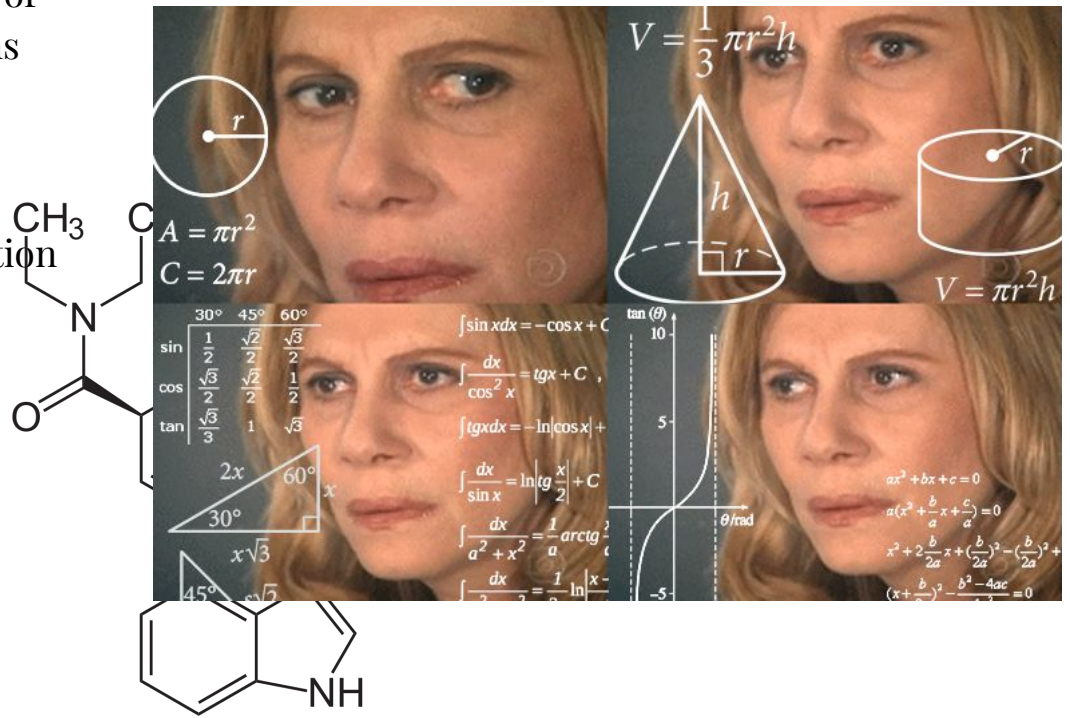
One Framework to Rule Them All

A framework for Internet-connected Device Census

The Main Searching Problems

1. How to combine all possible variations of different queries from different systems in one place?
2. How to find vulnerabilities and active services on founded hosts?
3. How to get all actual statistics information about founded results?



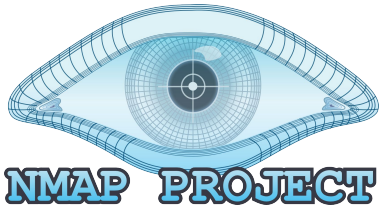

Pain and suffering

Grinder Framework was created to resolve all these problems automatically just in one touch!

~~Turn Down~~ for What?

One Framework to rule them all, One Framework to find them,
One Framework to bring them all and in the darkness bind them

Grinder Modules




IT'S MAGIC!
1. bash
usage: grinder.py [-h] [-r] [-u] [-q QUERIES_FILE] [-sk SHODAN_KEY] [-cu]
[-cp] [-ci CENSYS_ID] [-cs CENSYS_SECRET] [-cm CENSYS_MAX]
[-nm] [-nw NMAP_WORKERS] [-vs] [-vw VULNERS_WORKERS]
[-c CONFIDENCE] [-v [VENDORS [VENDORS ...]]] [-ml MAX_LIMIT]
The Grinder framework was created to automatically enumerate and fingerprint
different hosts on the Internet using different back-end systems
optional arguments:
-h, --help show this help message and exit
-r, --run Run scanning
-u, --update-markers Update map markers
-q QUERIES_FILE, --queries-file QUERIES_FILE
JSON File with Shodan queries
-sk SHODAN_KEY, --shodan-key SHODAN_KEY
Shodan API key
-cu, --count-unique Count unique entities
-cp, --create-plots Create graphic plots
-ci CENSYS_ID, --censys-id CENSYS_ID
Censys API ID key
-cs CENSYS_SECRET, --censys-secret CENSYS_SECRET
Censys API SECRET key
-cm CENSYS_MAX, --censys-max CENSYS_MAX
Censys default maximum results quantity
-nm, --nmap-scan Initiate Nmap scanning
-nw NMAP_WORKERS, --nmap-workers NMAP_WORKERS
Number of Nmap workers to scan
-vs, --vulners-scan Initiate Vulners API scanning
-vw VULNERS_WORKERS, --vulners-workers VULNERS_WORKERS
Number of Vulners workers to scan
-c CONFIDENCE, --confidence CONFIDENCE
Set confidence level
-v [VENDORS [VENDORS ...]], --vendors [VENDORS [VENDORS ...]]
Set list of vendors to search from queries file
-ml MAX_LIMIT, --max-limit MAX_LIMIT
Maximum number of unique entities in plots and results

Grinder Features

1. Search through different back-end systems such as Shodan, Censys
2. Search information about vulnerabilities from Shodan database
3. NMAP host scan, version and services detection
4. Vulners API vulnerability scan
5. Custom LUA and Python scripts support

