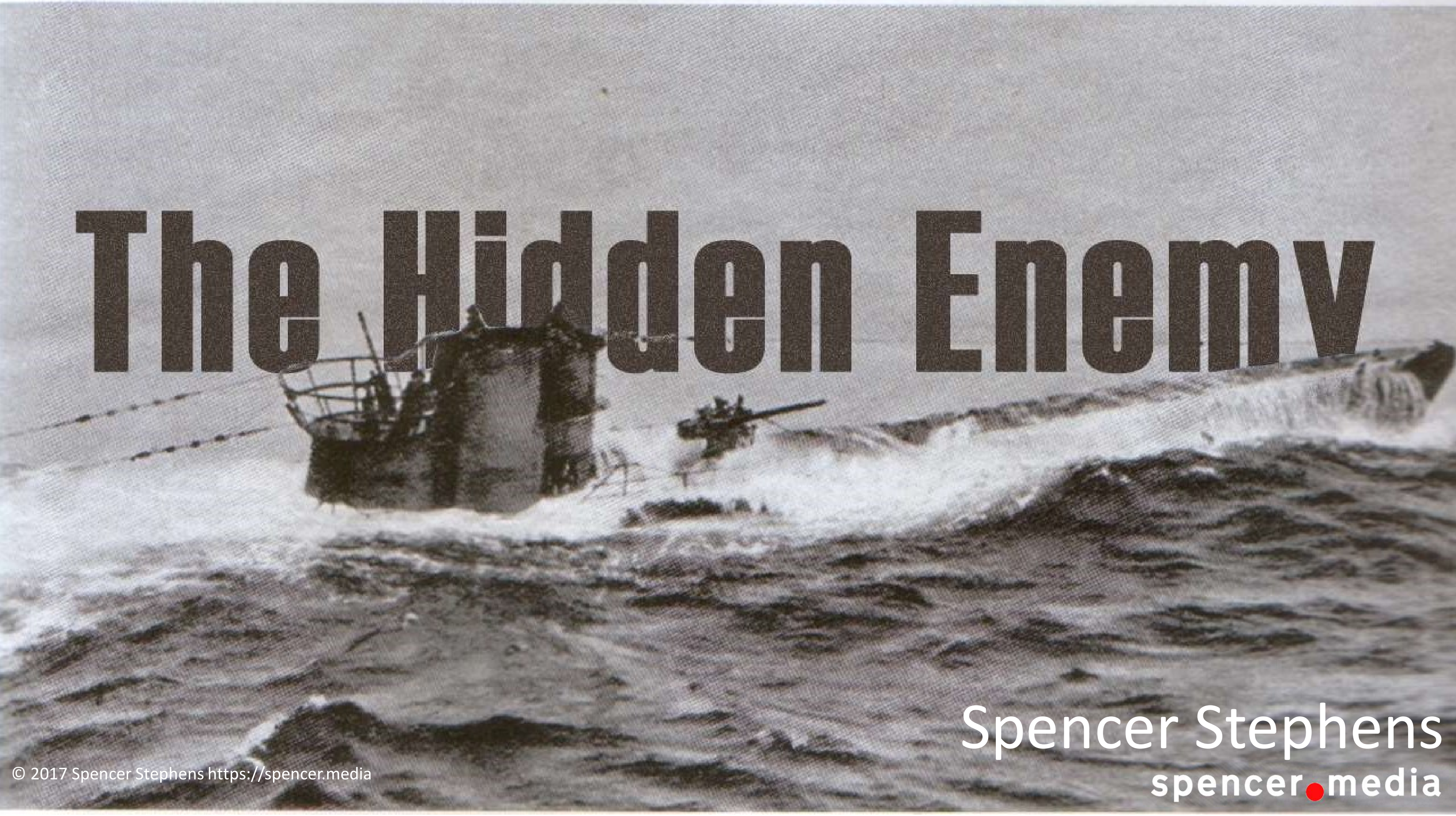


The Hidden Enemy

Spencer Stephens

spencer.media

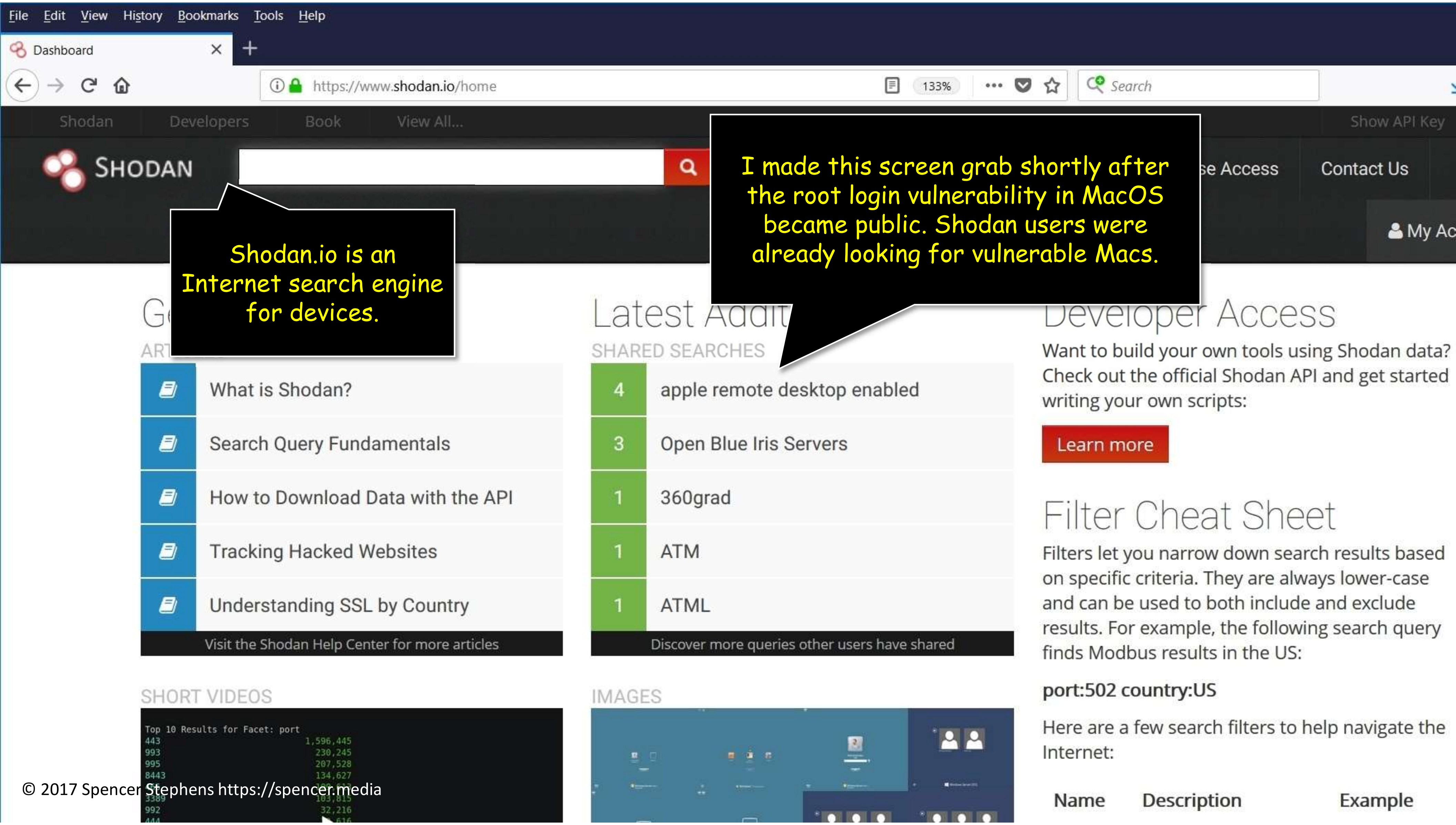
“There are known knowns, things we know that we know; and there are known unknowns, things that we know we don't know. But there are also unknown unknowns, things we do not know we don't know.”

Donald Rumsfeld
Known and Unknown: A Memoir

IoT

Rule 1: If it has a vulnerability and it’s connected the Internet, someone will find it and exploit it.

Rule 2: There is no evidence that a hacked IoT device affects sales.



Shodan.io is an Internet search engine for devices.

I made this screen grab shortly after the root login vulnerability in MacOS became public. Shodan users were already looking for vulnerable Macs.

Ge

ART

- What is Shodan?
- Search Query Fundamentals
- How to Download Data with the API
- Tracking Hacked Websites
- Understanding SSL by Country

Visit the Shodan Help Center for more articles

Latest Addit

SHARED SEARCHES

4	apple remote desktop enabled
3	Open Blue Iris Servers
1	360grad
1	ATM
1	ATML

Discover more queries other users have shared

Developer Access

Want to build your own tools using Shodan data? Check out the official Shodan API and get started writing your own scripts:

Learn more

Filter Cheat Sheet

Filters let you narrow down search results based on specific criteria. They are always lower-case and can be used to both include and exclude results. For example, the following search query finds Modbus results in the US:

port:502 country:US

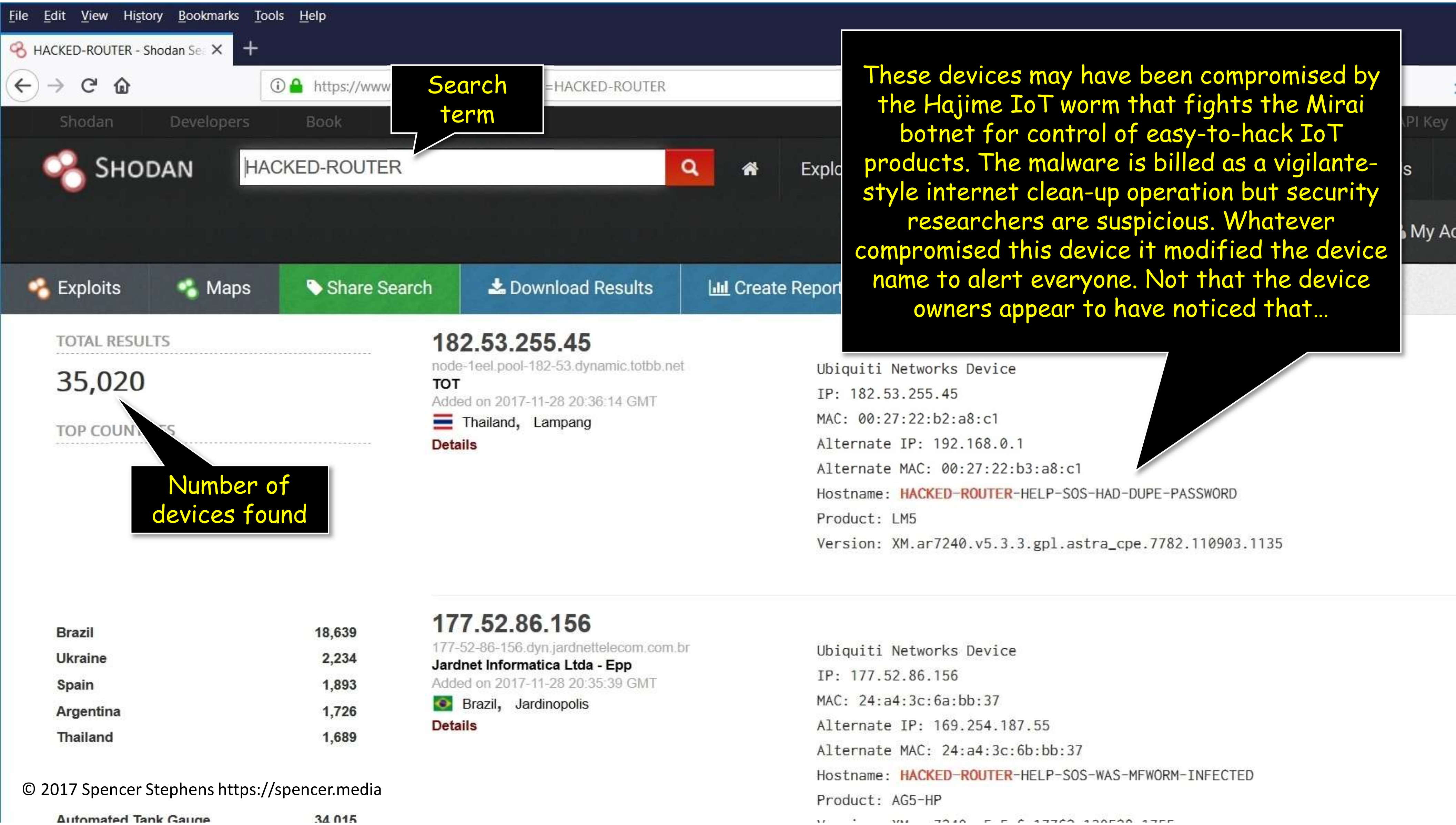
Here are a few search filters to help navigate the Internet:

Name	Description	Example

SHORT VIDEOS

```
Top 10 Results for Facet: port
443                               1,596,445
993                                 230,245
995                                 207,528
8443                                134,627
[illegible]
3389                                103,815
992                                  32,216
444                                     616
```

IMAGES



Search term

These devices may have been compromised by the Hajime IoT worm that fights the Mirai botnet for control of easy-to-hack IoT products. The malware is billed as a vigilante-style internet clean-up operation but security researchers are suspicious. Whatever compromised this device it modified the device name to alert everyone. Not that the device owners appear to have noticed that…

TOTAL RESULTS

35,020

Number of devices found

TOP COUNTRIES

Brazil	18,639
Ukraine	2,234
Spain	1,893
Argentina	1,726
Thailand	1,689

Automated Tank Gauge	34,015

182.53.255.45
node-1eel.pool-182-53.dynamic.totbb.net
TOT
Added on 2017-11-28 20:36:14 GMT
Thailand, Lampang
Details

```
Ubiquiti Networks Device
IP: 182.53.255.45
MAC: 00:27:22:b2:a8:c1
Alternate IP: 192.168.0.1
Alternate MAC: 00:27:22:b3:a8:c1
Hostname: HACKED-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD
Product: LM5
Version: XM.ar7240.v5.3.3.gpl.astra_cpe.7782.110903.1135
```

