

Trust, but Verify: Dangers of MaaS

Denis Kolegov, Antoniy Nikolaev
AISec Team

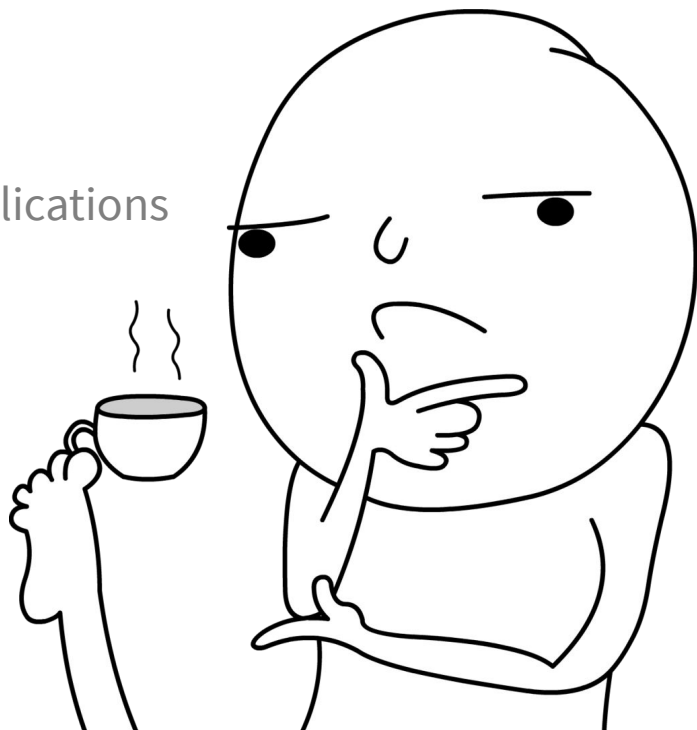


What it is All About?



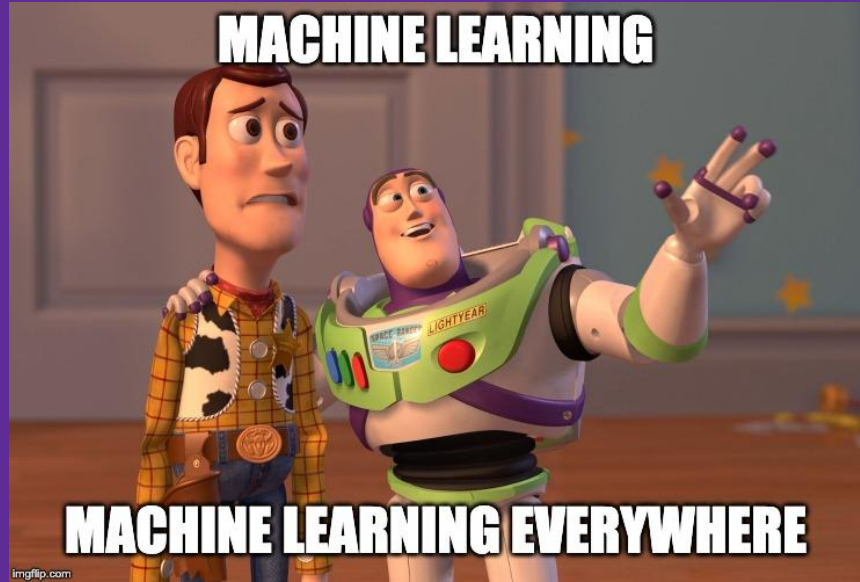
What it is All About?

1. How to find different machine learning applications and frameworks on the Internet?
2. Are those solutions internet-wide secure?
3. What information can be obtained from them?
4. In which countries running machine learning applications can be found and what is their purpose?



Why?

Why?



Cloud Text-to-Speech

Text-to-speech conversion powered by machine learning.