Grinder Workflow

QUERIES

PASSIVE SCANNING

Find products in Censys, Shodan

RAW HOSTS FROM ENGINES

ACTIVE SCANNING

Use NMAP and Vulners to find versions, services and vulnerabilities

PROCESSED HOSTS

ADDITIONAL CHECKS

Custom LUA and Python scripts scanning

HOSTS WITH FULL INFORMATION

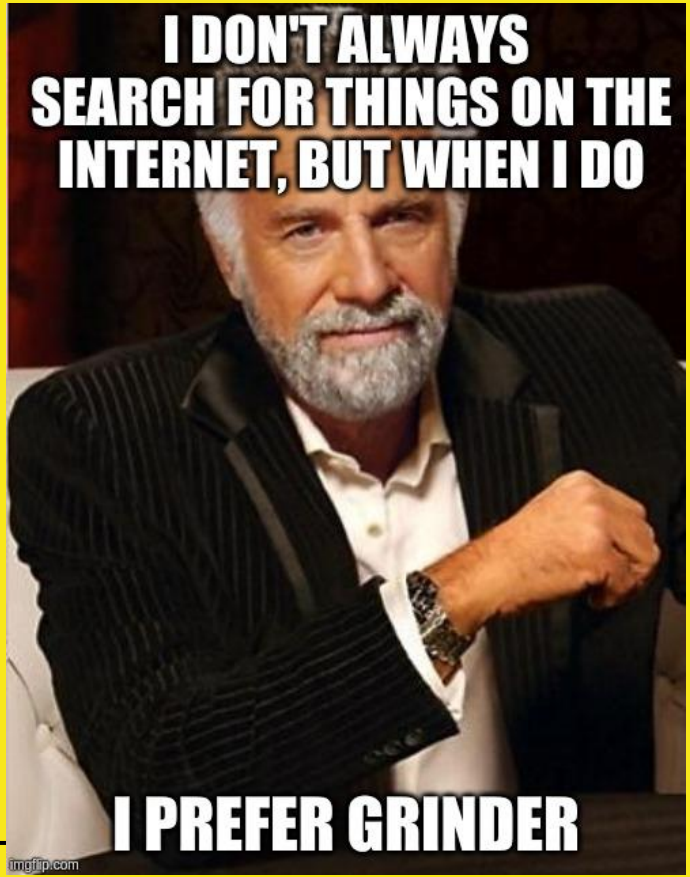
GENERATING REPORTS

Plots, JSONs, CSVs, statis

RESULTS

Grinder Framework Usage Examples

Or how to search for everything and everywhere 🔎



SD-WAN New Hope

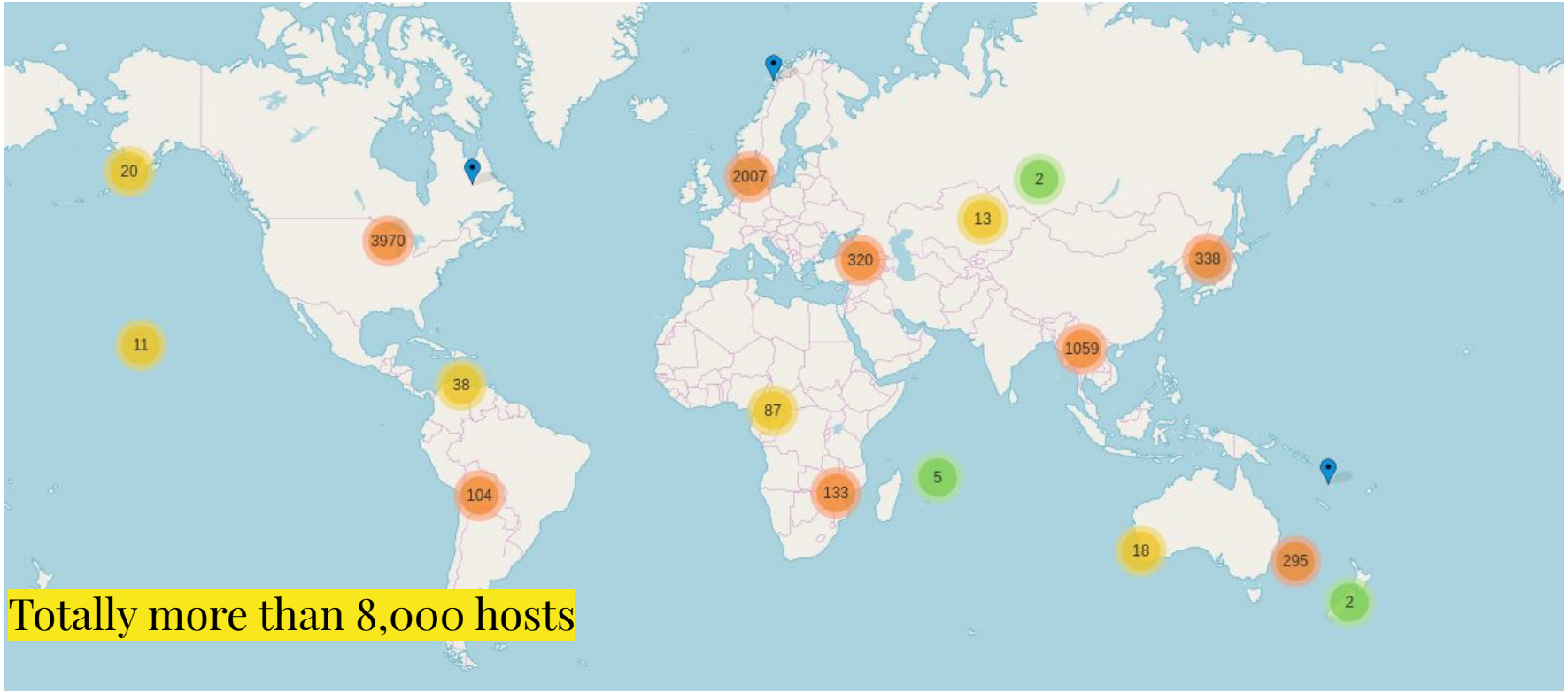
SD-WAN New Hope

github.com/sdnewhop

SDWAN NewHope

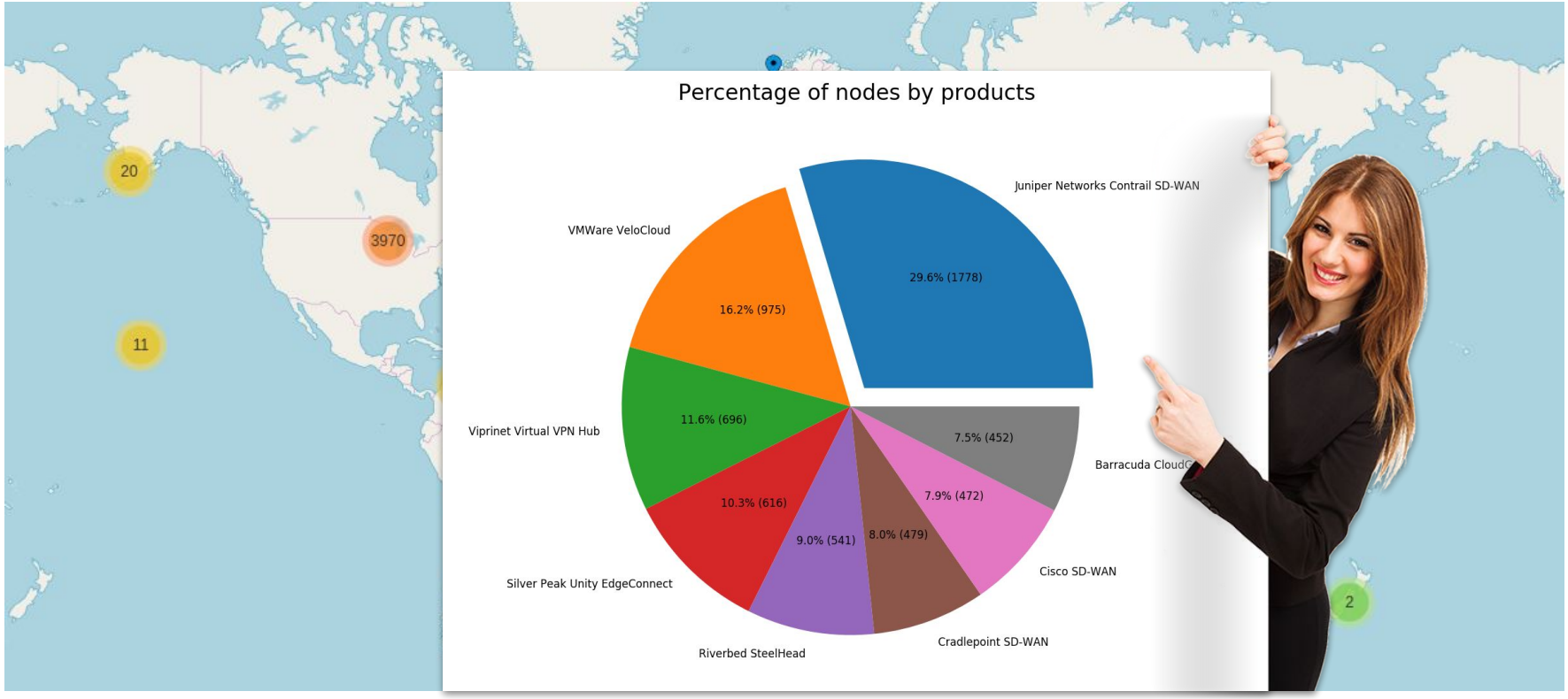