177.52.86.156
177-52-86-156.dyn.jardnettelecom.com.br
Jardnet Informatica Ltda - Epp
Added on 2017-11-28 20:35:39 GMT
Brazil, Jardinopolis
Details

```
Ubiquiti Networks Device
IP: 177.52.86.156
MAC: 24:a4:3c:6a:bb:37
Alternate IP: 169.254.187.55
Alternate MAC: 24:a4:3c:6b:bb:37
Hostname: HACKED-ROUTER-HELP-SOS-WAS-MFWORM-INFECTED
Product: AG5-HP
```

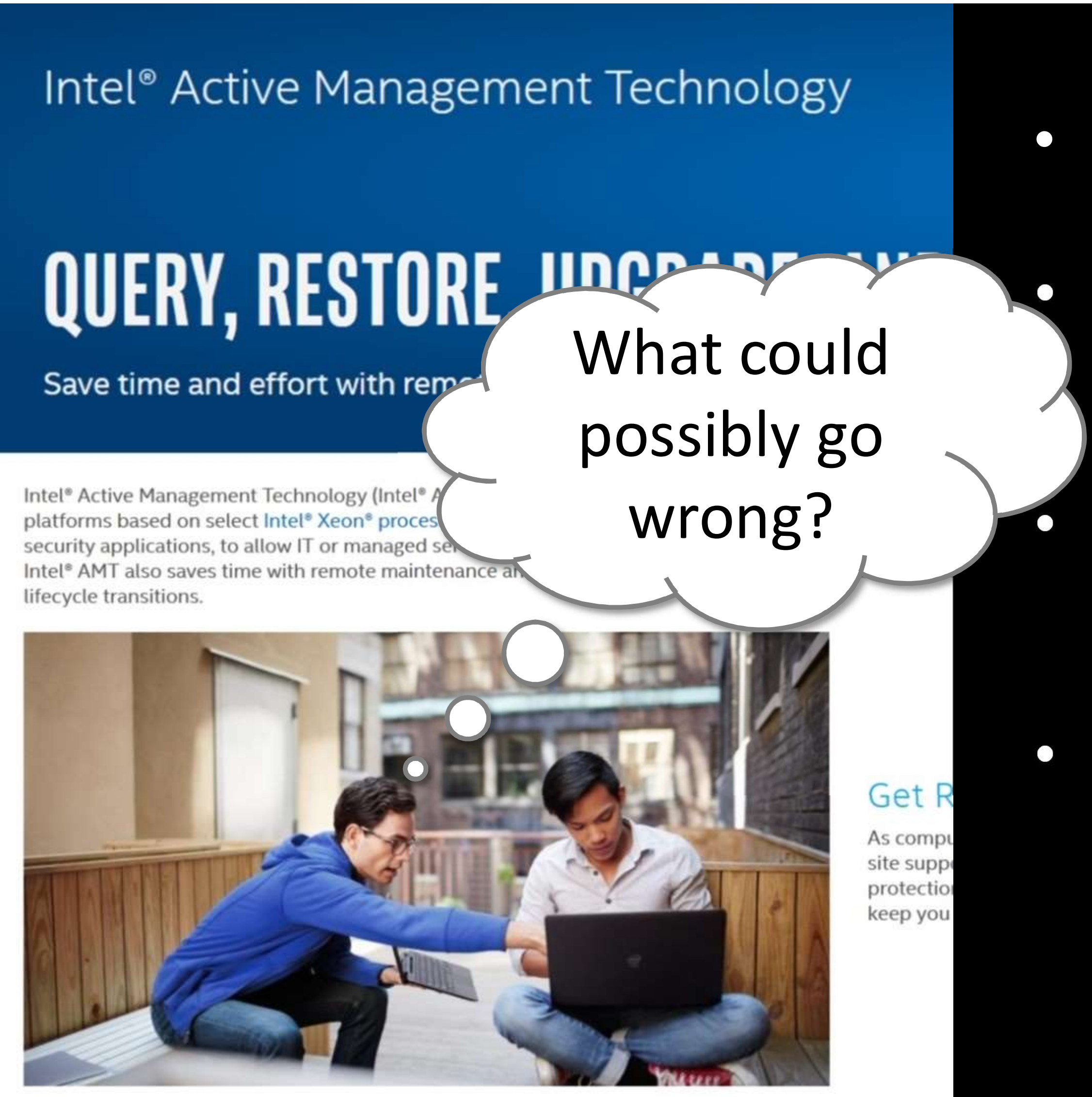
The security of an alarming number of IoT devices is, at best, comparable to the security of the content protection in a DVD player, CSS, which was launched over 20 years ago.

