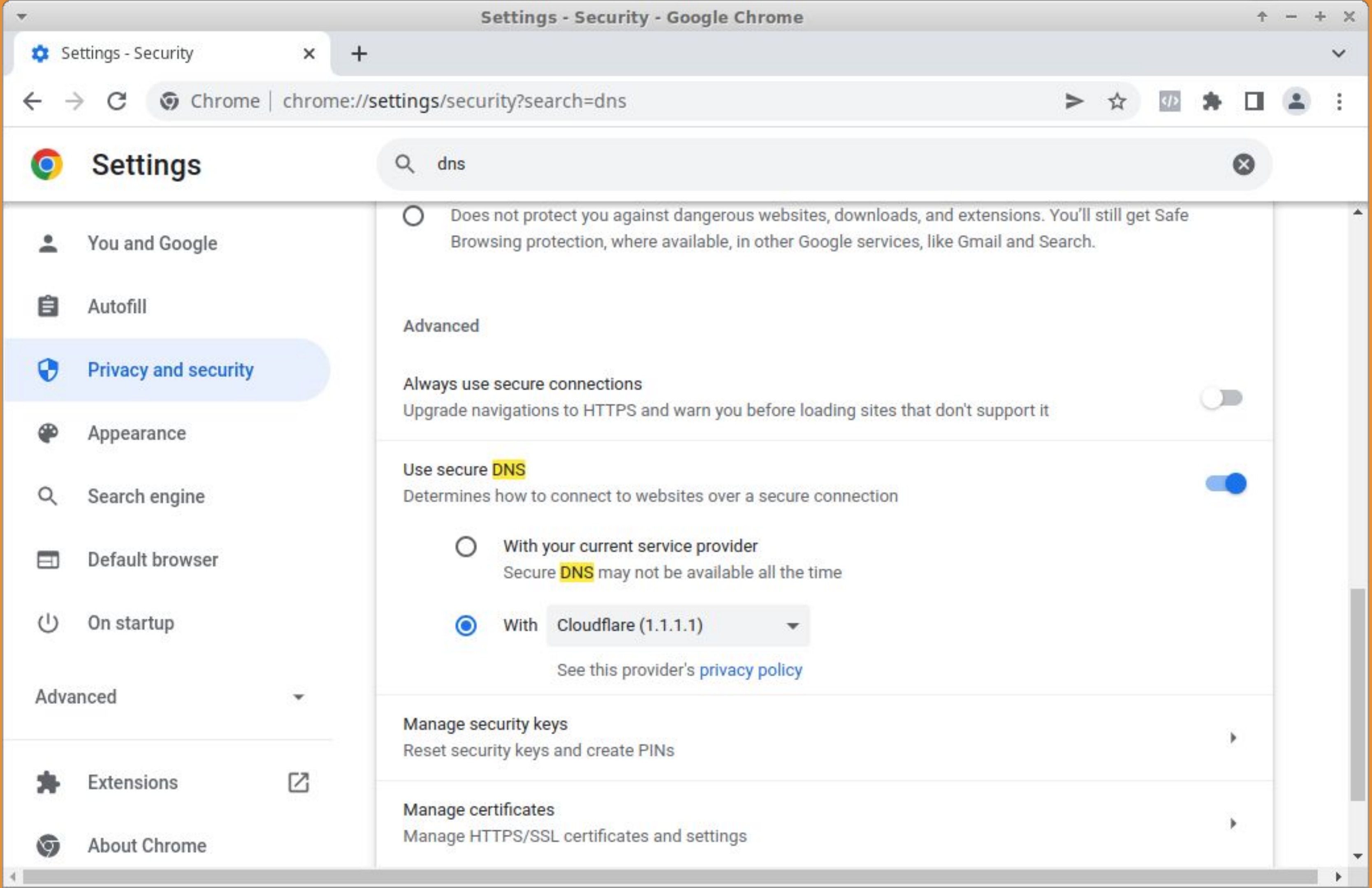
Get Started Now

Learn

Knowledge is Power

Go Beyond

With Wireshark Sponsors



○ Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Advanced

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

Use secure DNS
Determines how to connect to websites over a secure connection

○ With your current service provider
Secure DNS may not be available all the time

● With Cloudflare (1.1.1.1)

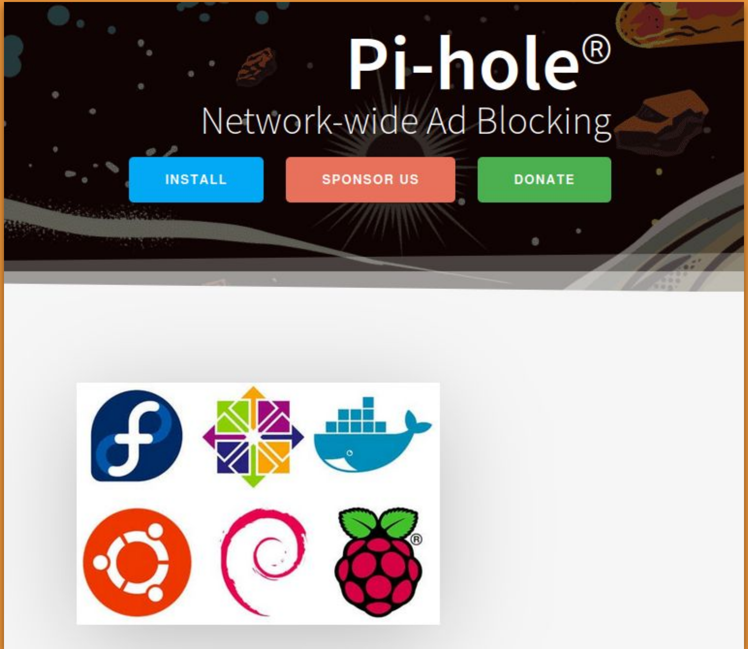
See this provider's privacy policy

Manage security keys
Reset security keys and create PINs

Manage certificates
Manage HTTPS/SSL certificates and settings

Countermeasures

- Few options are available (cf. adblockers)
- PiHole: DNS-based blocking



Recap

- Most smart and connected devices are privacy and security risks
- Smart TV channels contain many trackers
- Few defenses are available