One Framework To Rule Them All

A framework for Internet-connected Device Census

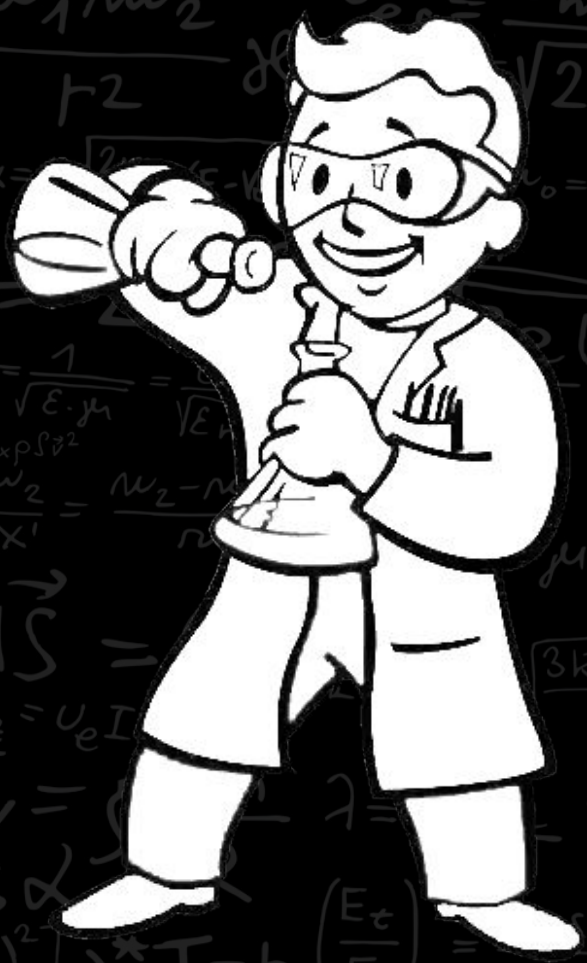
Antoniy Nikolaev

BI.ZONE

Moscow, 17 June 2019

The Main Searching Problems

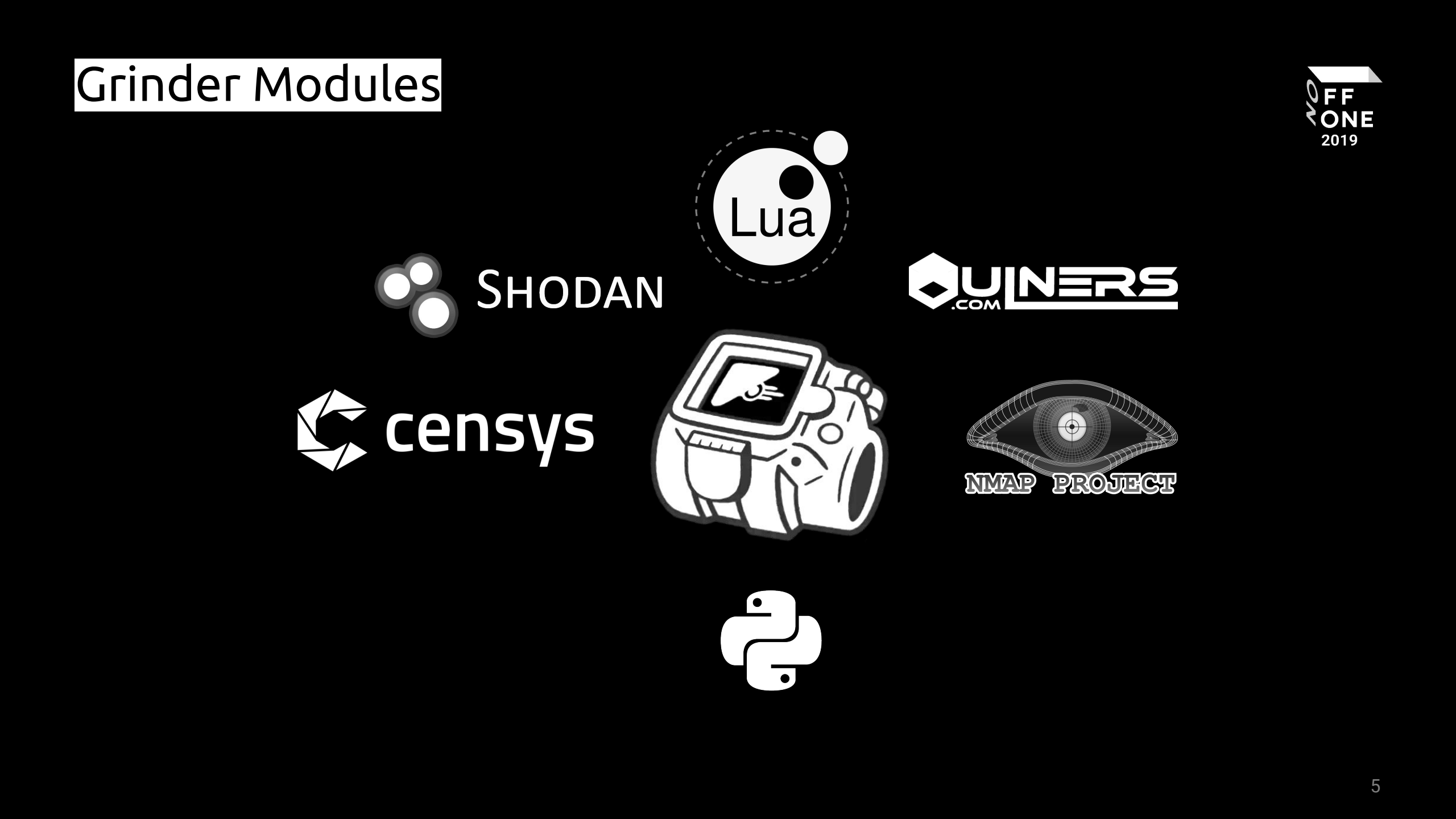
1. How to combine all possible variations of different queries from different systems in one place?
2. How to find vulnerabilities and active services on founded hosts?
3. How to get all actual statistics information about founded results?



