OSINT, <SOME_PERSON> & <YOUR_COMPANY>

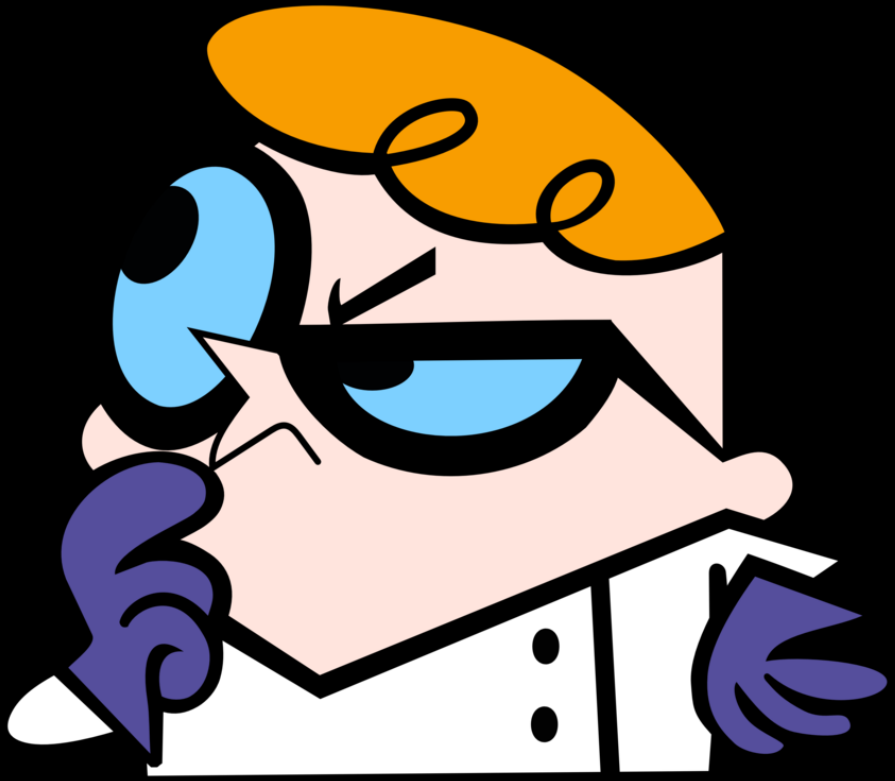
30th August, 2020

#whoami

junior security analyst @work
security researcher @home
musician @weekends
curious
full-time learner
vulnerable, not weak.

AGENDA

- what is OSINT
- why OSINT
- how to OSINT
- scenario
- defend yourself
- real world OSINT
- references
- discussion



DISCLAIMER

All the tools/techniques and procedures being exhibited here, are in no way related to my employer. This is a personal research/interest and pertains to my own findings and external references (if any) and not that of my employer in any way.

The following content is for educational/informative purposes only and is not at all meant to target any individual or any organization. Please do not do anything to anyone without prior consent/authorization.

what is OSINT

gathering info from publicly available sources, legally collection and correlation of information

passive reconnaissance

it’s ~~stalking~~ researching :)

“Information does not have to be secret to be valuable”

- C.I.A.

"Produced from **publicly available information** that is **collected**, **exploited** and **disseminated** in a timely manner to an appropriate audience for the purpose of addressing a **specific intelligence requirement**"

– US Department of Defense & Director of National Intelligence it’s important to know what you’re looking for.

why OSINT

Google

SHODAN

Censys.io

Binaryedge.io

_IntelligenceX

Reddit

Github

Google

SHODAN

Censys.io

Binaryedge.io

_IntelligenceX

Reddit

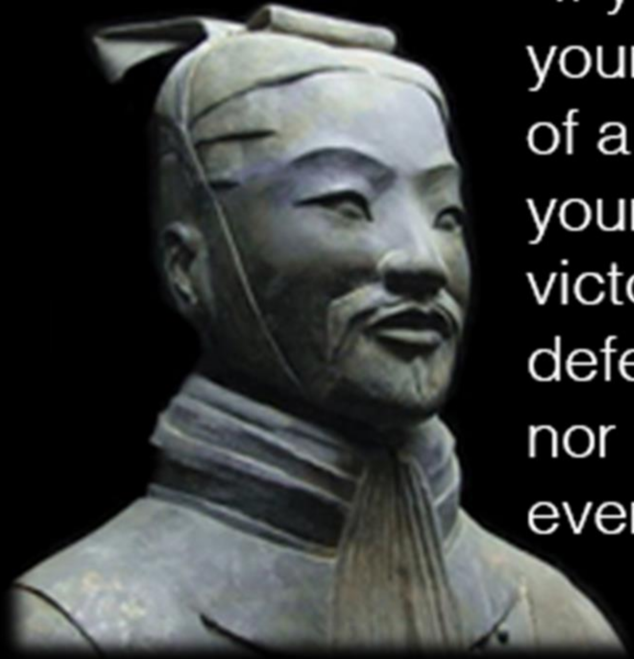
Github

Media – Newspapers, Magazines, Radio, Television

Professional Publications – Journals, Press Conferences

Grey Literature – Technical Reports, Patents, Newsletters

threat actors



"If you know your enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" - Sun Tzu, The Art of War detect/prevent data breaches & leaks

competitive market research

your dashboard might not be enough

map what’s publicly visible

primary attack scenarios

outdated softwares

compromised passwords

using software with known vulnerabilities

security misconfigurations

credential reuse

default credentials

admin:admin

admin:password

root:toor

USERNAME: ADMIN
PASSWORD: ADMIN

logical credentials too

logical credentials too

admin:december2019!