Content protection has come a long way since then: http://movielabs.com/solutions-specifications/enhanced-content-protection-ecp/

Feature	DVD Player	IoT Devices*
Security robustness not a selling feature	✓	✓
Security design limited by device processor/memory	✓	✓
Global secret	✓	✓
Secrets stored as plaintext	✓	✓
Hacked by downloadable exploits	✓	✓
Renewable security	✗	✗
Manufacturers expect to provide long term updates	✗	✗

* This is not to imply that all IoT devices exhibit any or all of these weaknesses

Malware in the Hardware



Intel® Active Management Technology

QUERY, RESTORE

Save time and effort with rem

Intel® Active Management Technology (Intel® A
platforms based on select Intel® Xeon® proces
security applications, to allow IT or managed se
Intel® AMT also saves time with remote maintenance ar
lifecycle transitions.

Get R

As compu
site supp
protectio
keep you

- AMT runs at the firmware level, below the operating system
- The code runs on Intel's Management Engine, a tiny computer within your computer
- It has full control of the hardware and talks directly to the network port
- AMT allows a device to be remotely controlled regardless of what OS and applications are running above it

MAY 2nd, 2017

CVE-2017-5689

An unprivileged network attacker could gain system privileges to provisioned Intel manageability SKUs: Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM). An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability SKUs: Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), and Intel Small Business Technology (SBT).

https://nvd.nist.gov/vuln/detail/CVE-2017-5689

This vulnerability is reported to have been in Intel’s Management Engine since 2010

November 20th, 2017

Intel today admitted its Management Engine (ME), Server Platform Services (SPS), and Trusted Execution Engine (TXE) are vulnerable to multiple worrying security flaws, based on the findings of external security experts.

The firmware-level bugs allow logged-in administrators, and malicious or hijacked high-privilege processes, to run code beneath the operating system to spy on or meddle with the computer completely out of sight of other users and admins. The holes can also be exploited by network administrators, or people masquerading as admins, to remotely infect machines with spyware and invisible rootkits, potentially.

Meanwhile, logged-in users, or malicious or commandeered applications, can leverage the security weaknesses to extract confidential and protected information from the computer's memory, potentially giving miscreants sensitive data – such as passwords or cryptographic keys – to kick off other attacks. This is especially bad news on servers and other shared machines.

https://www.theregister.co.uk/2017/11/20/intel_flags_firmware_flaws/

CVE-2017-5705
CVE-2017-5708
CVE-2017-5711
CVE-2017-5712
CVE-2017-5711
CVE-2017-5712
CVE-2017-5706
CVE-2017-5709
CVE-2017-5707
CVE-2017-5710

2FA

Pop quiz, which one?

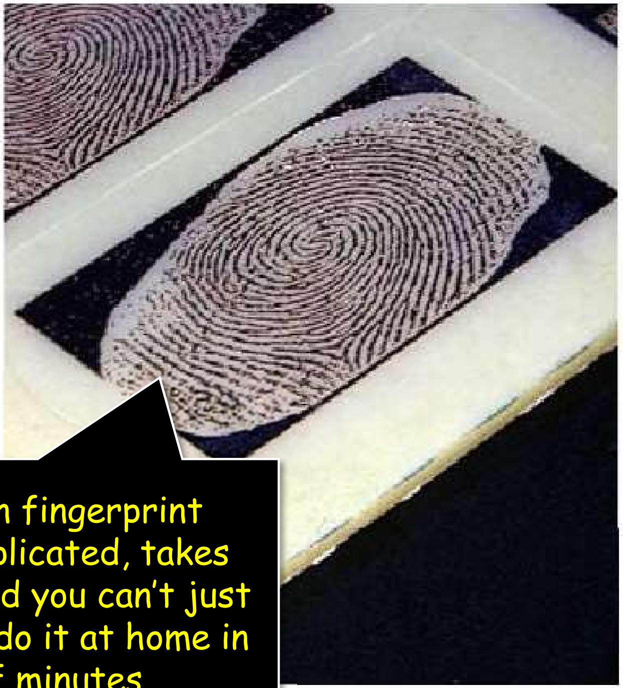
1. SMS message
2. Biometric
3. Token app

Developed in 1975, Signalling System No. 7 (SS7) is a set of telephony signaling protocols used to set up and tear down telephone calls on the world's public switched telephone networks (PSTN).

When SS7 was created, authentication of telephone switches was not necessary – they were on the other end of a piece of copper.