TRY IT FREE

[VIEW DOCUMENTATION](#)

OpenCV.js Demos

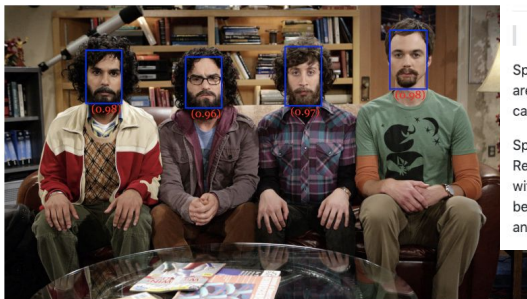
- Video processing (asm.js)
- Video processing (wasm)
- Face detection (asm.js)
- Face detection (wasm)

annyang! SpeechRecognition that just works

annyang is a tiny javascript library that lets your visitors control your site with voice commands. annyang supports multiple languages, has no dependencies, weighs just 2kb and is free to use.



face-api.js playground



Speech KITT

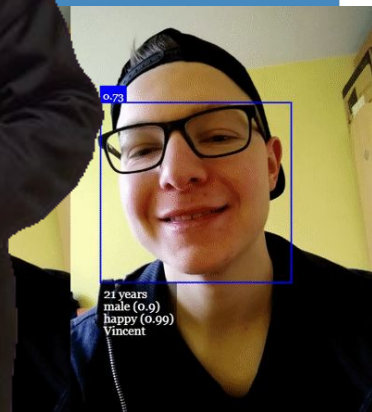
A flexible GUI for interacting with Speech Recognition

Speech KITT makes it easy to add a GUI to sites using Speech Recognition. Whether you are using **annyang**, a different library or **webkitSpeechRecognition** directly, KITT will take care of the GUI.

Speech KITT provides a **graceful** way for the user to start or stop Speech Recognition and see its status. It also help guide the user on how to interact with your site using **instructions** and **sample commands**. It can even be used to carry a **named** user, asking questions the user can answer with his voice.



Interested In
VOICING YOUR SITE
WITH... OF CODE?



So What About
Security*?



So What About Security*?

*(NOT EXACTLY)



The Problems

1. Many different interfaces of various ML frameworks are open and accessible from the Internet
2. Most of them don't have authentication mechanisms or got weak security policies
3. Default credentials almost the same and can be found in the documentation
4. Common vulnerabilities (web, software, etc.) both on server- and client-side

The Problems

1. Many different security policies
2. Most of the security policies are client-side
3. Default configuration is often insecure
4. Common vulnerabilities



accessible from
security policies
presentation
client-side

Vulnerabilities



Machine Learning Frameworks

 TensorFlow

 PyTorch

theano

Caffe

 mxnet



Chainer



Caffe2

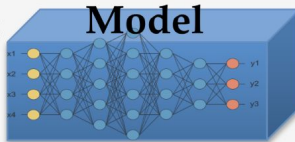
Software Layers in Machine Learning Apps