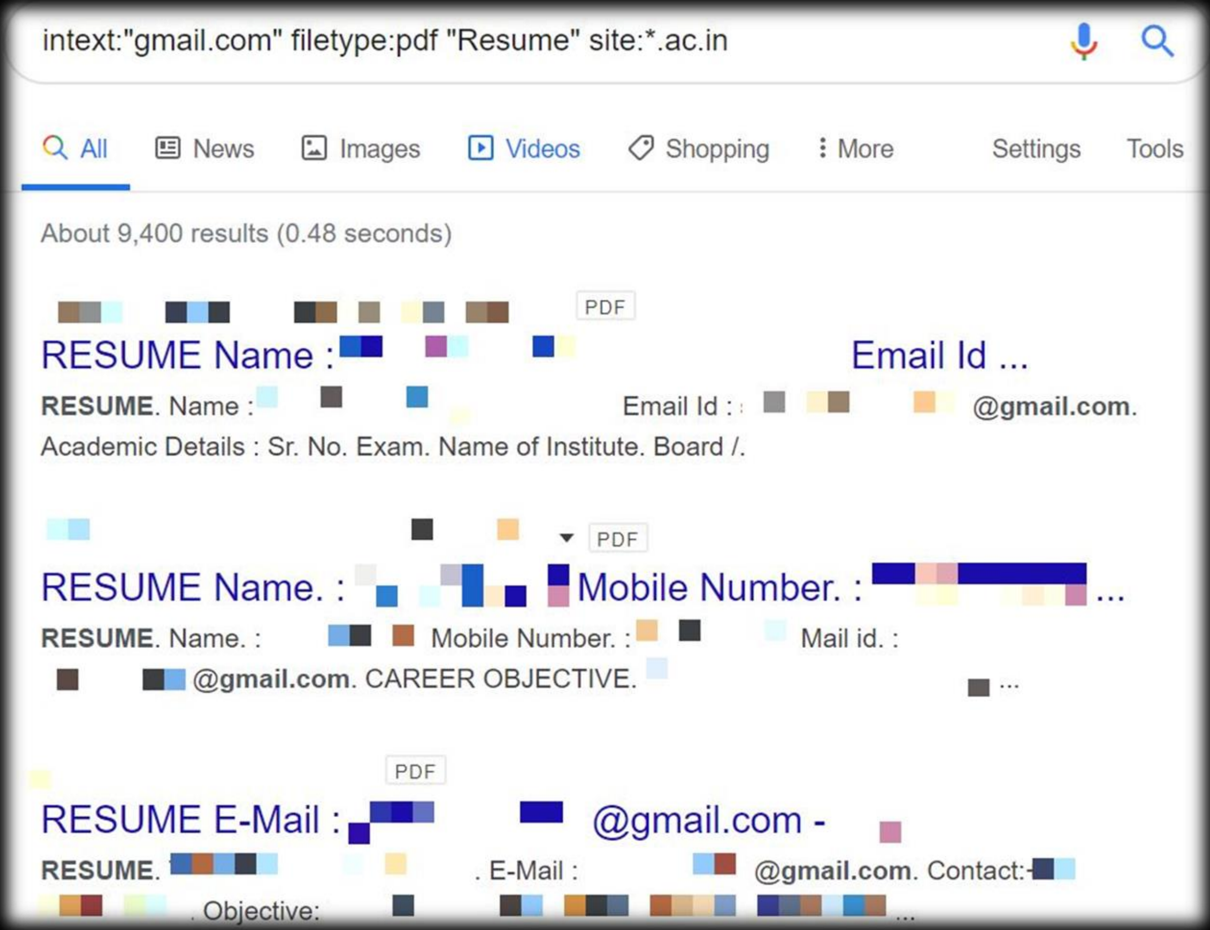
admin:470E50D2FF5998CC95C227CC3240720E!

OSINT TTPs

Google Dorks

- using Google Search for ‘focused’ queries
- query ANYTHING that has been indexed
- dorks are populated on Exploit-DB
- interesting searches can be
  - logs with ‘juicy’ info (eg. MySQL logs)
  - CSV files (eg. Payroll CSVs)
  - login Portals (eg. Admin portals)
  - sensitive directories and files (eg. SSH keys)

- various search operators
  - intext
  - filetype
  - site
  - inurl
  - “content within quotes”
  - regex and wildcards too
  - ext



intext:"gmail.com" filetype:pdf "Resume" site:*.ac.in

About 9,400 results (0.48 seconds)

[redacted] PDF

RESUME Name : [redacted] Email Id ...

RESUME. Name : [redacted] Email Id : [redacted] @gmail.com. Academic Details : Sr. No. Exam. Name of Institute. Board /.

[redacted] PDF

RESUME Name. : [redacted] Mobile Number. : [redacted] ...

RESUME. Name. : [redacted] Mobile Number. : [redacted] Mail id. : [redacted] @gmail.com. CAREER OBJECTIVE. [redacted] ...