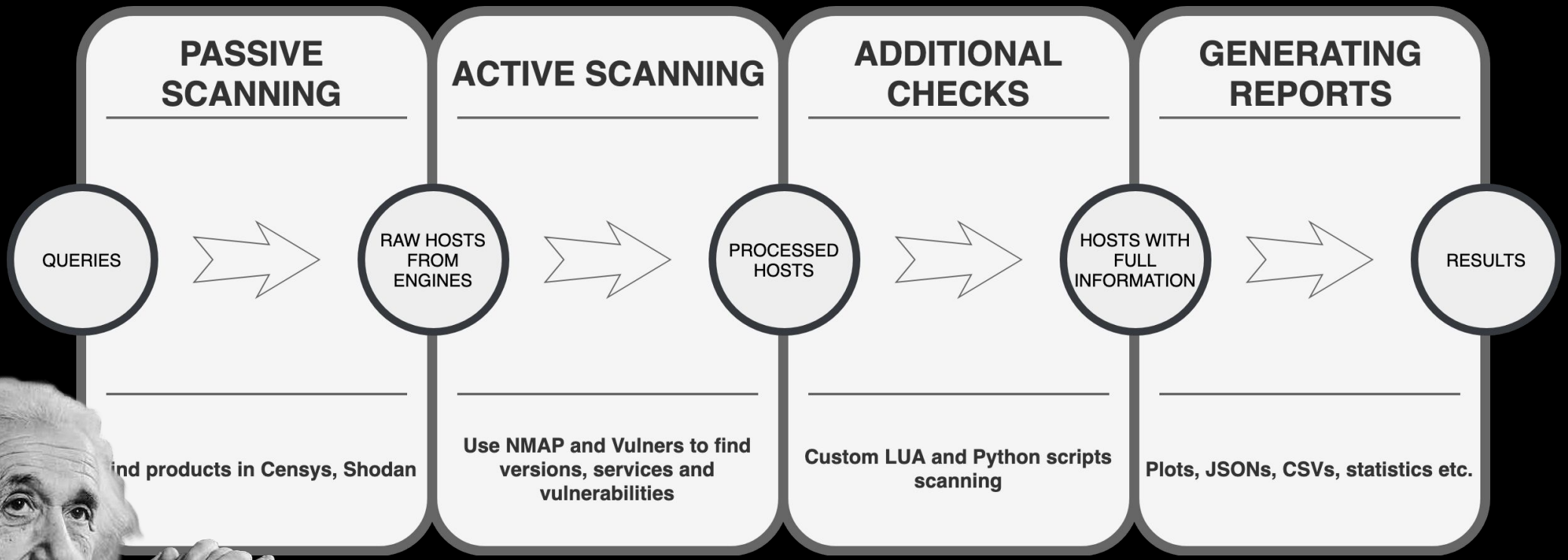
Hold up

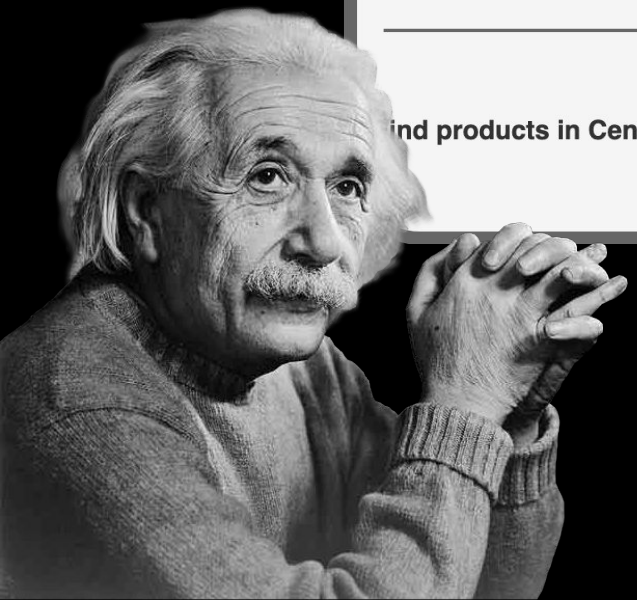
Grinder Framework was created to resolve all these problems automatically just in one touch

Grinder Modules



Grinder Workflow





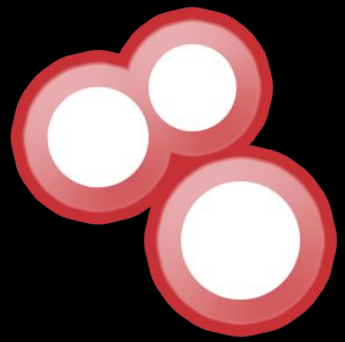
Grinder CLI

```
  .,-::::/ ::::::::..   :::::::.    :::.::::::::-.  .,:::::: ::::::::..
,;;;-'````'  ;;;;``;;;;  ;;;`;;;;,  `;;; ;;,    `';,;;;;''''  ;;;;``;;;;
[[[   [[[[[[/[[[,/[[['  [[[  [[[[[. '[[ `[[     [[ [[cccc   [[[,/[[['
"$$c.    "$$ $$$$$$c    $$$  $$$ "Y$c$$  $$,    $$ $$""""   $$$$$$c
 `Y8bo,,,o88o888b "88bo,888  888    Y88  888_,o8P' 888oo,__ 888b "88bo,
   `'YMUP"YMMMMMM   "W" MMM  MMM     YM  MMMP"`   """"YUMMMMMM   "W"

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
```

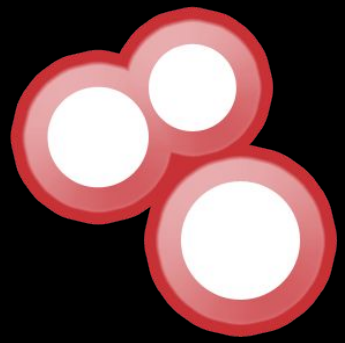
Grinder Features

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. Confidence levels and flexible parameters
5. Vulners API vulnerability scan
6. Custom LUA and Python scripts support

Search Engines



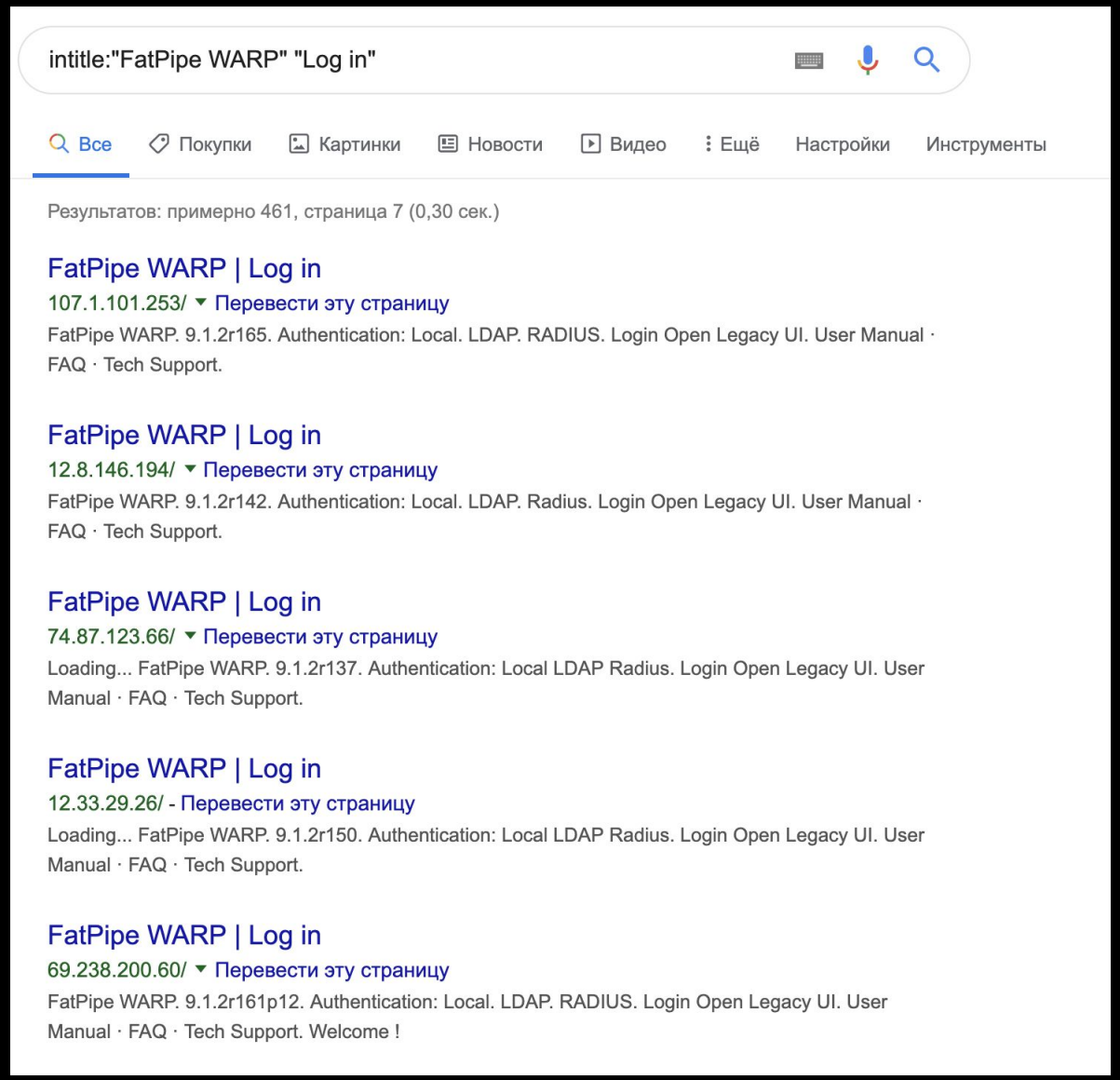
Search Engines



Different Syntax

```
1 Google:  intitle:"FatPipe WARP" "Log in"
2 Shodan:  title:"Fatpipe WARP" port:443
3 Censys:  443.https.get.title:"FatPipe WARP"
```