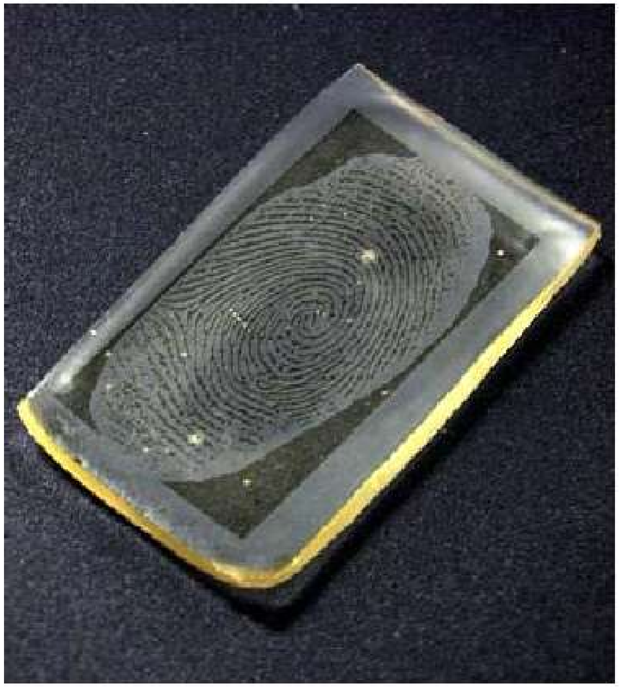
In May 2017, O2 Telefonica, a German mobile service provider, confirmed that cybercriminals had exploited SS7 vulnerabilities to divert 2FA SMS messages and made unauthorized withdrawals from users' bank accounts.

The Mold and the Gummy Finger



Mold: 70JPY/piece
(Ten molds can be obtained
in the PCB.)

This attack on fingerprint readers is complicated, takes time and skill, and you can’t just download it and do it at home in a couple of minutes.

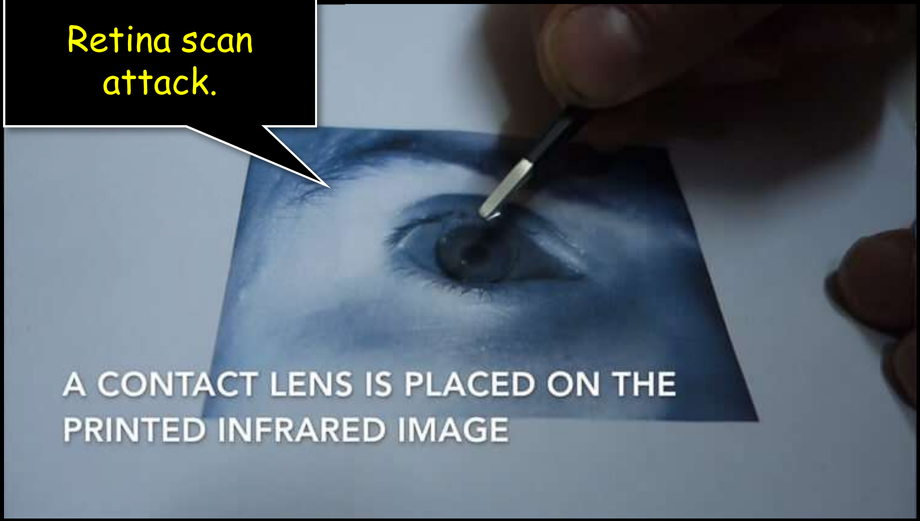


Gummy Finger: 50JPY/piece

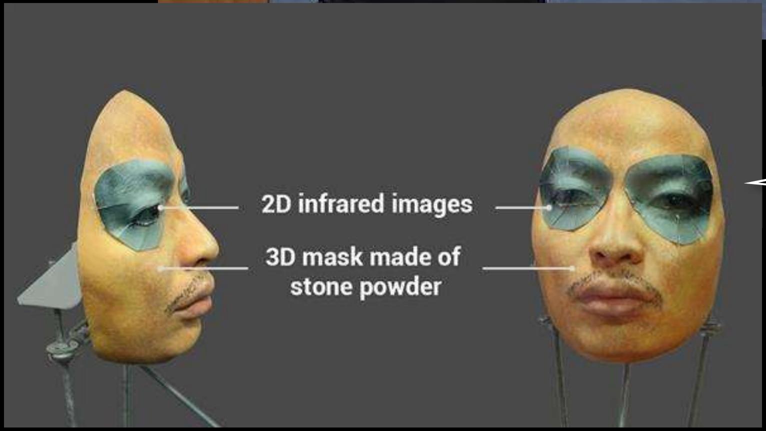
This attack on finger print scanners uses a standard inkjet printer loaded with the conductive ink and paper used to make flexile circuit boards.

“Hacking Mobile Phones Using 2D Printed Fingerprints”
Kai Cao and Anil K. Jain, Department of Computer Science and Engineering, Michigan State University.

Retina scan attack.