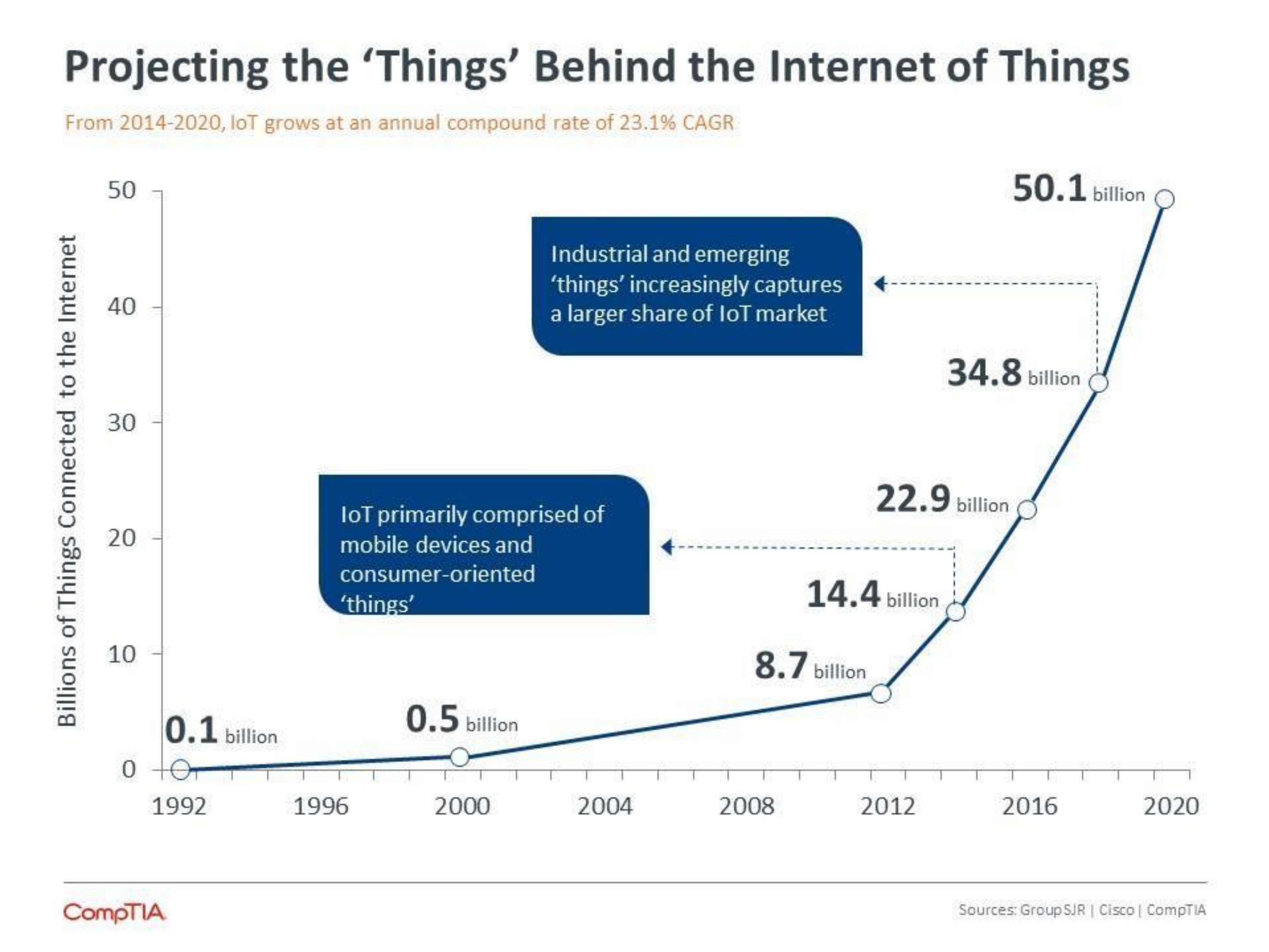
[redacted] PDF

RESUME E-Mail : [redacted] @gmail.com - [redacted]

RESUME. [redacted] . E-Mail : [redacted] @gmail.com. Contact:-[redacted] . Objective: [redacted] ...

Github Dorks

- using Github Search for ‘focused’ queries
- query ANYTHING that has been indexed
- interesting searches can be
  - logs with ‘juicy’ info
  - SSH Keys, API Keys
  - Hidden Endpoints/Documentation
  - Public Commit History
  - Hardcoded Credentials



Projecting the 'Things' Behind the Internet of Things

From 2014-2020, IoT grows at an annual compound rate of 23.1% CAGR

Industrial and emerging 'things' increasingly captures a larger share of IoT market

IoT primarily comprised of mobile devices and consumer-oriented 'things'