Software-defined networking in a wide area network (SD-WAN) quickly becomes very popular in Enterprise rs promises "on-the-fly agility, simplicity, security and automation" and many other benefits. What do you know D-WAN? What the "security" means from hand-on perspective? Are present SD-WAN solutions really secure? is to give answers on these questions by analysing different real SD-WAN solutions from the adver

SD-WAN New Hope Results

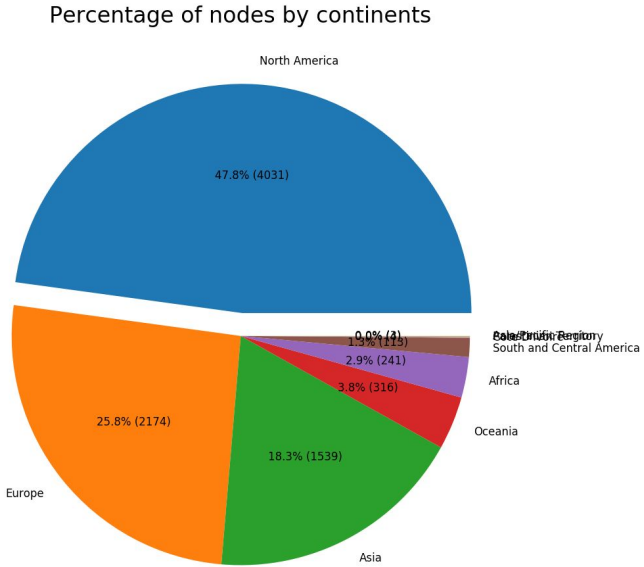


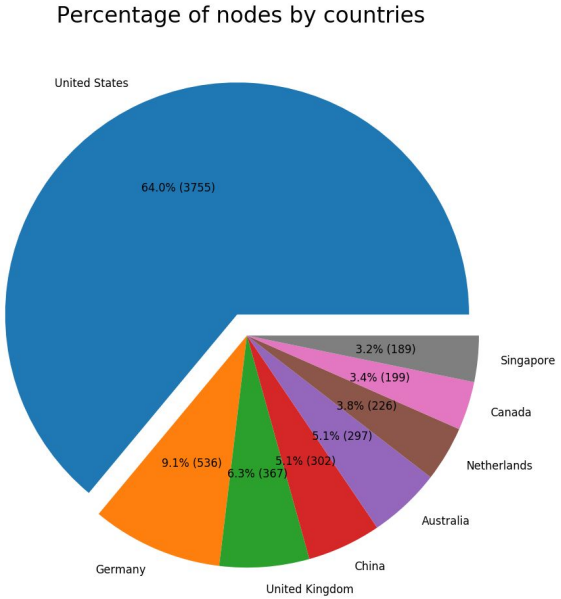
Totally more than 8,000 hosts

SD-WAN New Hope Results



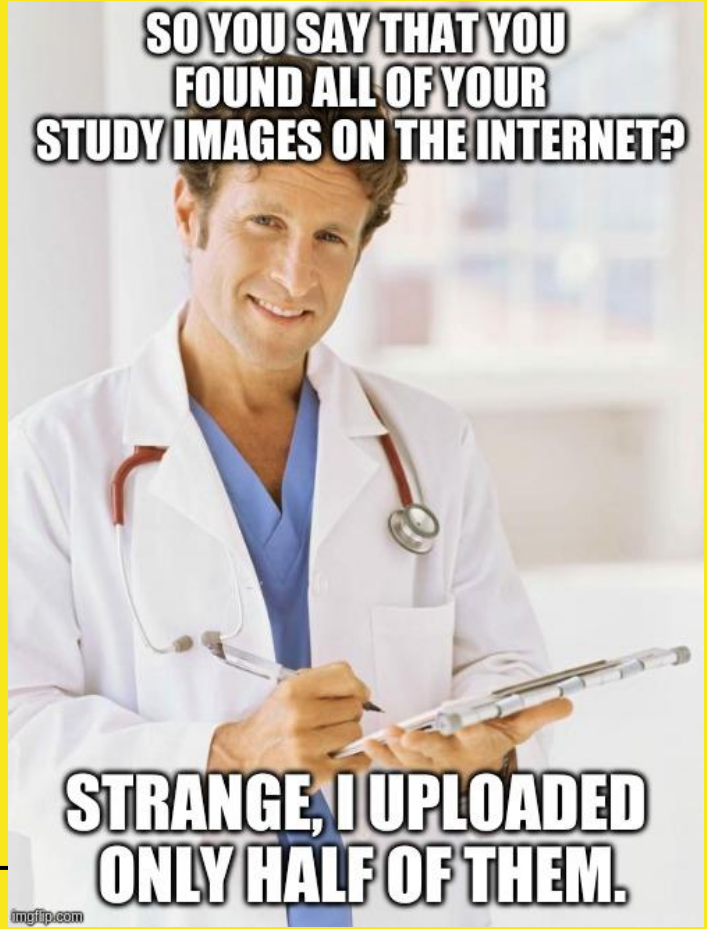
SD-WAN New Hope Results





Medicine

🎵 *“Somebody mixed my medicine”* and not only them



Dr. Jekyll and Mr. Shodan

Rules/Procedure for accessing the server (a full conformance statement will be written some day!):