Different Syntax



More Sophisticated Examples

```
80.http.get.body_sha256: 81a46930a7041737c0c2b94299c14672e192ae4555fccd88cbc369755e84edc7
```

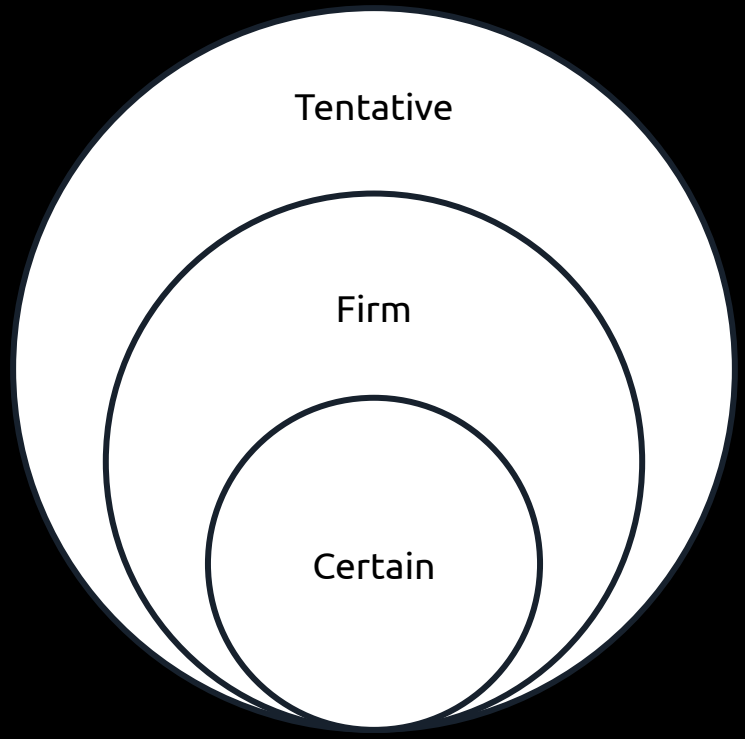
```
ssl:"O=CloudGenix Inc"
```

```
http.favicon.hash:-1338133217
```

```
ssl: "Viprinet" port:"161"
```

```
443.https.tls.certificate.parsed.subject.organization: "Ipanema Technologies"
```

Queries and Vendors Confidence



Grinder Framework Usage Examples

SD-WAN New Hope

Software-defined networking in a wide area network (SD-WAN) quickly becomes very popular in Enterprises. Vendors promises "on-the-fly agility, simplicity, security and automation" and many other benefits. What do you know about SD-WAN? What the "security" means from hand-on perspective? Are present SD-WAN solutions really secure? The goal of this project is to give answers on these questions by analysing different real SD-WAN solutions from the adversaries' point of view.

github.com/sdnewhop/

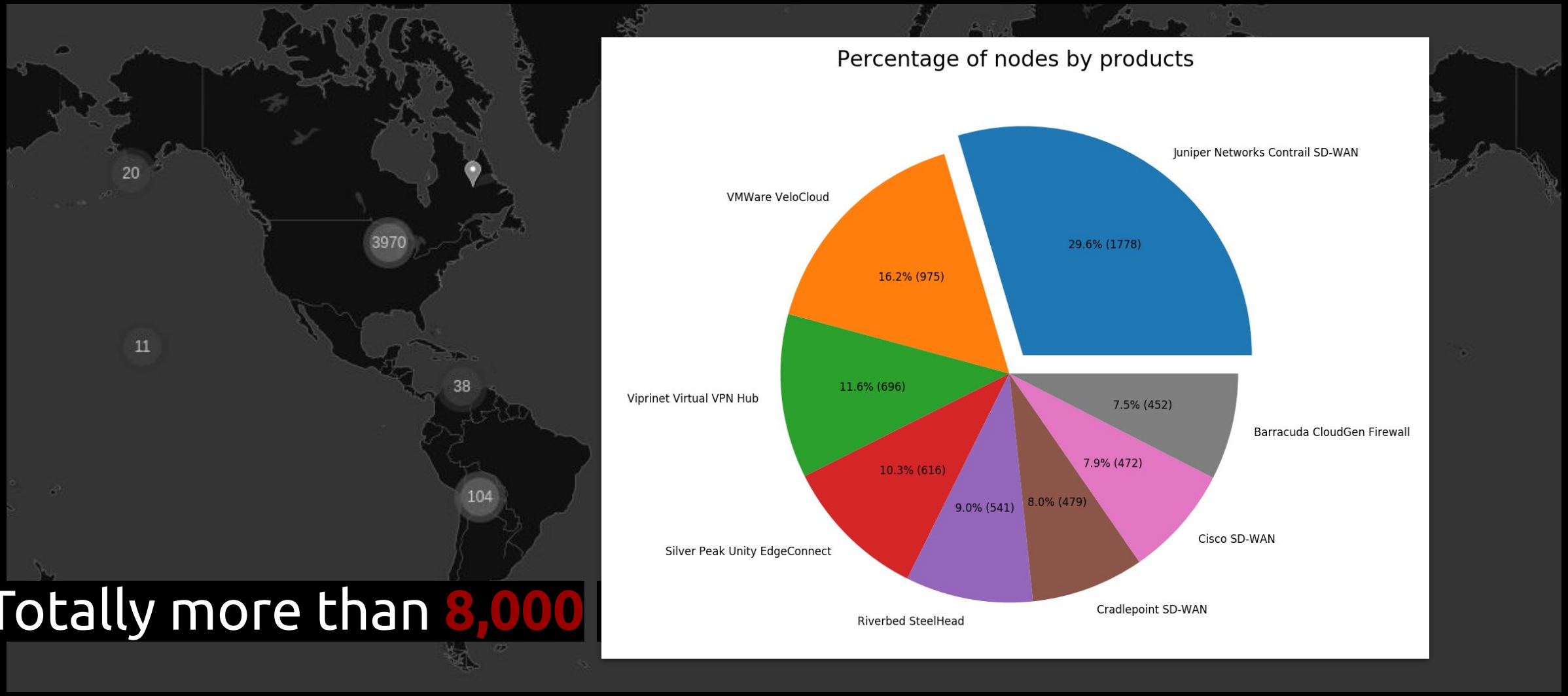
Other tools:

- SD-WAN Harvester
- SD-WAN Infiltrator

SD-WAN New Hope Results

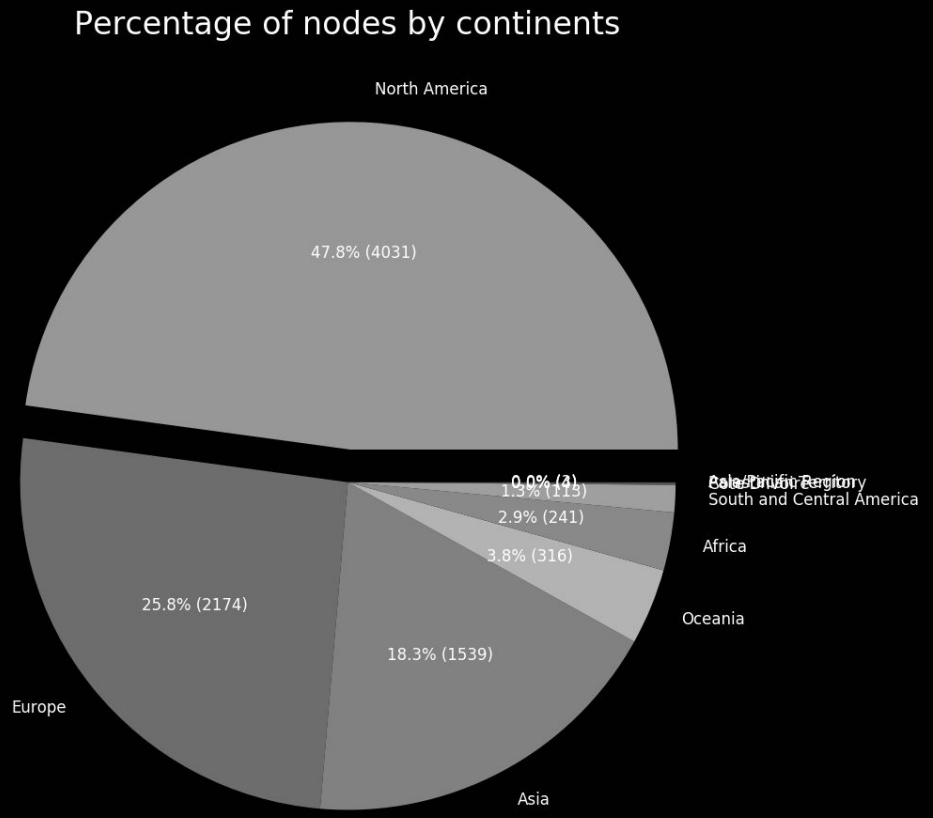
Totally more than **8,000** hosts

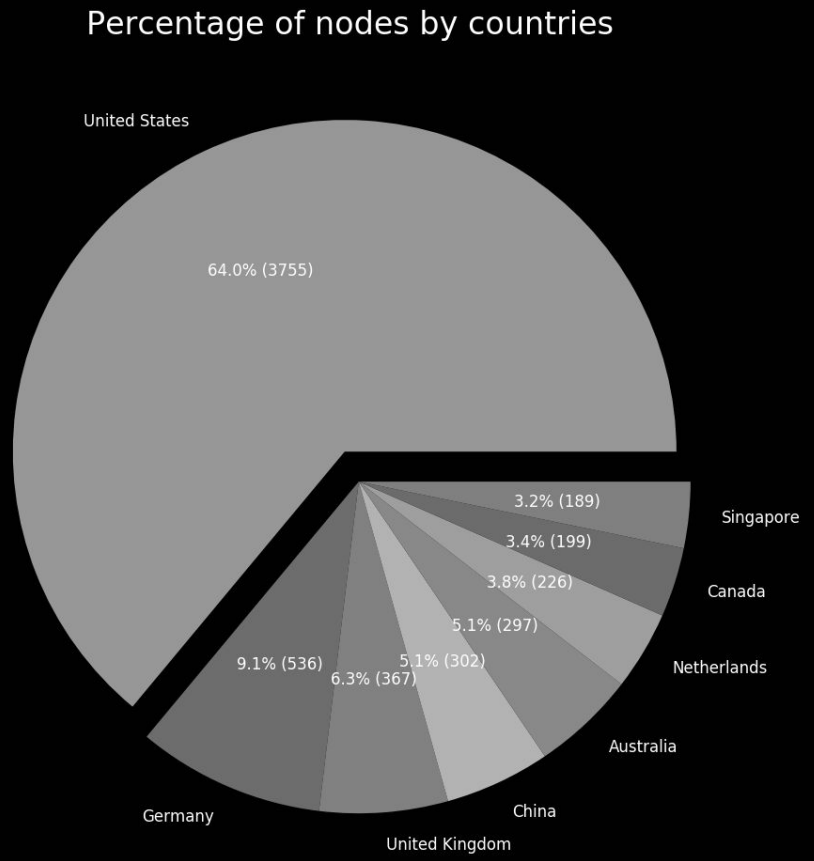
SD-WAN New Hope Results



Totally more than **8,000**

SD-WAN New Hope Results





Medicine

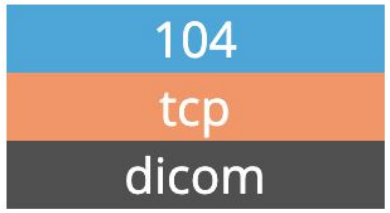
DICOM

2. **The DICOM protocol is a binary Upper Level Protocol (ULP) over TCP/IP**. Well known ports used by DICOM are 104, 2761, 2762 and 11112. It is used to process DICOM data, transmit, search/query, integrate, distribute, print, share, store, display medical images and patient data from the radiology archival/storage systems (PACS, RIS) to the workstation for the Radiologist to write reports.

DICOM have reserved the following TCP and UDP port numbers by the Internet Assigned Numbers Authority (IANA): 104 well-known port for DICOM over Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). Since 104 is in the reserved subset, many operating systems require special privileges to use it; 2761 registered port for DICOM using Integrated Secure Communication Layer (ISCL) over TCP or UDP; 2762 registered port for DICOM using Transport Layer Security (TLS) over TCP or UDP; 11112 registered port for DICOM using standard, open communication over TCP or UDP. The standard recommends but does not require the use of these port numbers.

2. *The port number is not already taken by another application.* For example, using port 80 for DICOM would not be wise because port 80 is traditionally used by Web browsers, and won't be available for anything else. If you do not like standard DICOM port 104, try using ports with high numbers (say, 10,000 and up); their chances of being used are usually lower.

DICOM



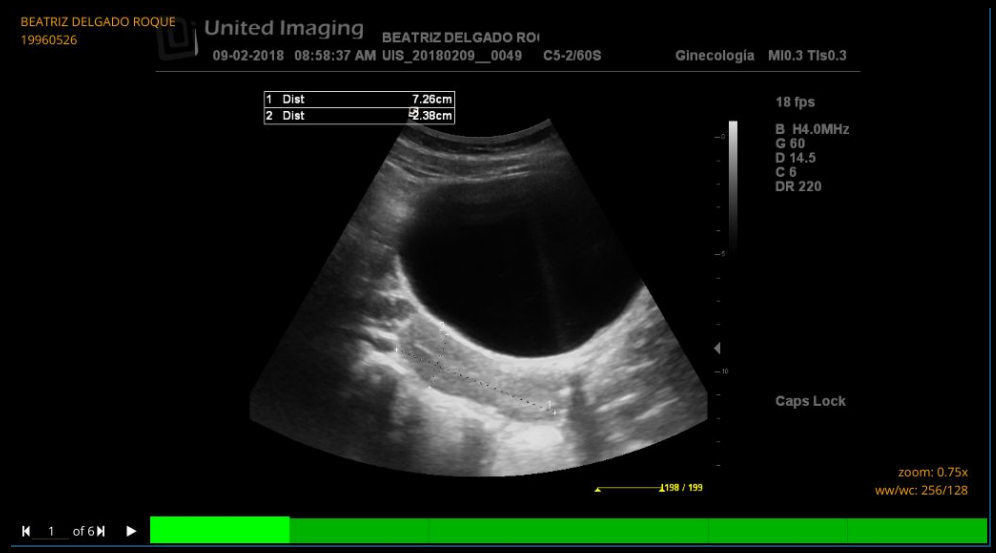

```
DICOM Server Response
\x02\x00\x00\x00\x00\xb3\x00\x01\x00\x00ANY-SCP         FINDSCU
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00
\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x03\x00@\x00\x00\x
111.2.840.10008.1.2P\x00\x005Q\x00\x00\x04\x00\x00\xff\xffR\x00\x00\x
181.3.6.1.4.1.11157.4.8.17U\x00\x00\rmsiCOM3 4.8.q
```