CompTIA

Sources: Group SJR | Cisco | CompTIA

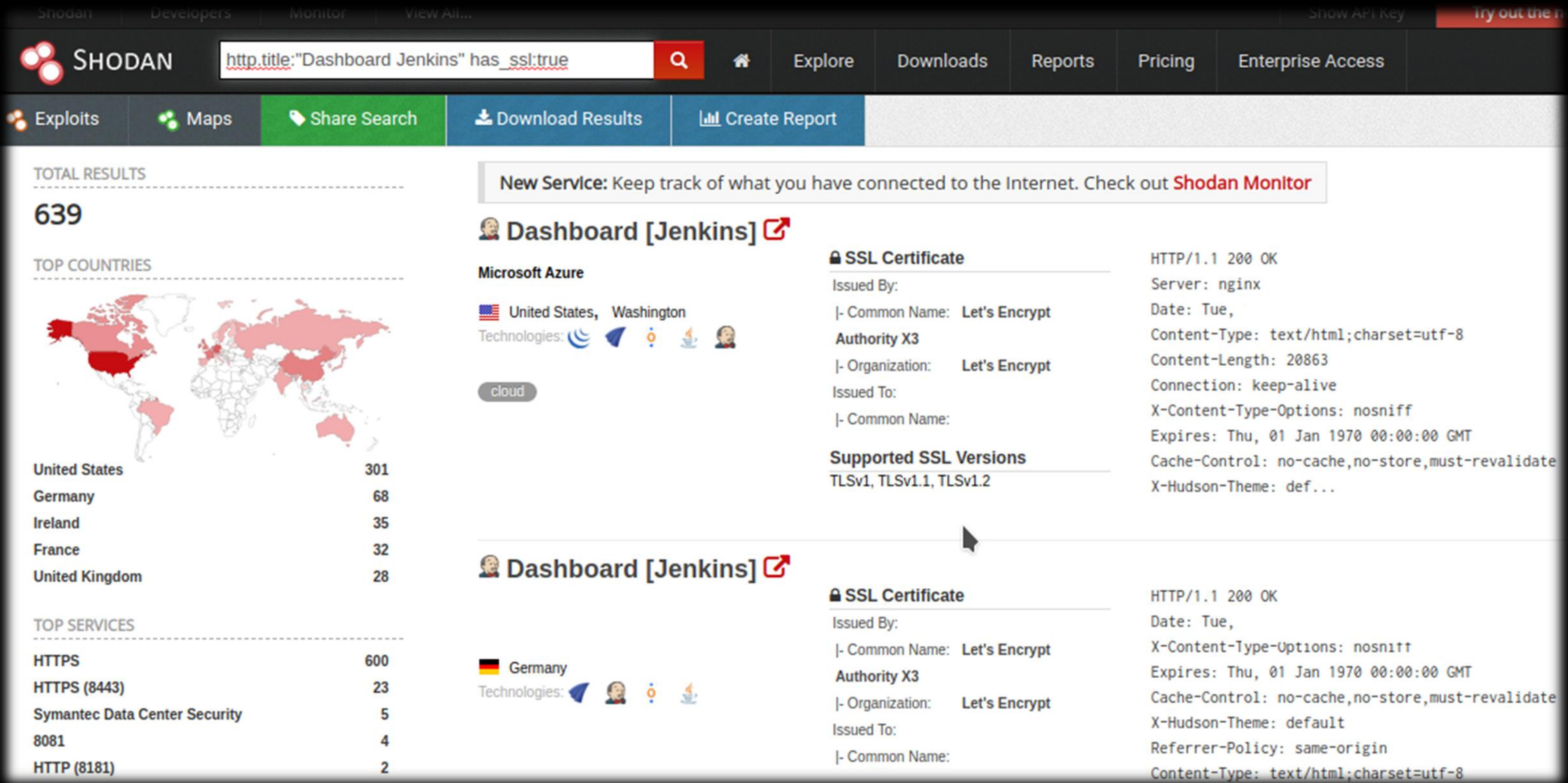
SHODAN

I saw something that allowed you to change the flow of water through a city. It was basically opening and closing the ports that control the dam structure. It was wide open. – Daniel Miessler

SHODAN

- passive recon technique for the IoT
- "…scariest search engine of the world" – CNN
- one can look up:
  - SCADA & ICS (Nuclear Powerplants, Petrol pumps..)
  - remote desktops and Application Layer Tech (ssh,smtp,ftp..)
  - network devices (routers, switches, webcams..)
  - cloud instances (SonarQube, Jenkins, Kibana, MongoDB..)

anything with an IP address, connected to the internet anything with an IP address, connected to the internet



http.title:"Dashboard Jenkins" has_ssl:true

TOTAL RESULTS

639

TOP COUNTRIES

United States	301
Germany	68
Ireland	35
France	32
United Kingdom	28

TOP SERVICES

HTTPS	600
HTTPS (8443)	23
Symantec Data Center Security	5
8081	4
HTTP (8181)	2

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Dashboard [Jenkins]

Microsoft Azure

United States, Washington

Technologies:

cloud

SSL Certificate

Issued By:
|- Common Name: **Let's Encrypt Authority X3**
|- Organization: **Let's Encrypt**
Issued To:
|- Common Name:

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue,
Content-Type: text/html;charset=utf-8
Content-Length: 20863
Connection: keep-alive
X-Content-Type-Options: nosniff
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: def...
```

Dashboard [Jenkins]

Germany

Technologies:

SSL Certificate

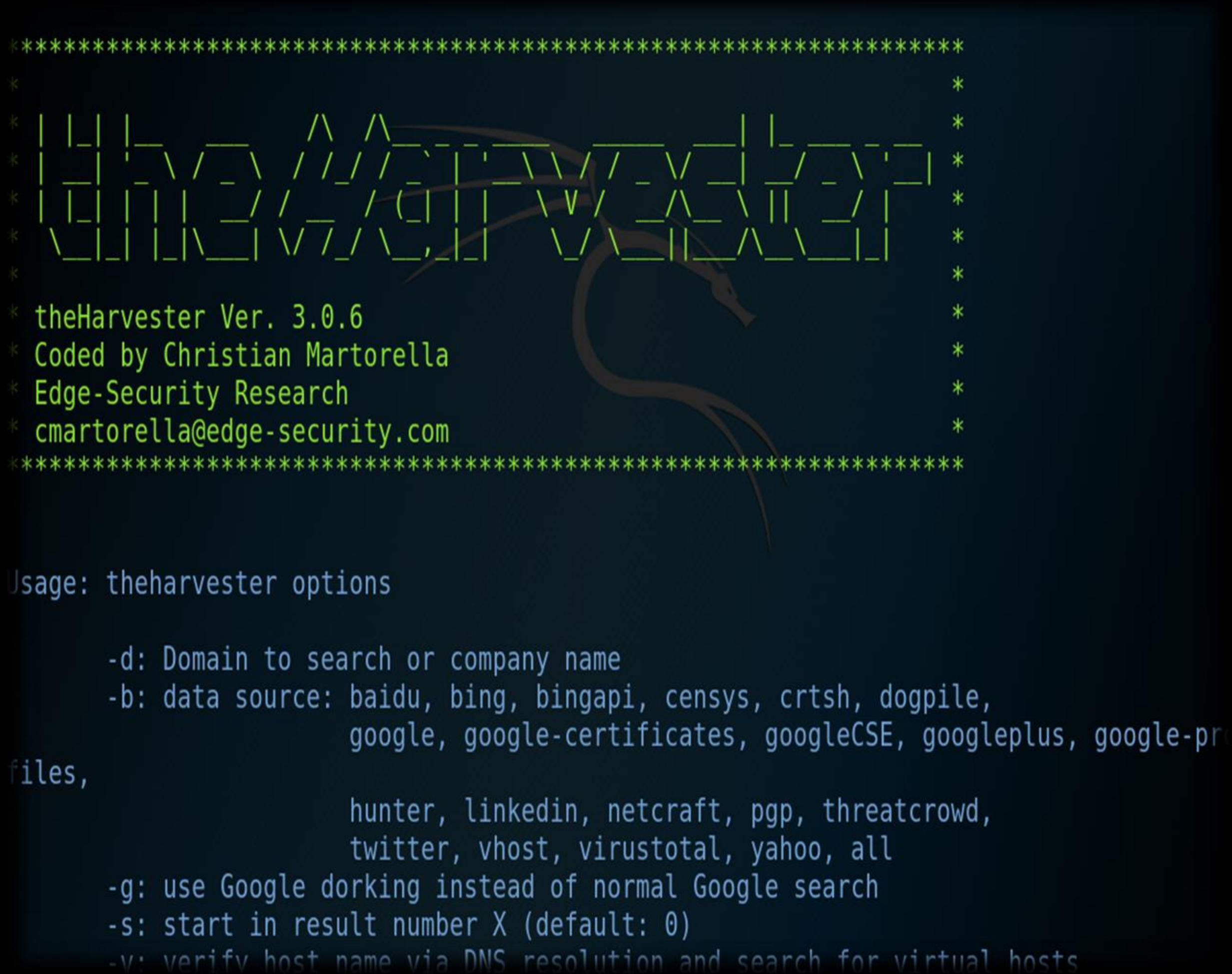
Issued By:
|- Common Name: **Let's Encrypt Authority X3**
|- Organization: **Let's Encrypt**
Issued To:
|- Common Name:

```
HTTP/1.1 200 OK
Date: Tue,
X-Content-Type-Options: nosniff
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: default
Referrer-Policy: same-origin
Content-Type: text/html;charset=utf-8
```

if you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees. – Kahlil Gibran

theHarvester

- gather emails, subdomains, hosts, open ports, banner
- different public sources like
  - Google
  - Bing
  - Yahoo
  - LinkedIn
  - Baidu
  - Twitter
  - Virustotal
- open source and API integration available

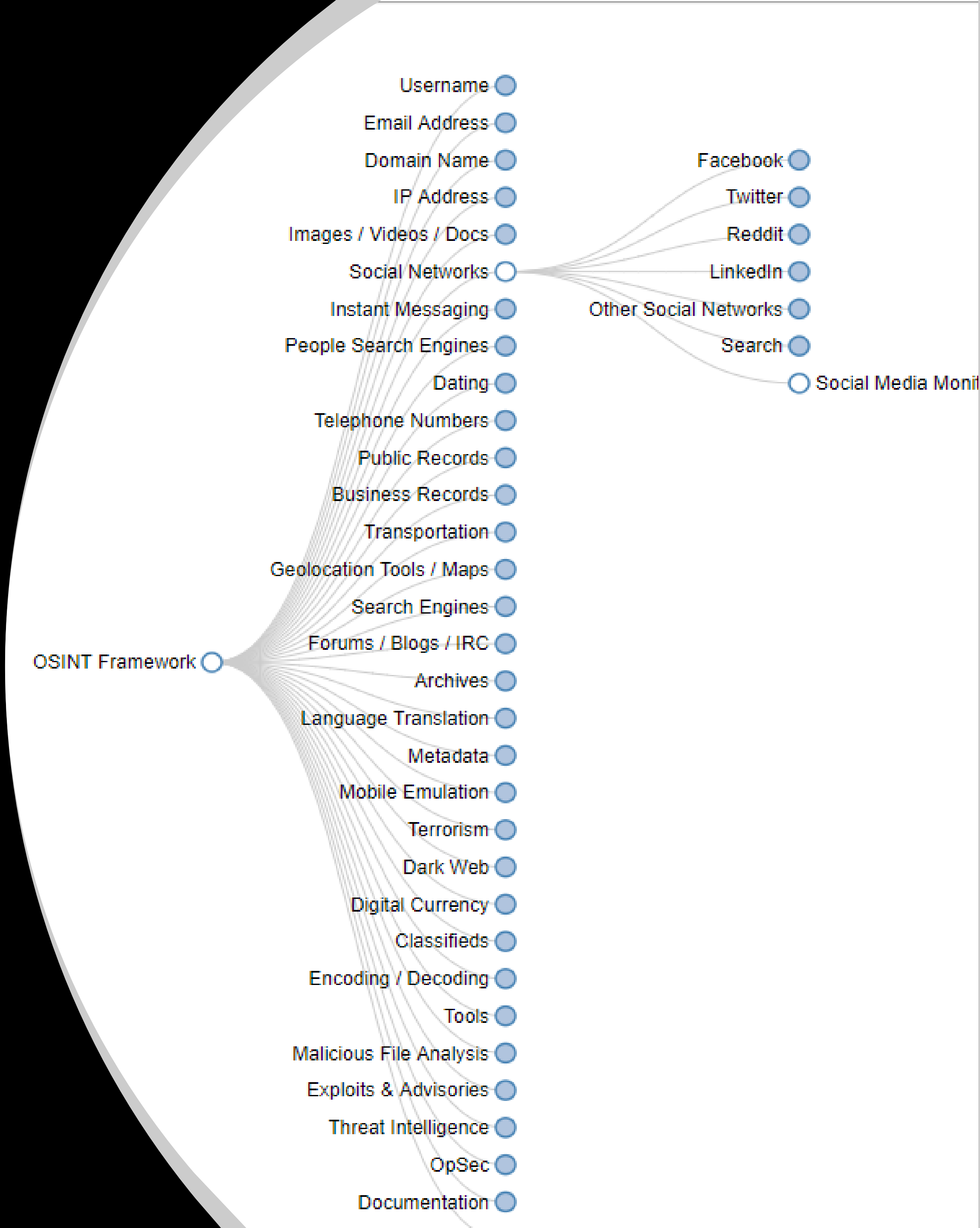