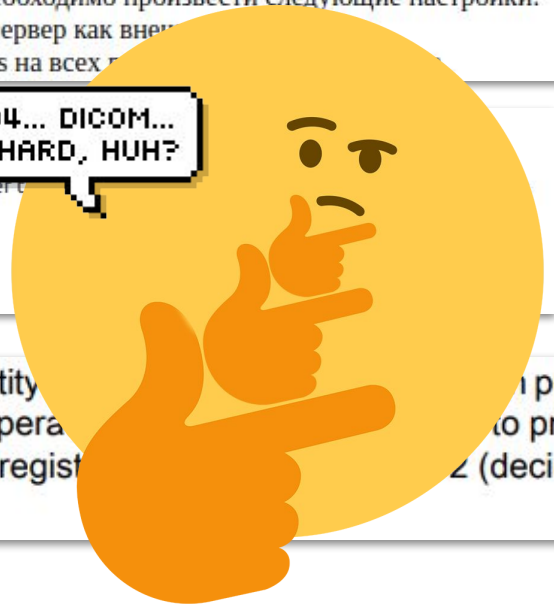
- Server is at www.dicomserver.co.uk
- **Ports are 104 and 11112**

На рабочих станциях с приборами DICOM необходимо произвести следующие настройки:
1) зарегистрировать МЕДИАЛОГ DICOM-сервер как вне
2) открыть порт 104 в Брандмауэре Windows на всех

Parameters of a DICOM server

Historically, the DICOM protocol was designed to work over point-to-point links. Nowadays, the DICOM protocol is used over
be identified by specifying the parameters of its network socket:

1. Its **IP address** (or, equivalently, its symbolic DNS hostname).
2. Its **TCP port** (the standard DICOM port is 104, but Orthanc uses the non-priviliged port 4242 by default).



It is strongly recommended that systems supporting a single DICOM UL entity
port" regis
for the DICOM Upper Layer Protocol: port number 104 (decimal), if the opera
o privileged
(in the range 0 to 1023), otherwise it is recommended that they use the "regist
(decimal). Se
tp://www.iana.org/assignments/port-numbers".

Let’s help Dr. Cox to find all DICOM servers

And maybe something else?

104
tcp
dicom

DICOM Server Response

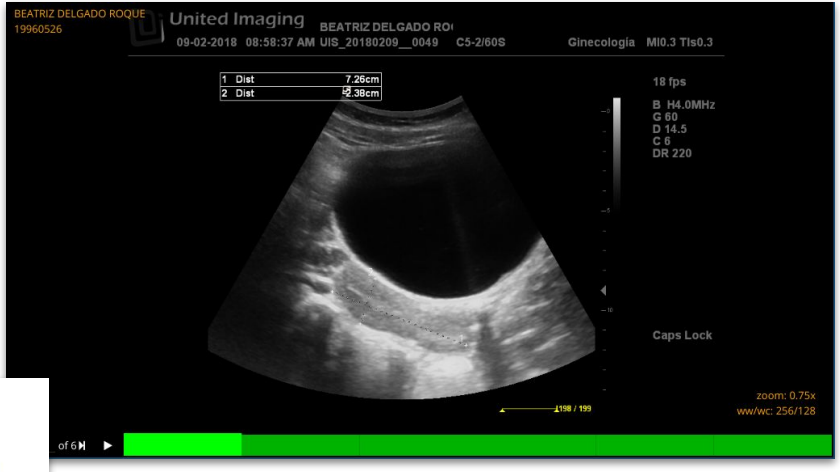
```
\x02\x00\x00\x00\x00\xab\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x0
1\x00\x00\x00@\x00\x00\x111.2.840.10008.1.2P\x00\x00-Q\x00\x00\x04\x00\x00\xfd\xe8R\x
00\x00\x121.2.840.113845.1.1U\x00\x00\x0bSyn4,4,1,11
```

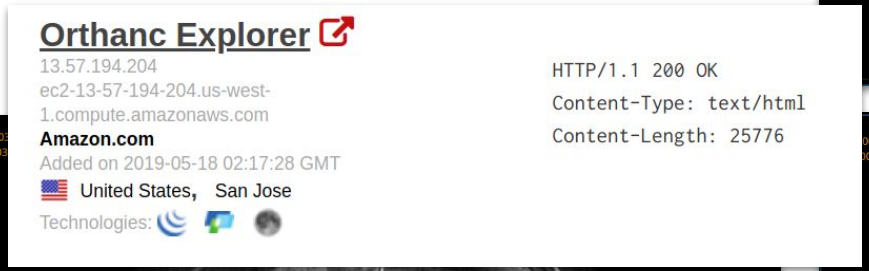
DICOM Results

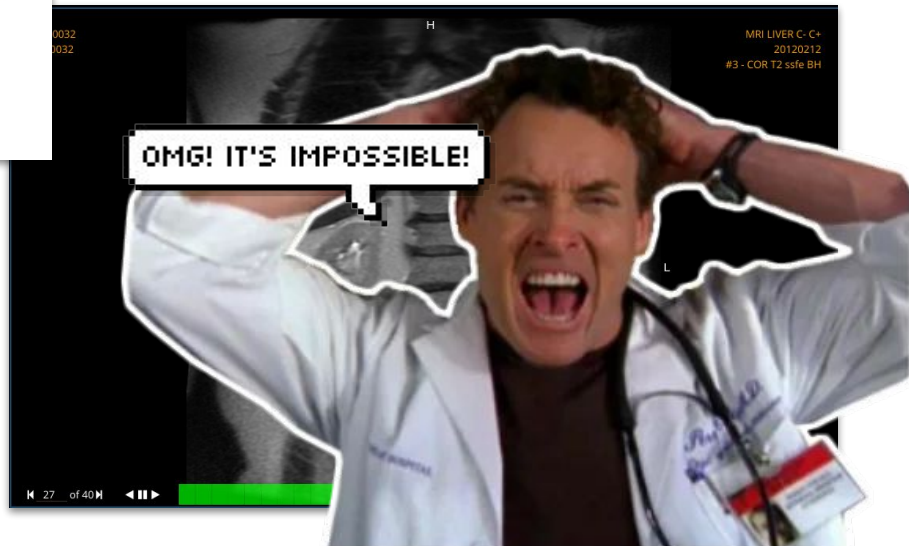
More than 1,700 results

In addition

You can also find patient data like studies, personal information, etc.