DL
Applications

Program Logic



Model



Data



DL
Frameworks

Torch theano
TensorFlow Caffe

Framework
Dependencies



GNU LibC



protobuf
Protocol Buffers



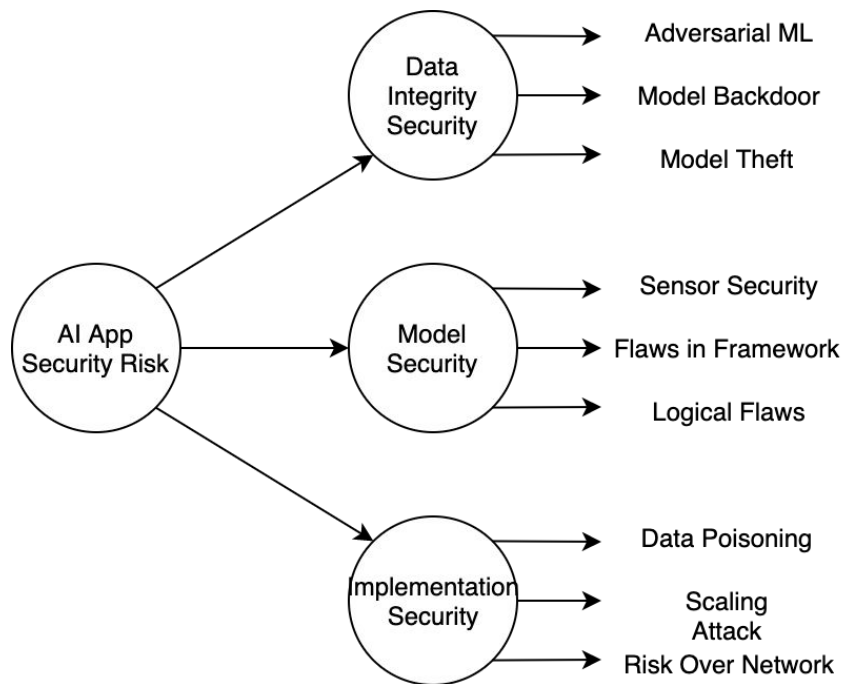
NumPy

zlib



OpenCV

AI or ML Application Threat Landscape



Frameworks Complexity and Dependencies

ML Framework	Lines of Code	Number of Dep. Packages	Sample Packages
Caffe	127K+	137	Libprotobuf, libz, opencv, libopenblas
TensorFlow	887K+	97	numpy, librosa
Torch	590K+	48	xlua, qtsvg, opencv

Common Bugs Found in ML Frameworks and Dependencies

ML Framework	dep. packages	CVE-ID	Potential Threats
TensorFlow	numpy	CVE-2017-12852	DOS
TensorFlow	wave.py	CVE-2017-14144	DOS
Caffe	libjasper	CVE-2017-9782	Heap Overflow
Caffe	openEXR	CVE-2017-12596	Crash
Caffe/Torch	opencv	CVE-2017-12597	Heap Overflow
Caffe/Torch	opencv	CVE-2017-12598	Crash
Caffe/Torch	opencv	CVE-2017-12599	Crash
Caffe/Torch	opencv	CVE-2017-12600	DOS
Caffe/Torch	opencv	CVE-2017-12601	Crash