```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester Ver. 3.0.6                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
                        google, google-certificates, googleCSE, googleplus, google-pr
files,
                        hunter, linkedin, netcraft, pgp, threatcrowd,
                        twitter, vhost, virustotal, yahoo, all
       -g: use Google dorking instead of normal Google search
       -s: start in result number X (default: 0)
       -v: verify host name via DNS resolution and search for virtual hosts
```

OSINT Framework by Justin Nordine @jnordine



fictional accounts

sock puppets for OSINT research

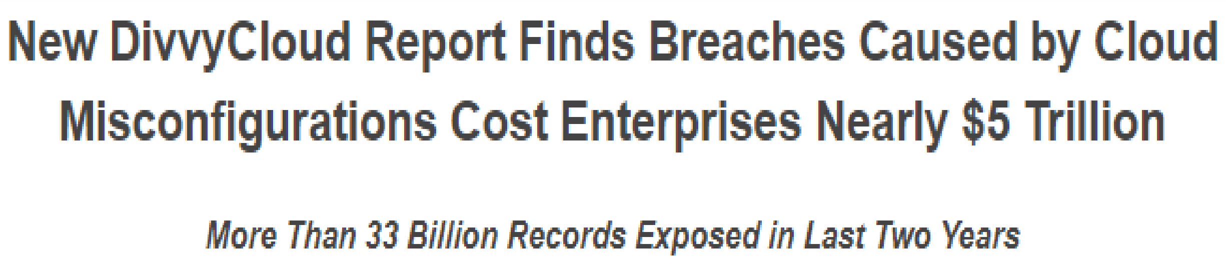
- This Person Does Not Exist
- This Resume Does Not Exist
- This Rental Does Not Exist
- Fake Name Generator
- Random User
- Uinames
- UK Name Generator
- Random Word Generator
- Elfqrin Fake ID
- Behind the Name
- Else Where

scenario

“Source code of critical applications of company ‘X’ along with the database of around ‘x’ million users was dumped onto the Darkweb. The hacker claims to have exploited a misconfigured AWS S3 Bucket”.

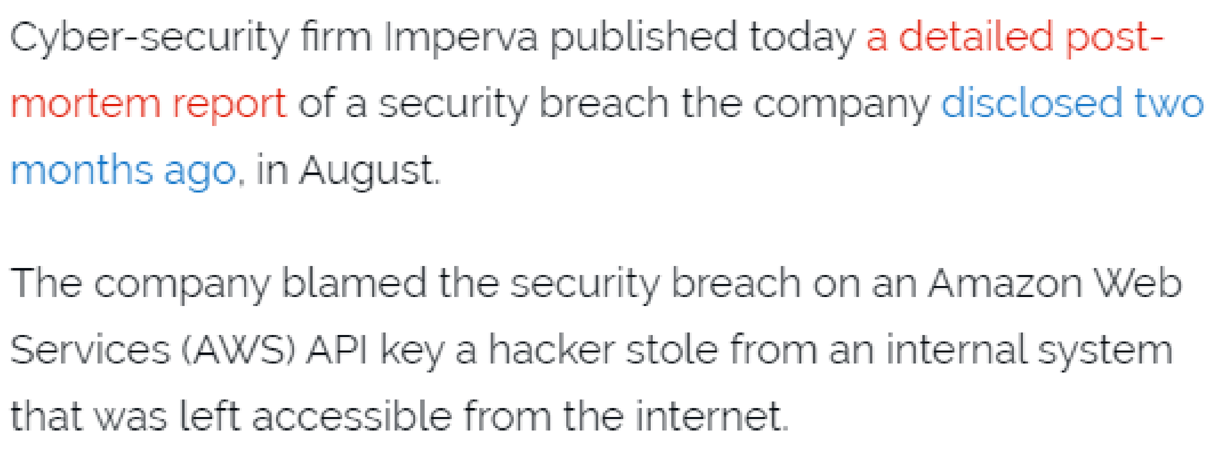
source code

customer data



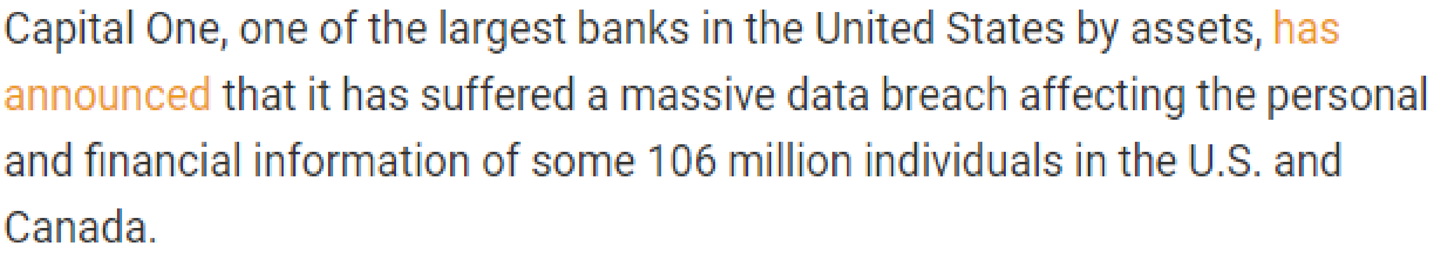
New DivvyCloud Report Finds Breaches Caused by Cloud Misconfigurations Cost Enterprises Nearly $5 Trillion

More Than 33 Billion Records Exposed in Last Two Years

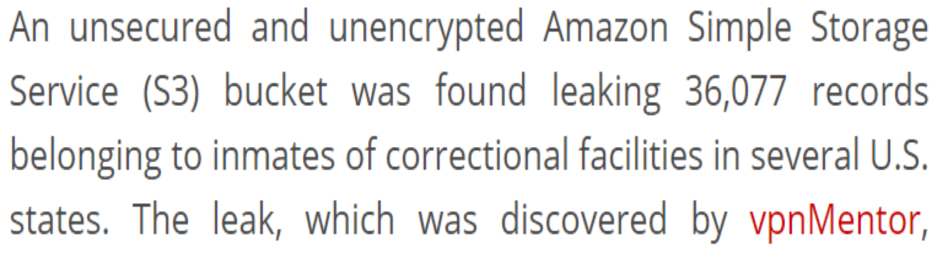


Cyber-security firm Imperva published today a detailed post-mortem report of a security breach the company disclosed two months ago, in August.