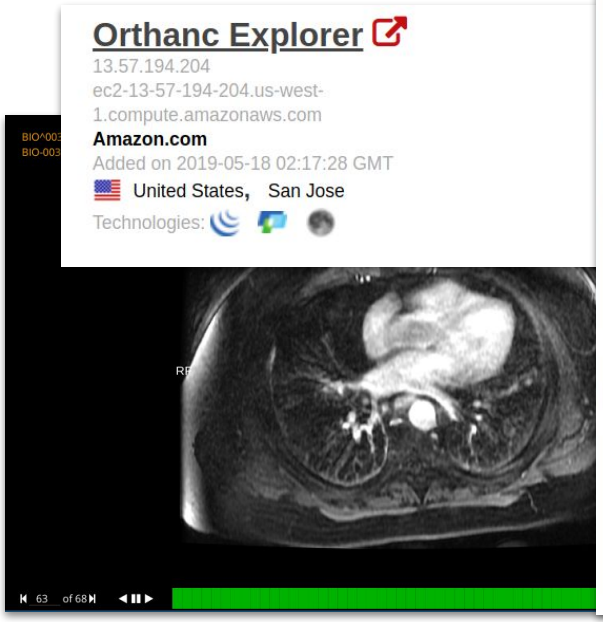




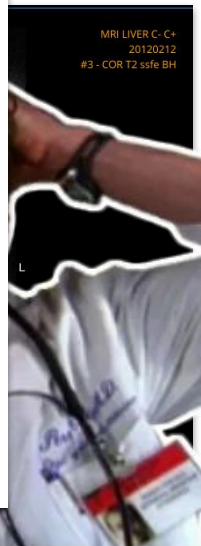


In addition

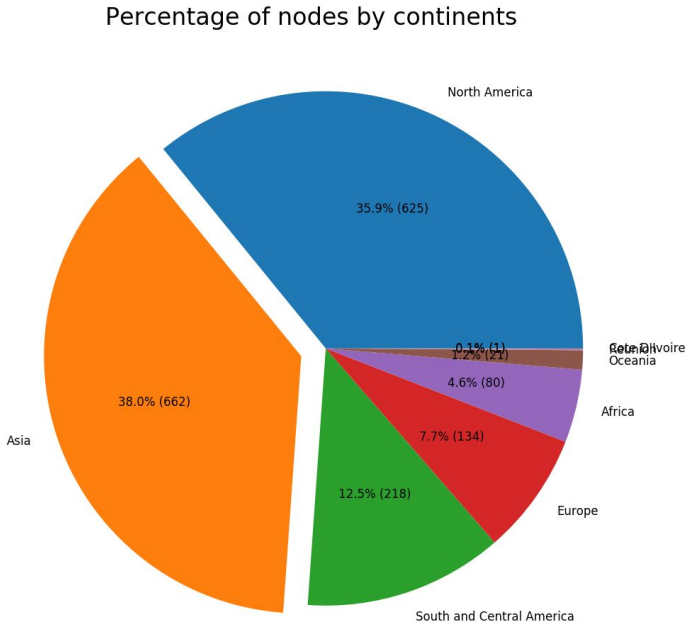
You can also find patient data like studie
personal information, etc.

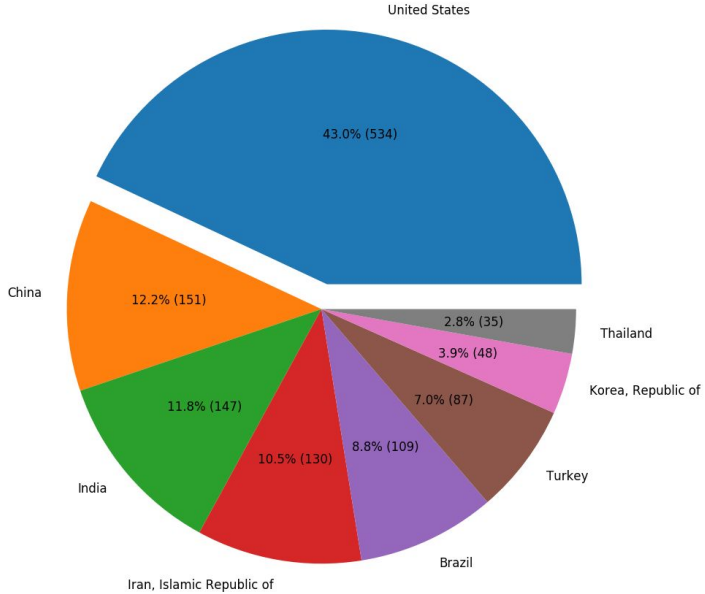



```
(nnnn,0000) BD S Group Length           # of bytes in group nnnn
(nnnn,4000) AT M Comments

(0008,0010) AT S Recognition Code       # ACR-NEMA 1.0 or 2.0
(0008,0020) AT S Study Date             # yyyy.mm.dd
(0008,0021) AT S Series Date            # yyyy.mm.dd
(0008,0022) AT S Acquisition Date       # yyyy.mm.dd
(0008,0023) AT S Image Date             # yyyy.mm.dd
(0008,0030) AT S Study Time             # hh.mm.ss.frac
(0008,0031) AT S Series Time            # hh.mm.ss.frac
(0008,0032) AT S Acquisition Time       # hh.mm.ss.frac
(0008,0033) AT S Image Time             # hh.mm.ss.frac
(0008,0060) AT S Modality               # CT,NM,MR,DS,DR,US,OT

(0010,0010) AT S Patient Name
(0010,0020) AT S Patient ID
(0010,0030) AT S Patient Birthdate      # yyyy.mm.dd
(0010,0040) AT S Patient Sex            # M, F, O for other
(0010,1010) AT S Patient Age            # xxxD or W or M or Y

(0018,0010) AT M Contrast/Bolus Agent   # or NONE
(0018,0030) AT M Radionuclide
(0018,0050) AN S Slice Thickness        # mm
(0018,0060) AN M KVP
(0018,0080) AN S Repetition Time        # ms
(0018,0081) AN S Echo Time              # ms
(0018,0082) AN S Inversion Time         # ms
(0018,1120) AN S Gantry Tilt            # degrees

(0020,1040) AT S Position Reference     # eg. iliac crest
(0020,1041) AN S Slice Location         # in mm (signed)

(0028,0010) BI S Rows
(0028,0011) BI S Columns
(0028,0030) AN M Pixel Size             # row\col in mm
(0028,0100) BI S Bits Allocated         # eg. 12 bit for CT
(0028,0101) BI S Bits Stored            # eg. 16 bit
(0028,0102) BI S High Bit               # eg. 11
(0028,0103) BI S Pixel Representation   # 1 signed, 0 unsigned
```