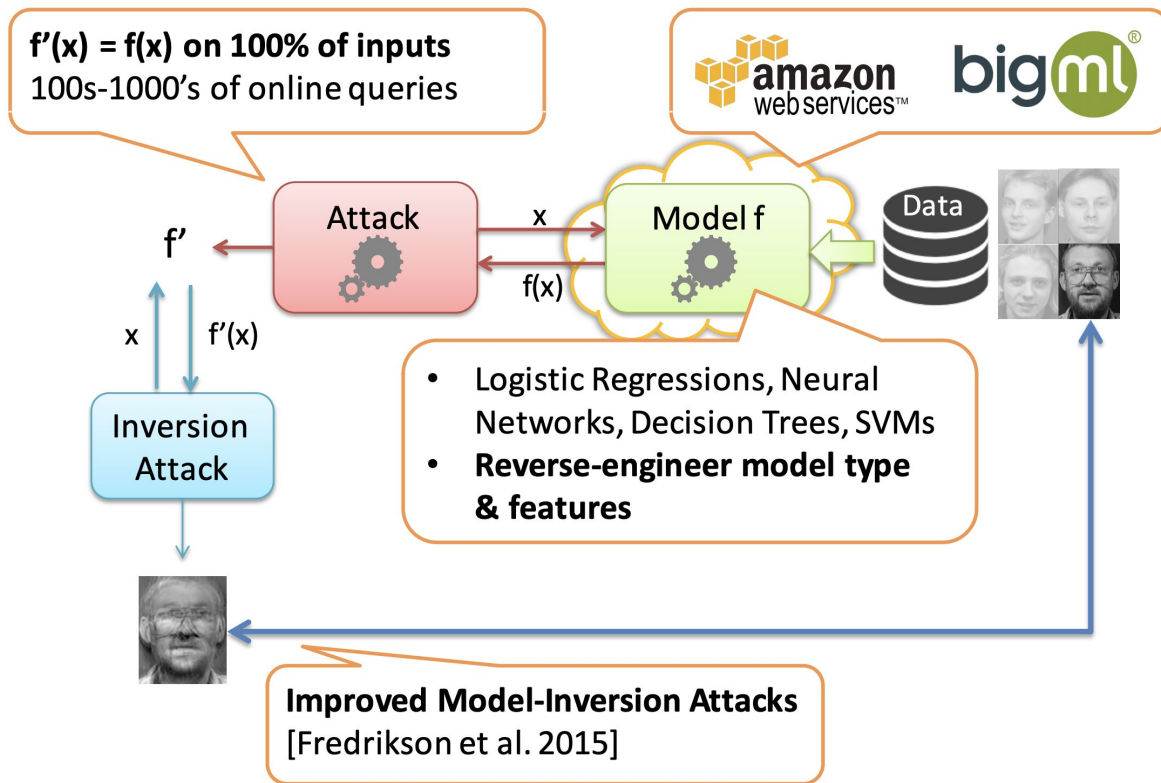
ML Framework	dep. packages	CVE-ID	Potential Threats
Caffe/Torch	opencv	CVE-2017-12602	DOS
Caffe/Torch	opencv	CVE-2017-12603	Crash
Caffe/Torch	opencv	CVE-2017-12604	Crash
Caffe/Torch	opencv	CVE-2017-12605	Crash
Caffe/Torch	opencv	CVE-2017-12606	Crash
Caffe/Torch	opencv	CVE-2017-14136	Integer Overflow

What Does it Mean?

Machine Learning applications and related infrastructure (servers, wrappers, handlers) are vulnerable to different kinds of vulnerabilities: crashes, denial of service, integer and heap overflows, etc.



Model Extraction Attacks



How to Find ML Frameworks and Applications?



Search Engines

Google

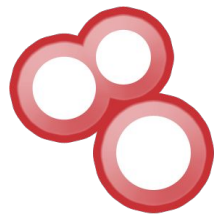


Search Engines



How can we search
deeper?

Search Engines



SHODAN



censys

ZoomEy👁

Grinder Framework

grinder

🔍 Python framework to automatically discover and enumerate hosts from different back-end systems (Shodan, Censys)