The company blamed the security breach on an Amazon Web Services (AWS) API key a hacker stole from an internal system that was left accessible from the internet.



Capital One, one of the largest banks in the United States by assets, has announced that it has suffered a massive data breach affecting the personal and financial information of some 106 million individuals in the U.S. and Canada.



An unsecured and unencrypted Amazon Simple Storage Service (S3) bucket was found leaking 36,077 records belonging to inmates of correctional facilities in several U.S. states. The leak, which was discovered by vpnMentor,

There is no cloud
it's just someone else's computer

defend yourself

try to hack into yourself

don’t publish information that makes you vulnerable follow CERTs and CISA Advisories

keep a security.txt in place

create a threat model

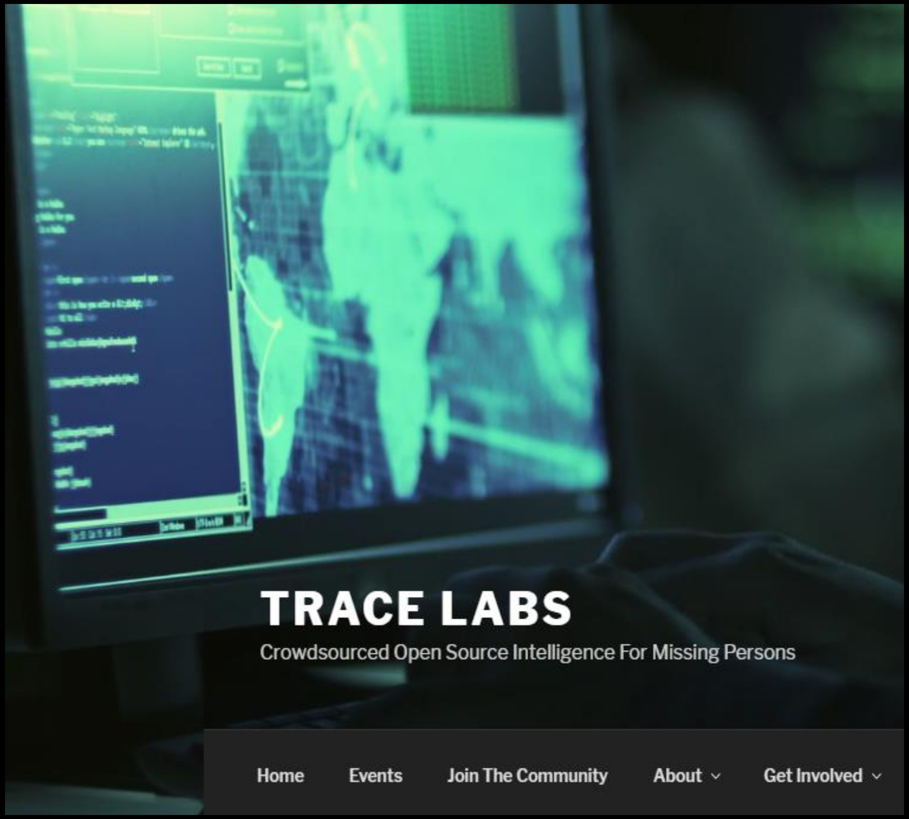
separate dev and prod environments

read/think/analyze before you click

1-click is all they need

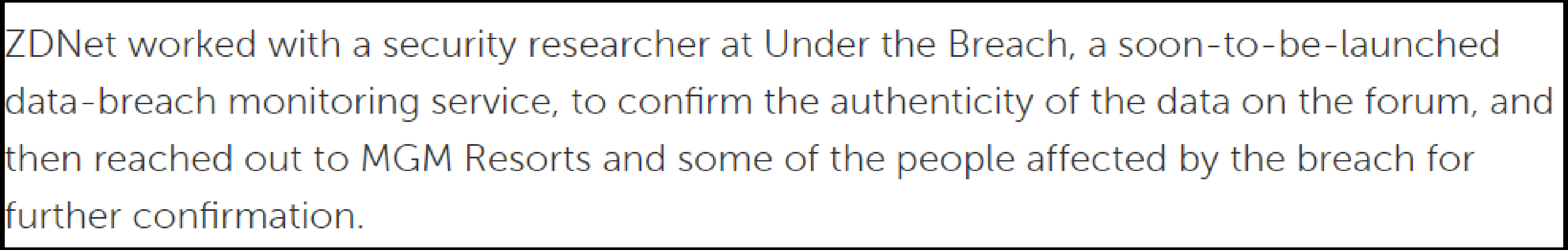
real world OSINT

Tracelabs, an OSINT based startup conducts CTFs on missing people

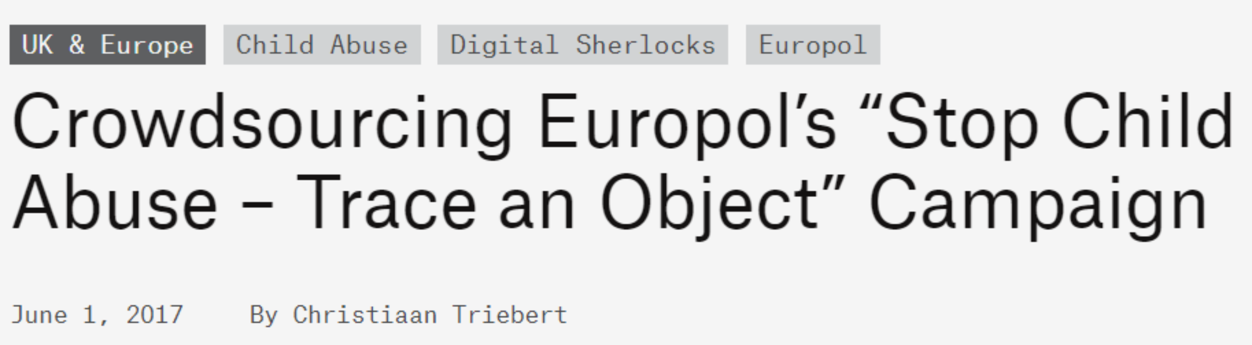


Security Researcher providing Cybercrime investigations and updates. www.underthebreach.com

Under The Breach



ZDNet worked with a security researcher at Under the Breach, a soon-to-be-launched data-breach monitoring service, to confirm the authenticity of the data on the forum, and then reached out to MGM Resorts and some of the people affected by the breach for further confirmation.