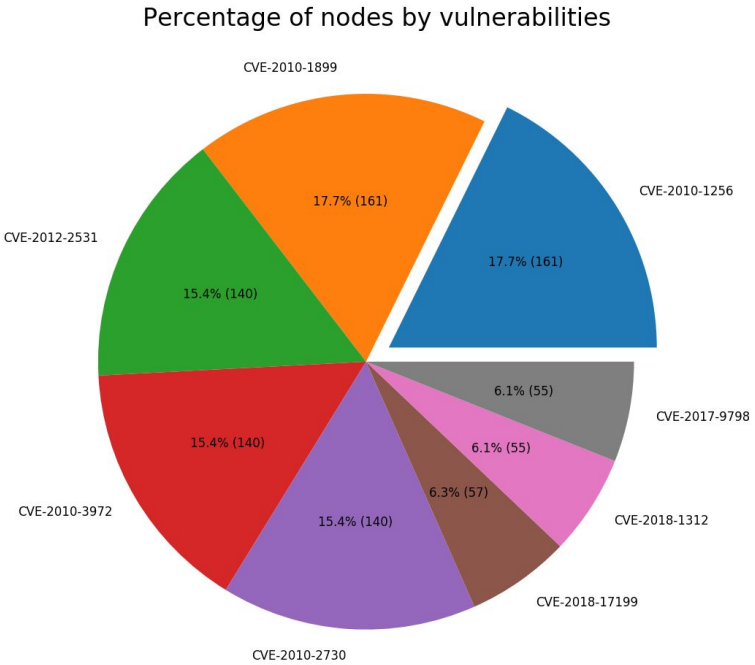


DICOM Results





DICOM Results



1. CVE-2010-1256 - 161
2. CVE-2010-1899 - 161
3. CVE-2012-2531 - 140
4. CVE-2010-3972 - 140
5. CVE-2010-2730 - 140
6. CVE-2018-17199 - 57
7. CVE-2018-1312 - 55
8. CVE-2017-9798 - 55
9. CVE-2018-1283- 55
10. CVE-2017-15715 - 55

Maybe Door Controllers?

VertX™ V100 Door/ Reader Interface

ACCESS CONTROL PROCESSING FOR TWO READERS/ TWO DOORS • 70100

- Reports supervised inputs.
- Connects to the V1000 via RS-485.
- Receives and processes real-time commands from the V1000.
- Reports all activity to the V1000.
- Attractive polycarbonate enclosure protects components from damage.
- All connections and indicators are fully identified by silk-screened nomenclature on the cover.
- Processes off-line access control decisions based on facility code.
- UL® 294 and UL® 1076 recognized components.

The HID VertX™ products provide to the V1000 through a high speed

Maybe Door Controllers?

VertX™ V100 Door/
Reader Interface

Flaw in popular door controllers allow hackers to easily unlock secure doors

The attack doesn't require authentication and can be launched for all door controllers on a network at the same time

The flaw exists in the widely used VertX and Edge lines of door controllers from HID Global, one of the world's largest manufacturers of smartcards, card readers and access control systems.

Reports all activity to the V1000.