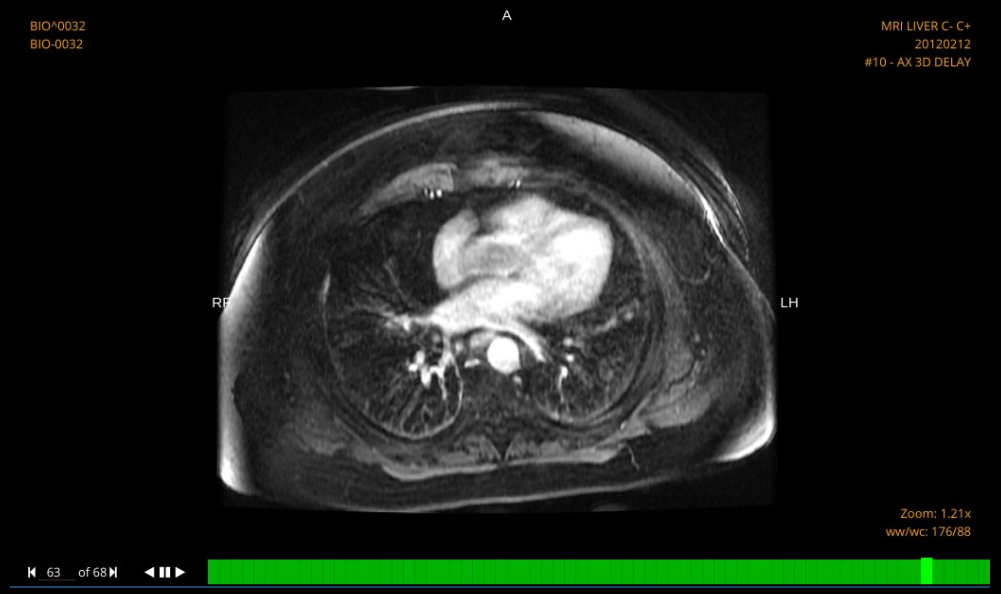
DICOM Results

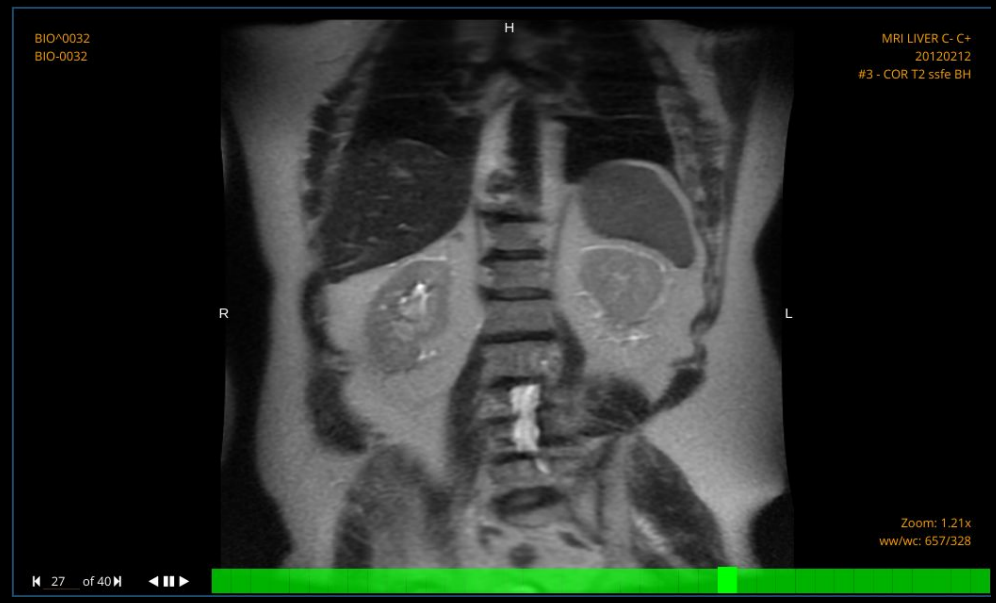
Totally more than **1,700** hosts

In Addition

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

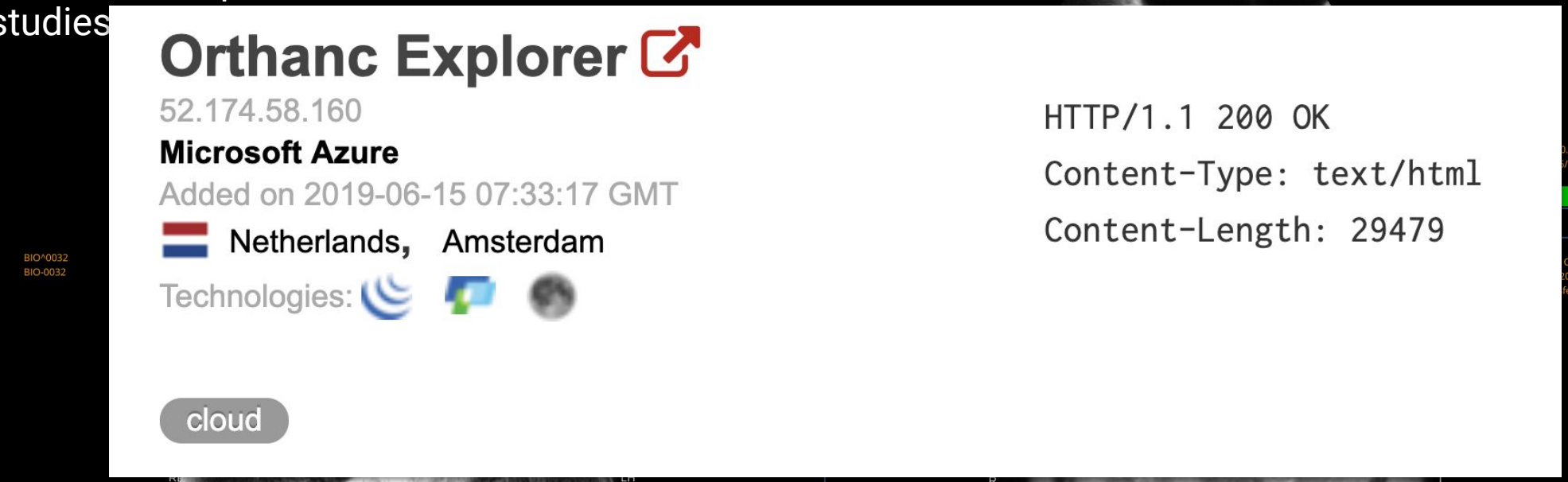






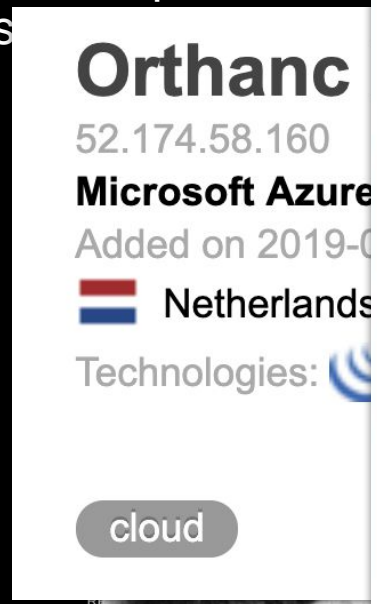
In Addition

You can also find patient data like studies



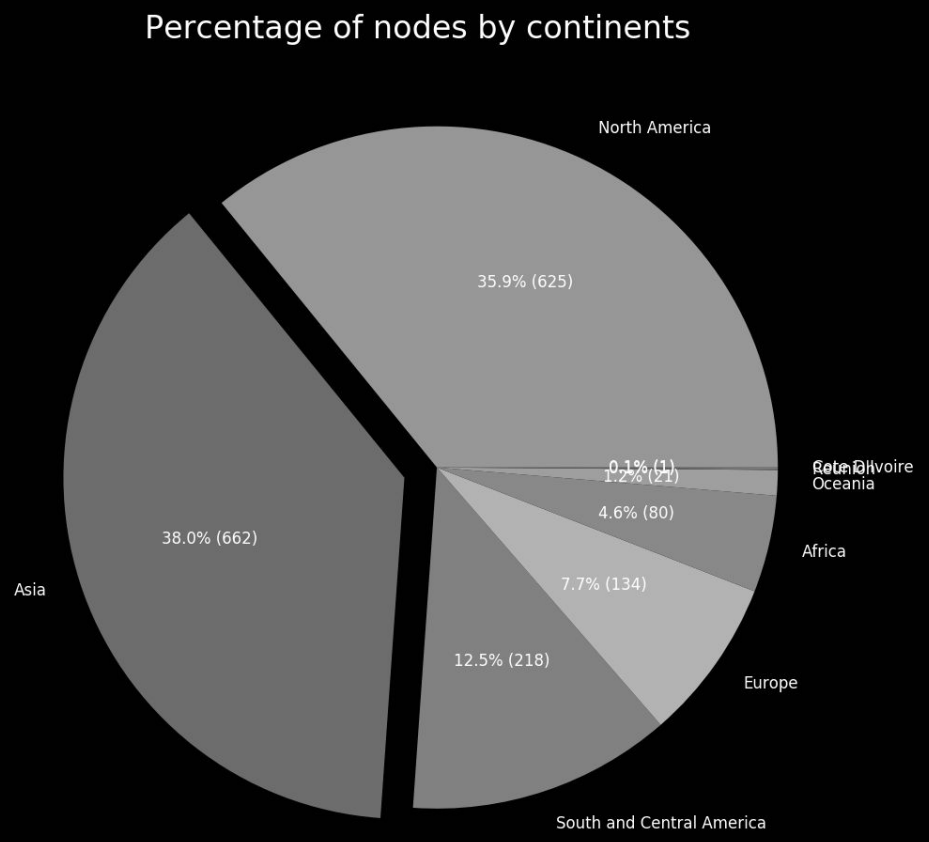
In Addition

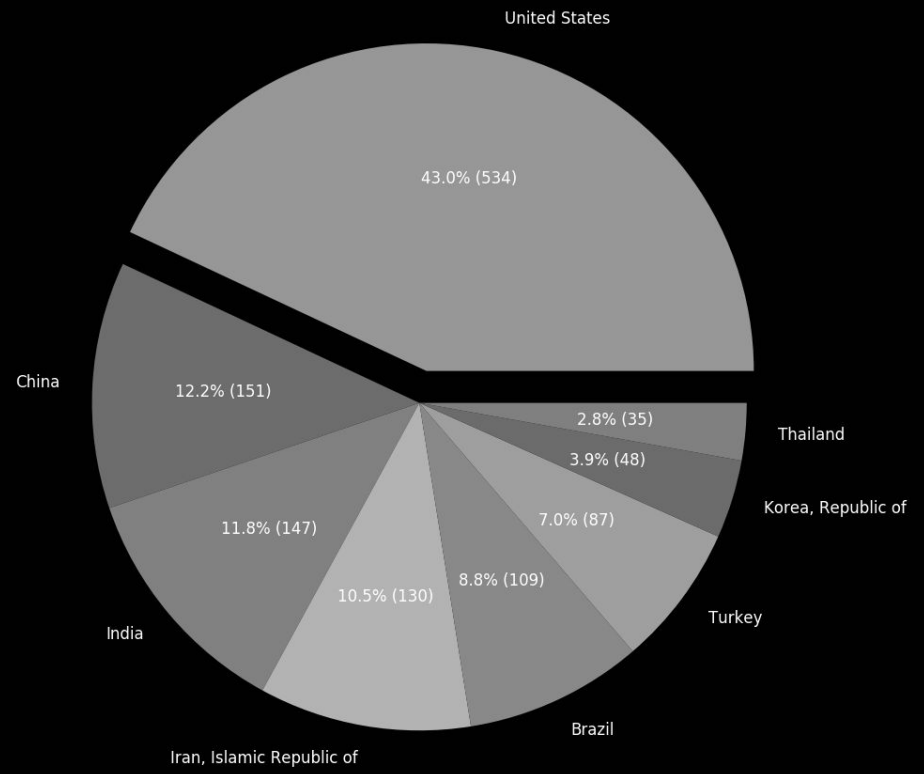
You can also find patient dat
like studies