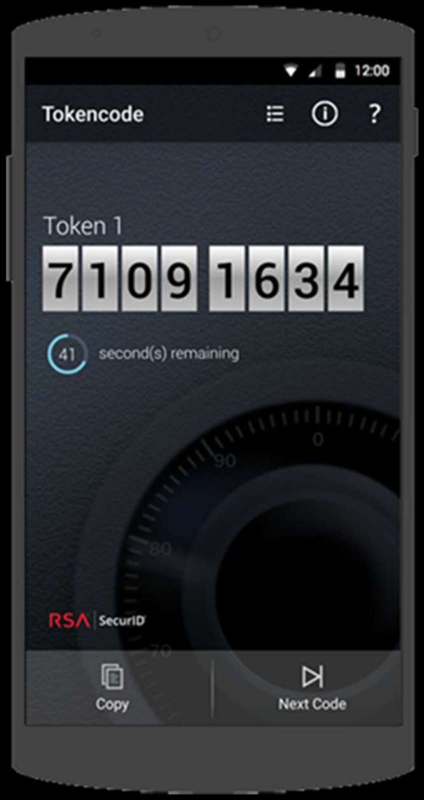


http://ccc.de/de/updates/2017/iriden



Face ID attack.

https://www.theregister.co.uk/2017/11/13/iphone_x_face_id/

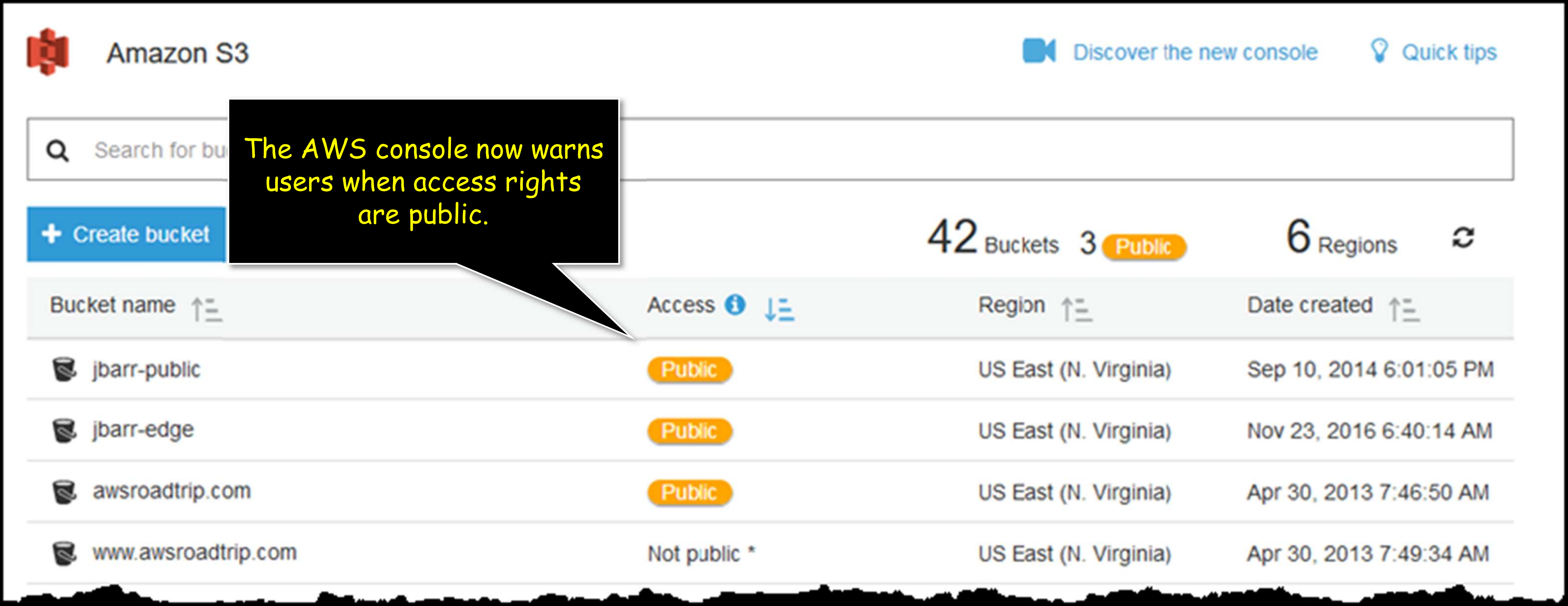


When you lock your phone, you are locking access to your 2FA. How do you do that?

- PIN/Password?
- Swipe pattern?
- Fingerprint?
- Retinal scan?
- Face ID?

CLOUD

What’s the biggest threat to your cloud data?