Let Me Get That Door for You: Remote Root Vulnerability in HID Door Controllers

HID VertX/Edge discoveryd Command Injection Remote Code Execution Vulnerability

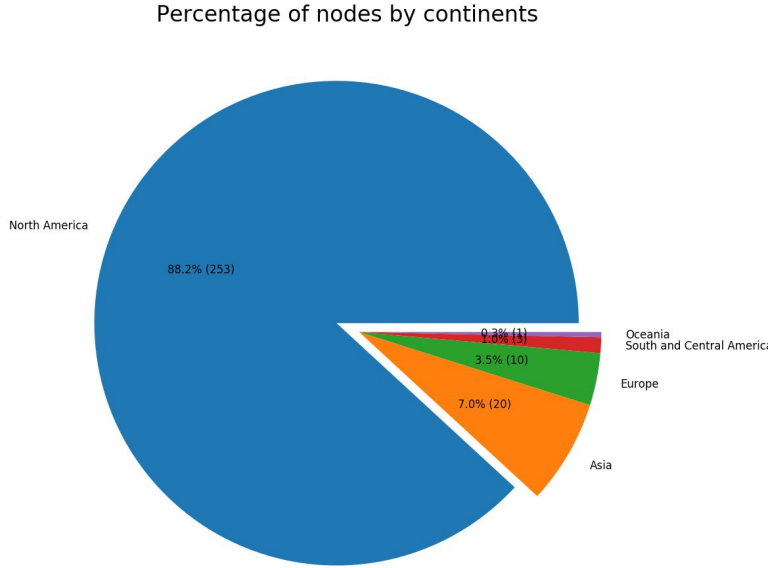
ZDI-16-223
ZDI-CAN-3177

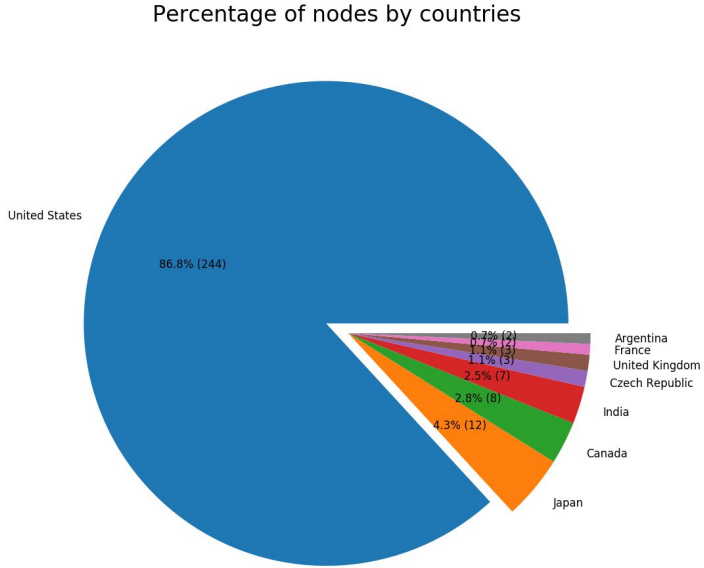
university
, or office
ID's brand

The HID VertX™ products provide

to the V1000 through a high speed

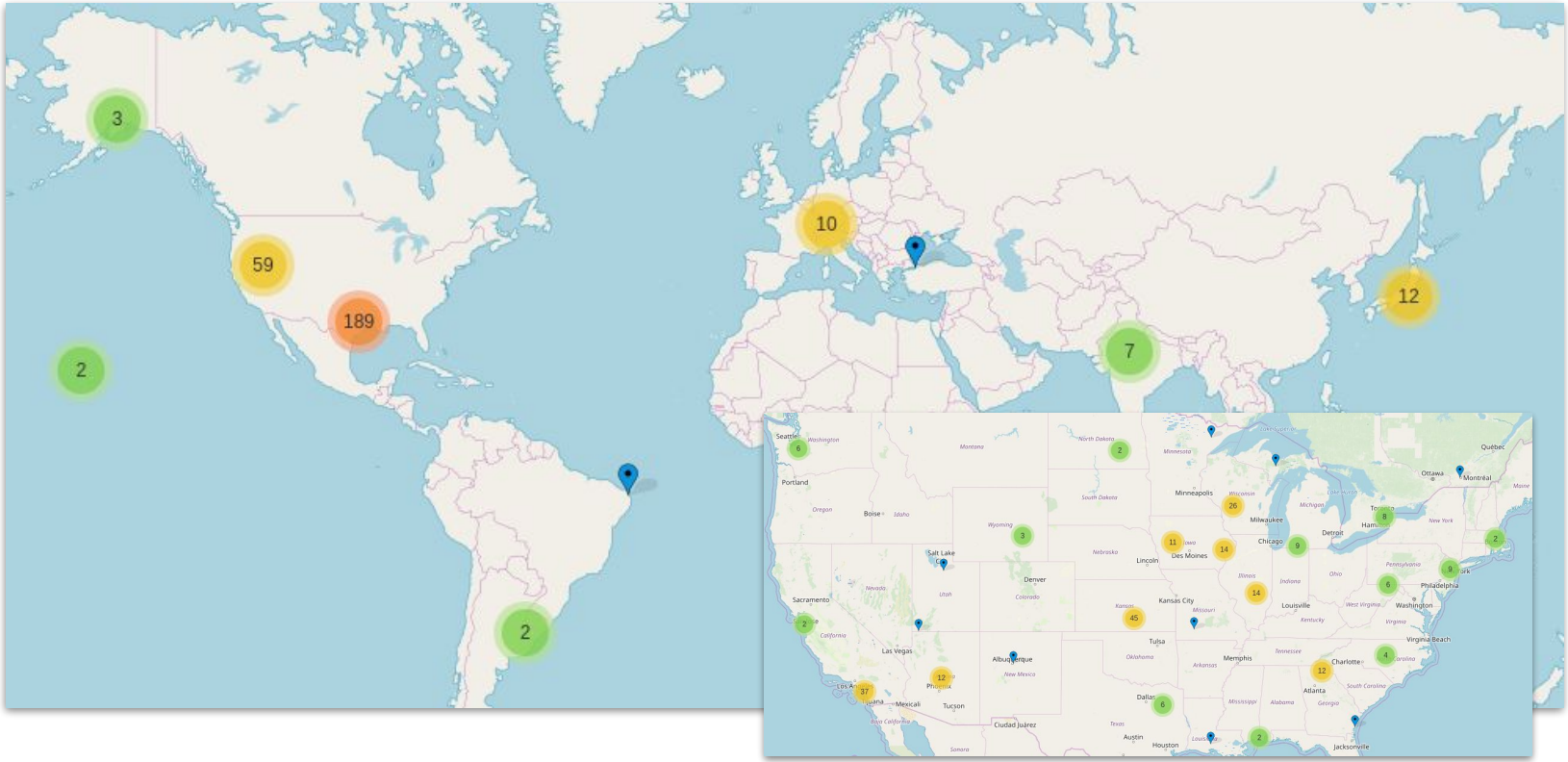
VertX Door Controllers Results





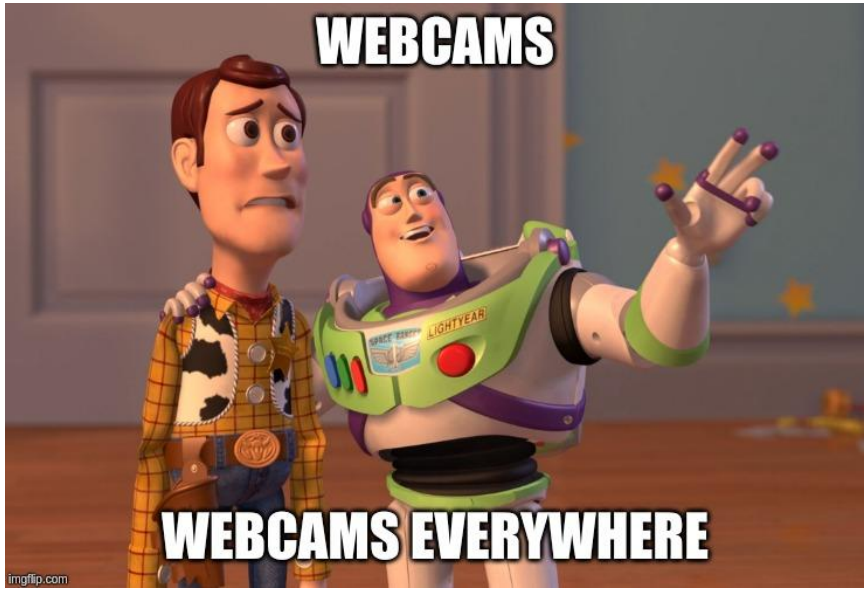
About 300 hosts

VertX Door Controllers Results



VertX Door Controllers Results

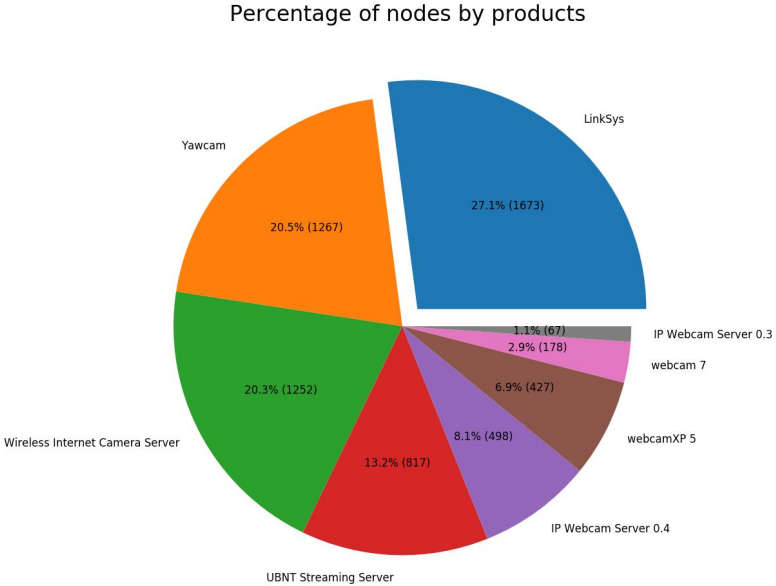
Webcams - Wait... Again?