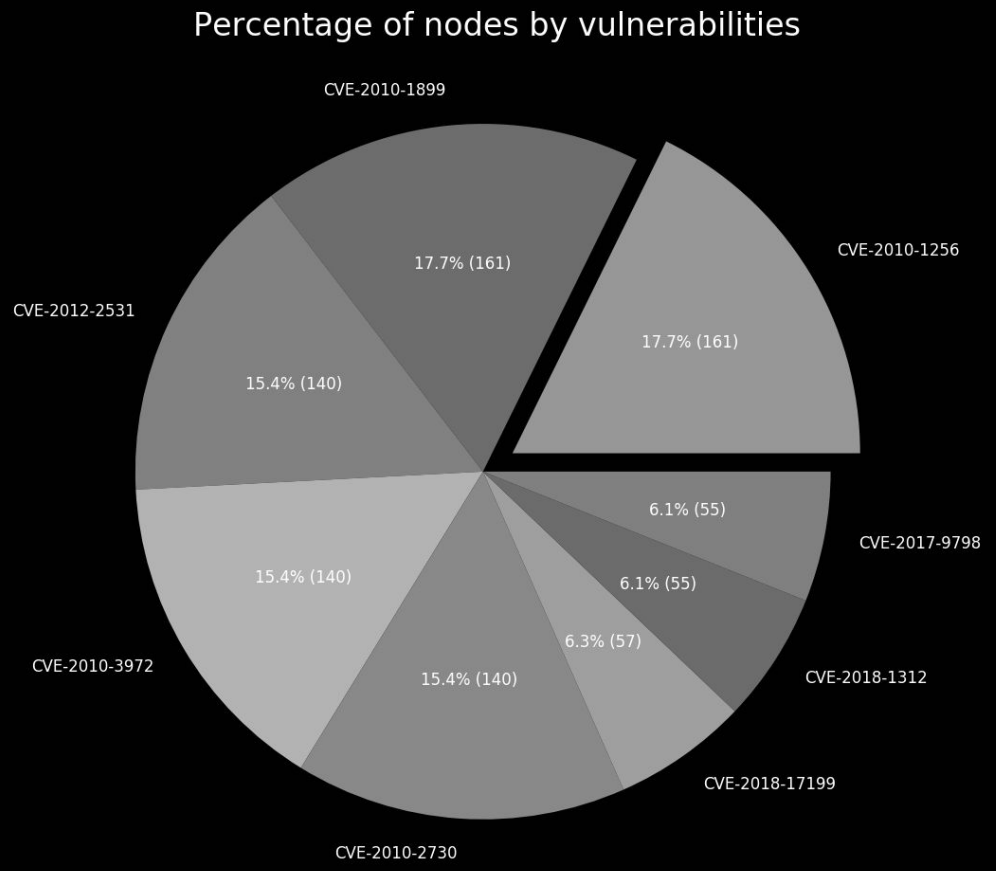

```
(nnnn,0000) BD S Group Length          # of bytes in group nnnn
(nnnn,4000) AT M Comments

(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

Physical Access

VertX Door Controllers

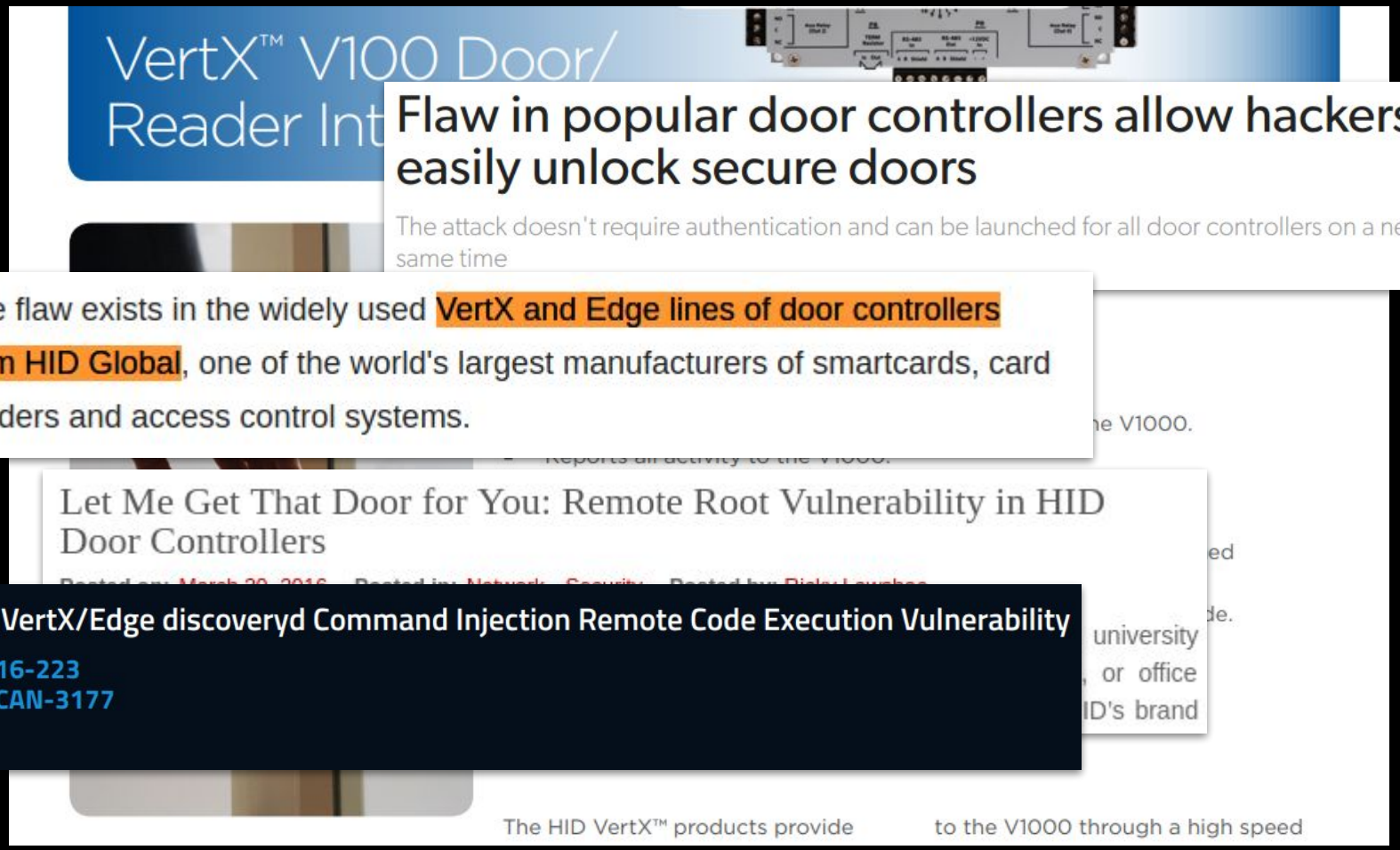
VertX™ V100 Door/ Reader Interface

ACCESS CONTROL PROCESSING FOR TWO READERS/ TWO DOORS • 70100

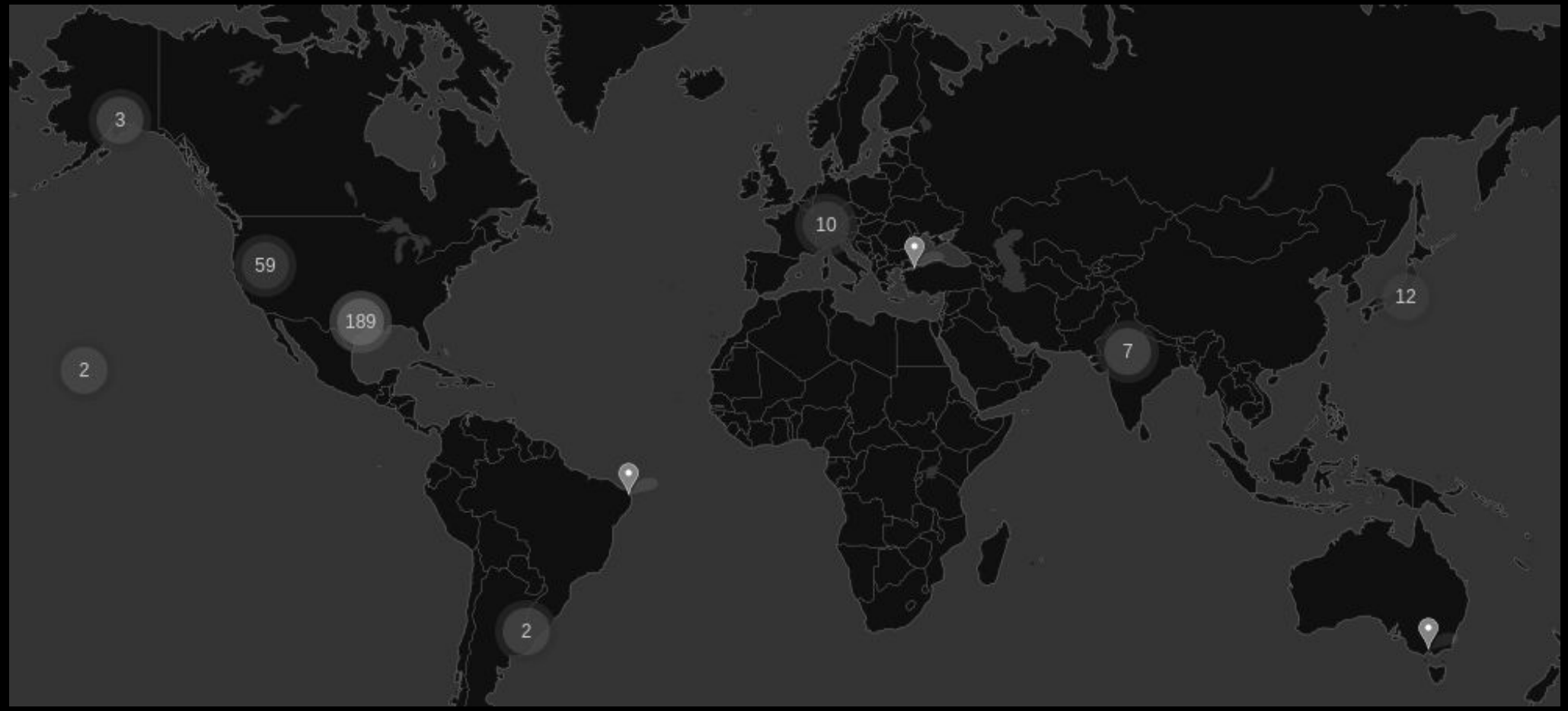
- Reports supervised inputs.
- Connects to the V1000 via RS-485.
- Receives and processes real-time commands from the V1000.