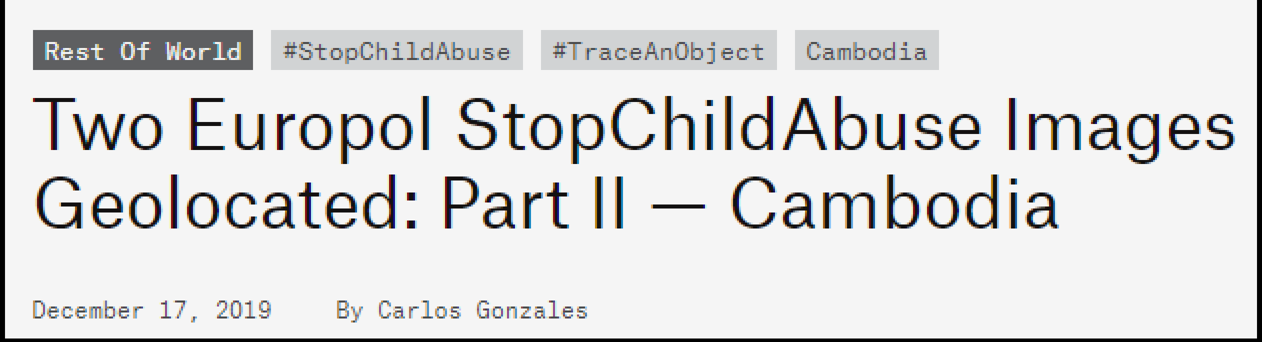

UK & Europe Child Abuse Digital Sherlocks Europol

Crowdsourcing Europol's "Stop Child Abuse – Trace an Object" Campaign

June 1, 2017 By Christiaan Triebert

Investigative journalism website that specializes in fact-checking and open-source intelligence

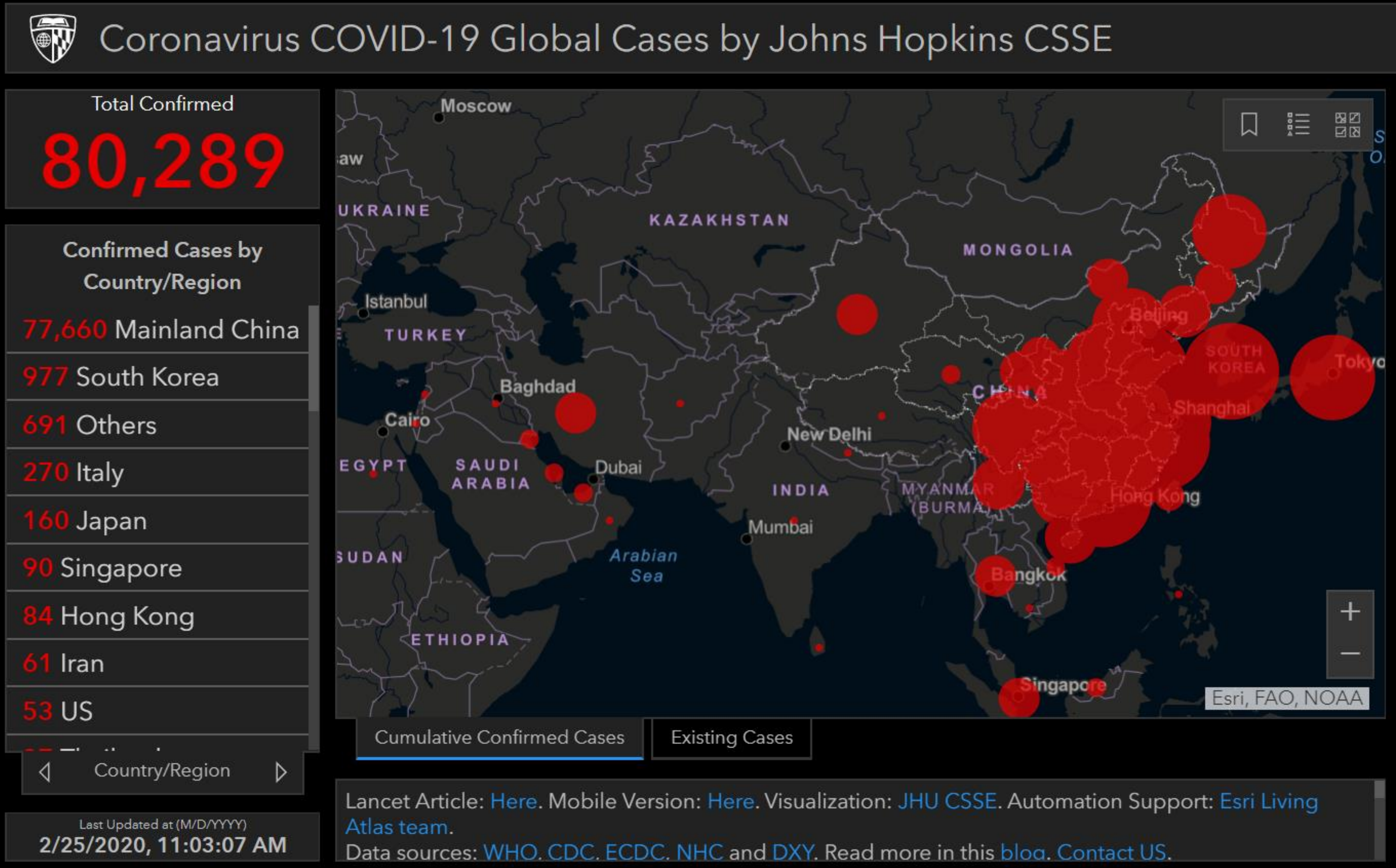
bell¿ngcat


Rest Of World #StopChildAbuse #TraceAnObject Cambodia

Two Europol StopChildAbuse Images Geolocated: Part II — Cambodia

December 17, 2019 By Carlos Gonzales

Tracking Coronavirus using OSINT



Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed

80,289

Confirmed Cases by Country/Region

77,660	Mainland China
977	South Korea
691	Others
270	Italy
160	Japan
90	Singapore
84	Hong Kong
61	Iran
53	US

Country/Region

Last Updated at (M/D/YYYY)

2/25/2020, 11:03:07 AM

Cumulative Confirmed Cases | Existing Cases

Lancet Article: Here. Mobile Version: Here. Visualization: JHU CSSE. Automation Support: Esri Living Atlas team.
Data sources: WHO, CDC, ECDC, NHC and DXY. Read more in this blog. Contact US.

references

https://www.flaticon.com/authors/freepik
https://www.flaticon.com/authors/pixel-perfect
https://osintframework.com
https://archive.org
https://osint.link/
https://github.com/jakejarvis/awesome-shodan-queries
https://osintframework.com/
https://osint.best/
https://osintcurio.us/
https://github.com/jivoi/awesome-osint
https://sherlock-project.github.io
https://www.osinttechniques.com/

discussions