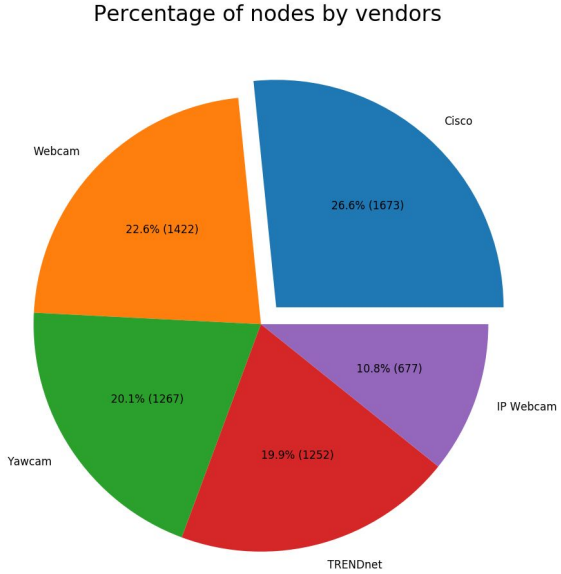


1. Low-hanging fruit for anyone who has access to Shodan, Censys or any other search engine for internet-connected devices.
2. Most people **don't care** about the security of their webcams or other devices.
3. Most cameras **store archived recordings** so you can view the recordings of previous days.

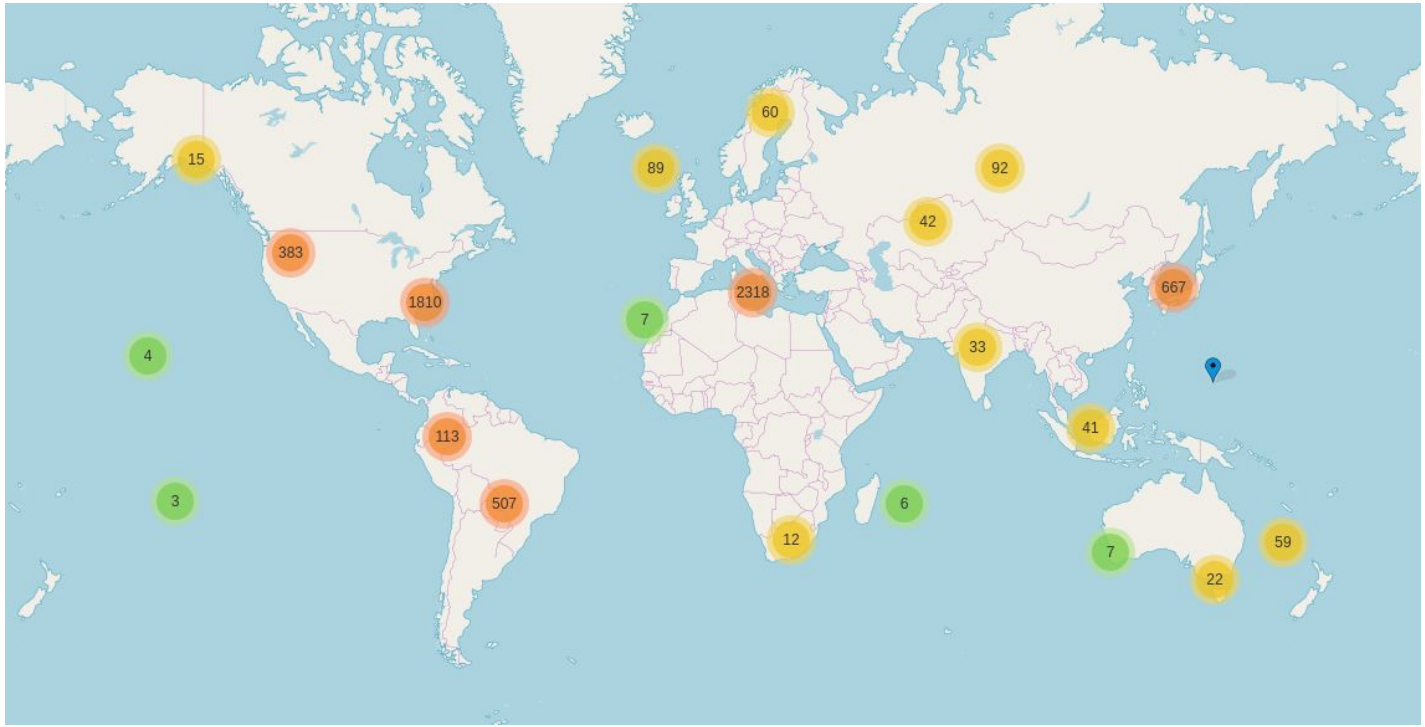

05/18/2019 01:32
05/18/2019 05:37
Black Cisco
05/18/2019 06:00
WHERE IS MY HOUSE?

Webcams Results





Webcams Results



What About Searching for a Job?

```
* Shodan query: "X-Hacker:"
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 18 May 2019 08:29:14 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-hacker: If you're reading this, you should visit automattic.com/jobs and apply to join the fun, mention this he...
```

```
HTTP/1.1 200 OK
Server: Apache
X-Recruiting: If you are reading this, maybe you should be working at PayPal instead! Check out https://www.paypal.com/us
webapps/mpp/paypal-jobs
Paypal-Debug-Id: 92f10fe86ad7d
Cache-Control: no-cache
x-content-type-options: nosniff
x-xss-protection: 1; mode=b...
```

```
* Shodan query: "X-Recruiting:"
```


```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Date: Fri, 17 May 2019 18:59:19 GMT
Location: https://owners.oyorooms.com/
Server: nginx
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Hi-Hacker: Come work with us, email us at careers@oyorooms.com.
X-XSS-Protection: 1...
```

```
* Shodan query: "X-Hi-Hacker:"
```

Thanks for attention!

@manmoleculo

github.com/sdnewhop/grinder