- Reports all activity to the V1000.
- Attractive polycarbonate enclosure protects components from damage.
- All connections and indicators are fully identified by silk-screened 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

VertX Door Controllers

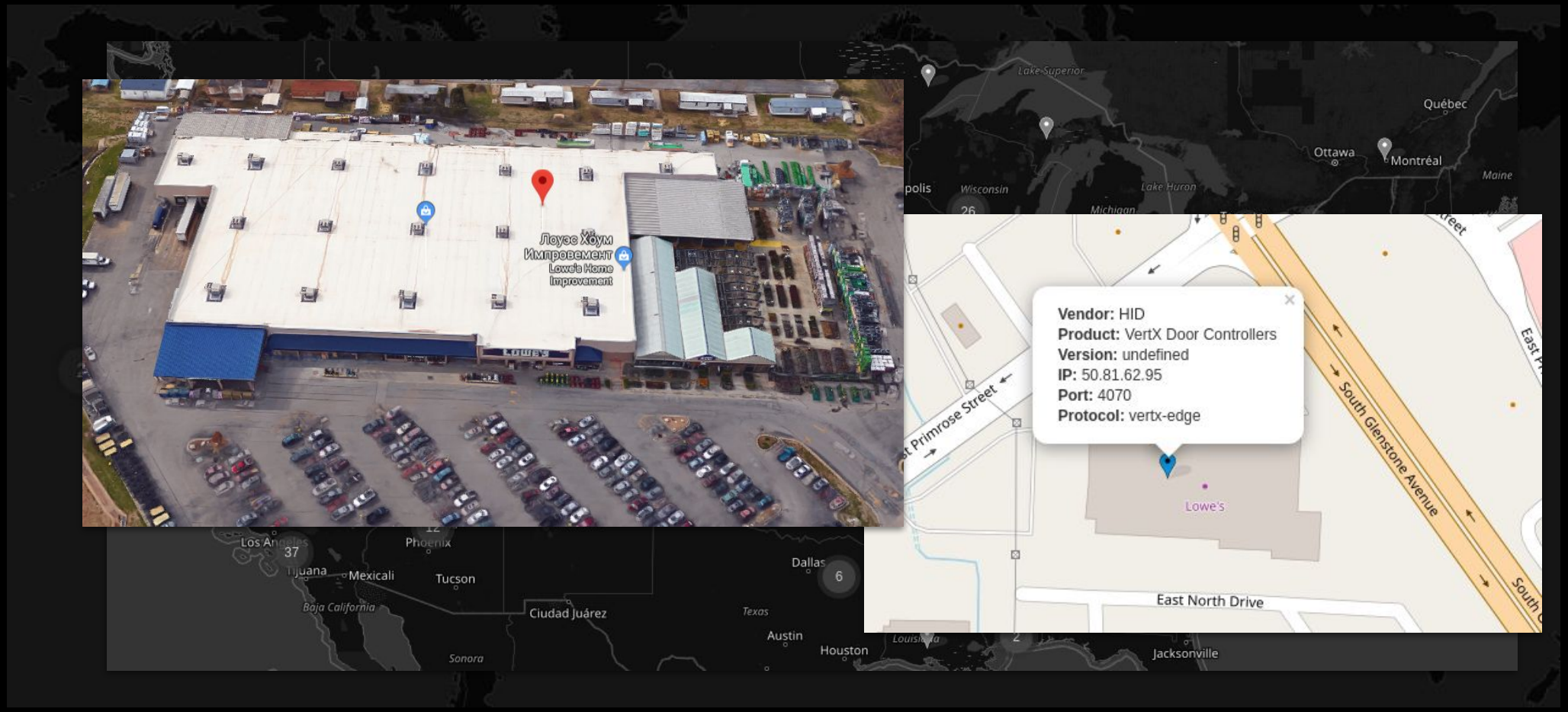


VertX Door Controllers



VertX Door Controllers

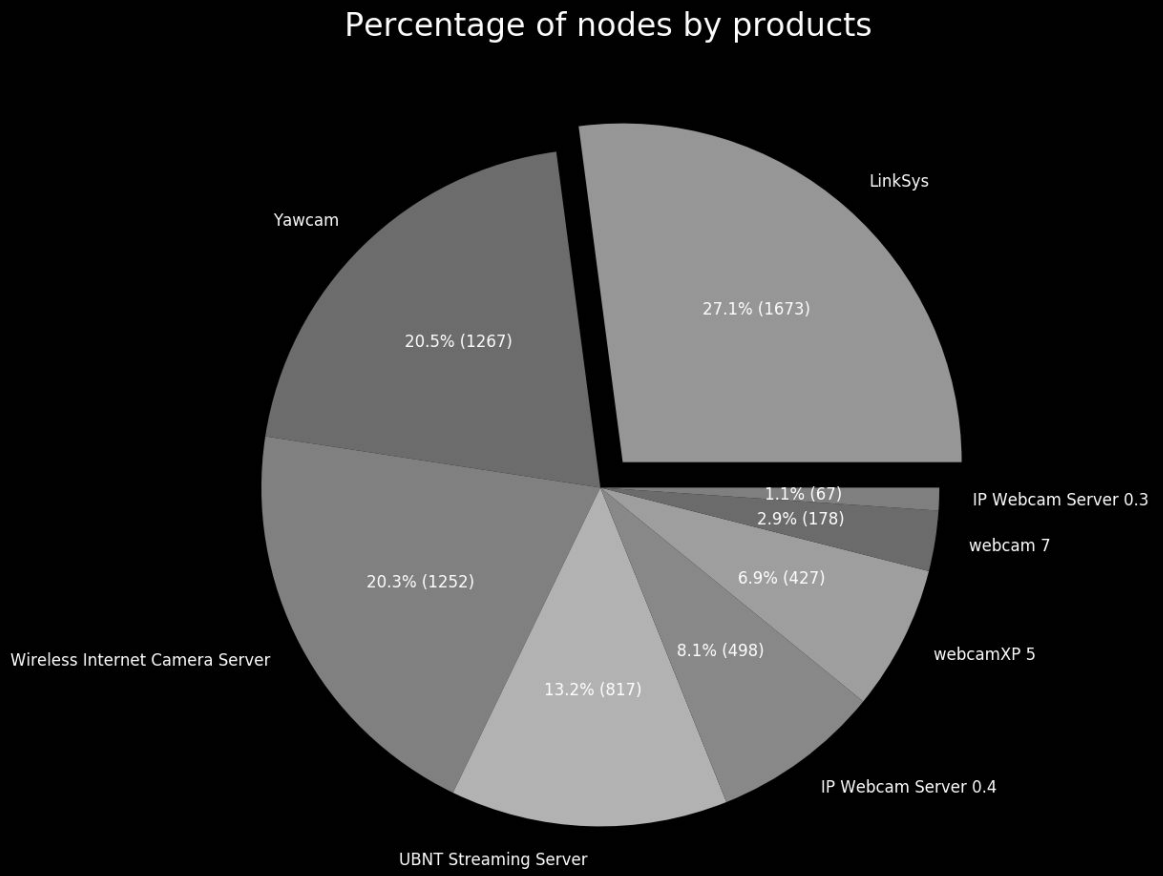
VertX Door Controllers

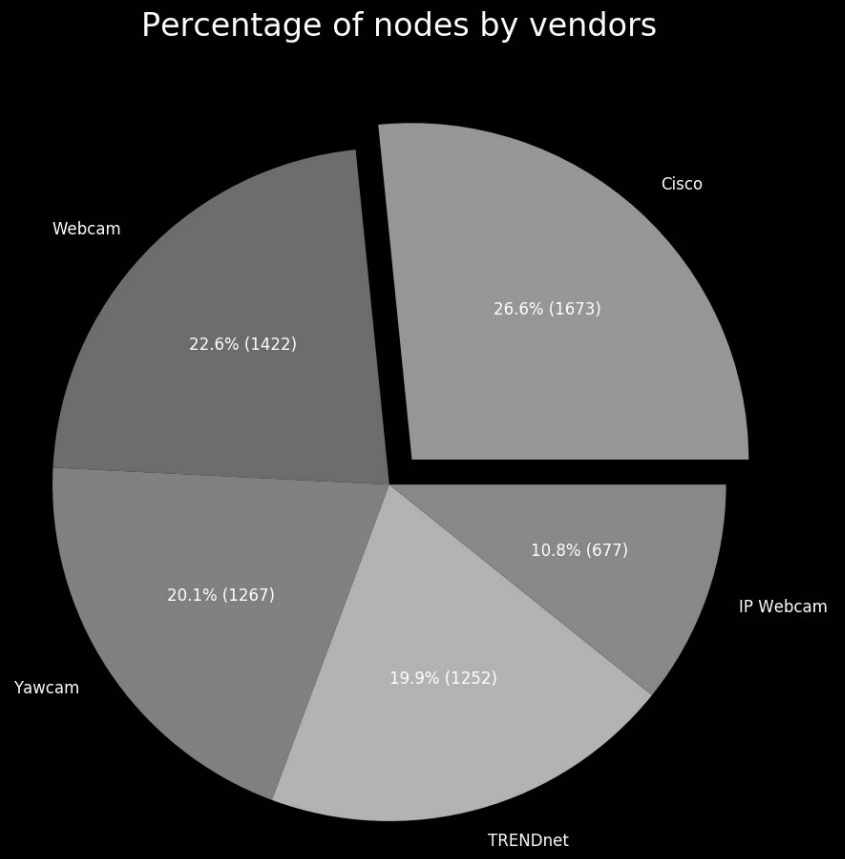


Webcams

Webcams

Webcams


Percentage of nodes by products
LinkSys
27.1% (1673)
Yawcam
20.5% (1267)
IP Webcam Server 0.3
1.1% (67)
webcam 7
2.9% (178)
webcamXP 5
6.9% (427)
IP Webcam Server 0.4
8.1% (498)
UBNT Streaming Server
13.2% (817)
Wireless Internet Camera Server
20.3% (1252)


Percentage of nodes by vendors
Cisco
26.6% (1673)
Webcam
22.6% (1422)
IP Webcam
10.8% (677)
TRENDnet
19.9% (1252)
Yawcam
20.1% (1267)

Webcams Map

Thanks for attention.
Got questions?


@manmoleculo


github.com/sdnewhop/grinder

Grinder Framework

github.com/sdnewhop/grinder