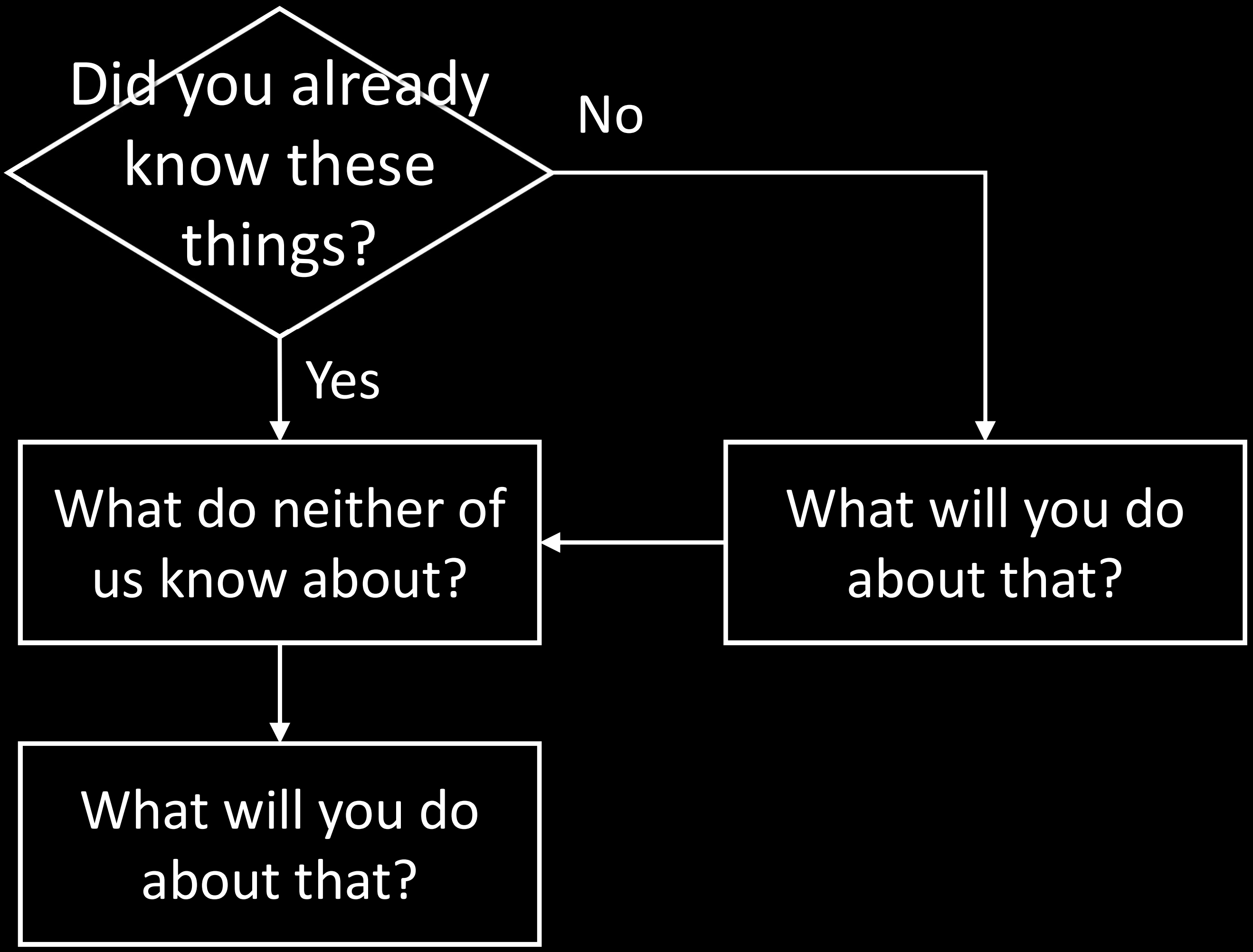


The AWS console now warns users when access rights are public.

Bucket name	Access	Region	Date created
jbarr-public	Public	US East (N. Virginia)	Sep 10, 2014 6:01:05 PM
jbarr-edge	Public	US East (N. Virginia)	Nov 23, 2016 6:40:14 AM
awsroadtrip.com	Public	US East (N. Virginia)	Apr 30, 2013 7:46:50 AM
www.awsroadtrip.com	Not public *	US East (N. Virginia)	Apr 30, 2013 7:49:34 AM

Bad configuration!!

Or variations on that such as publishing your secret keys on Github.
See https://regmedia.co.uk/2017/11/16/whyiwalkedfrom3k.pdf



Did you already know these things?

No

Yes

What do neither of us know about?

What will you do about that?

What will you do about that?

“Those who made the decisions with imperfect knowledge will be judged in hindsight by those with considerably more information at their disposal and time for reflection.”

— Donald Rumsfel Known and Unknown: A Memoir

Remember this quote from Rumsfeld if you are in anyway responsible for the security of a system. It highlights the need to engage and educate top management in security strategy before there is a breach.

Spencer Stephens
https://spencer.media