python

nmap

vulnerability-scanners

python-framework

shodan-api

vulners

censys-api

Python GPL-2.0 4 22 0 0 Updated 7 days ago



github.com/sdnewhop/grinder

```

x.x.x.x.x x.x.x.x.x x.x.x.x.x x.x.x.x.x x.x.x.x.x x.x.x.x.x x.x.x.x.x x.x.x.x.x
$- - - - - / - - - - - : - - - - - : - - - - - : - - - - - : - - - - - : - - - - - : - - - - - :
CCC CCCCCC/CCC/CCE' CCC CCCCC 'CC 'CC CC [[cccc [CC/'CCC'
"$Sc. "$ $$$$$$$$ $$$ $$$ '$c$c$ $$, $$ $$$$$$
`Y8bo,,,o88o888b "88bo,888 888 Y88 888,,o8P' 888oo,___ 888b "88bo,
`YMUP"YMMMMM "W" MM MMM MM YM MMMP" """"YUMMMMM "W"

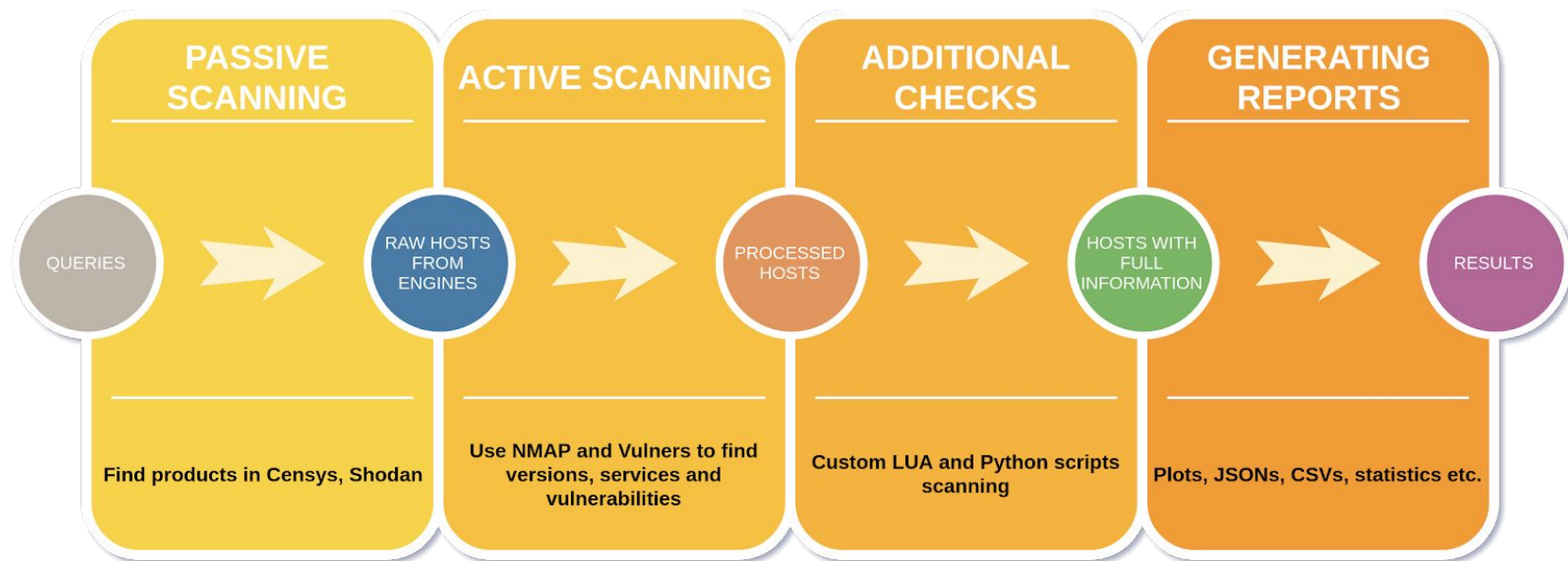
usage: grinder.py [-h] [-r] [-u] [-q QUERIES_FILE] [-sk SHODAN_KEY] [-cu]
                  [-cp] [-ci CENSYS_ID] [-cs CENSYS_SECRET] [-cm CENSYS_MAX]
                  [-nm] [-nw NMAP_WORKERS] [-vs] [-vw VULNERS_WORKERS]
                  [-c CONFIDENCE] [-v [VENDORS [VENDORS ...]]] [-ml MAX_LIMIT]

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 Workflow



Training Systems

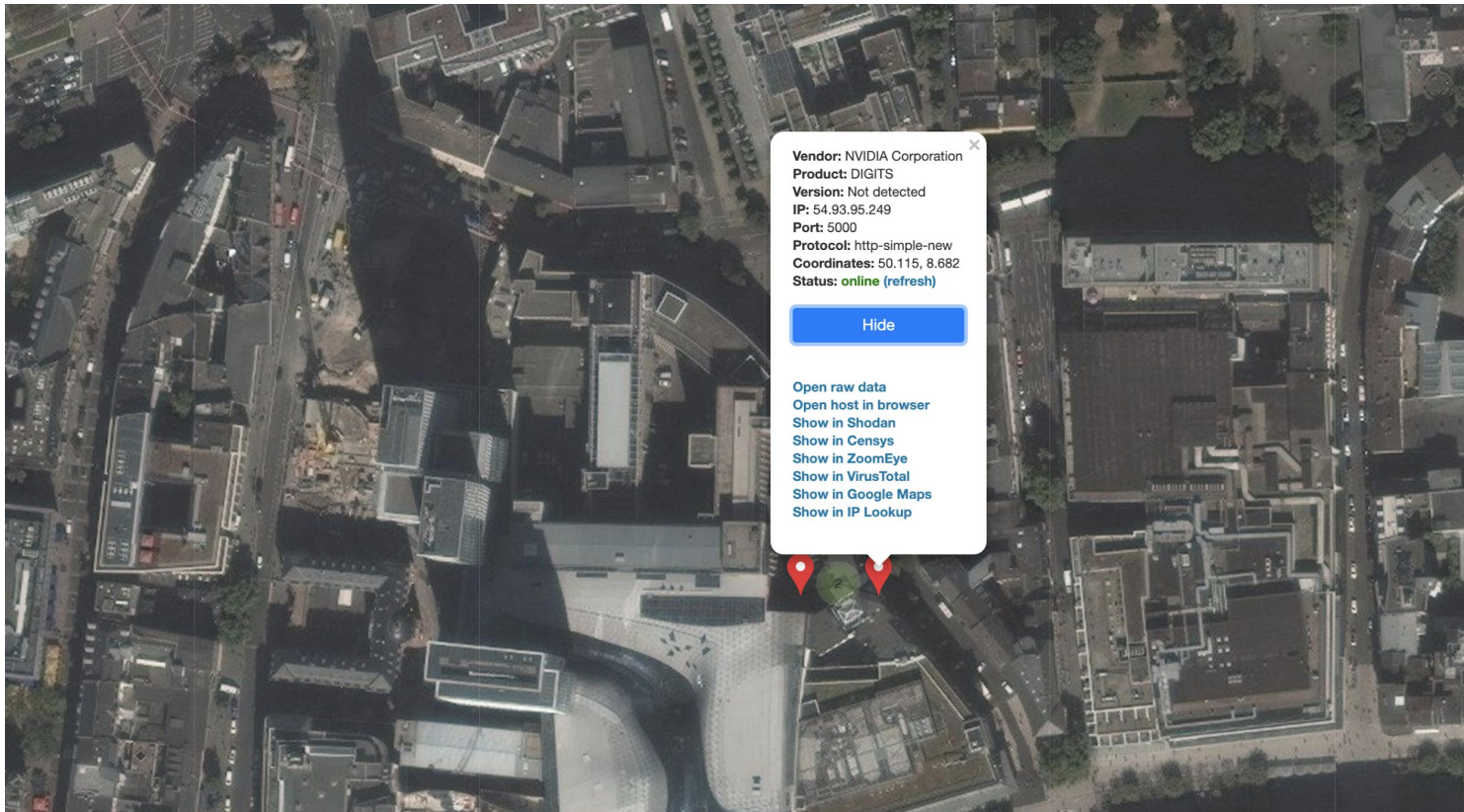


NVIDIA DIGITS



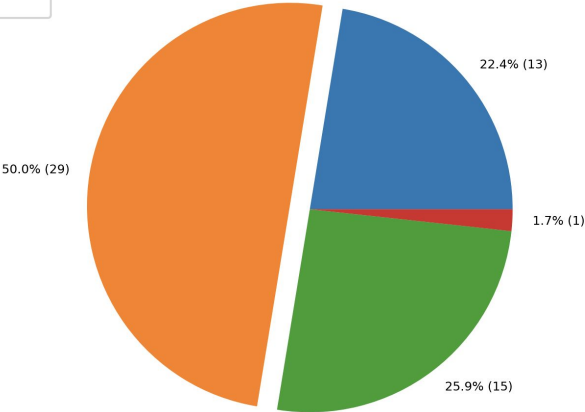
Totally more than 50 results

NVIDIA DIGITS

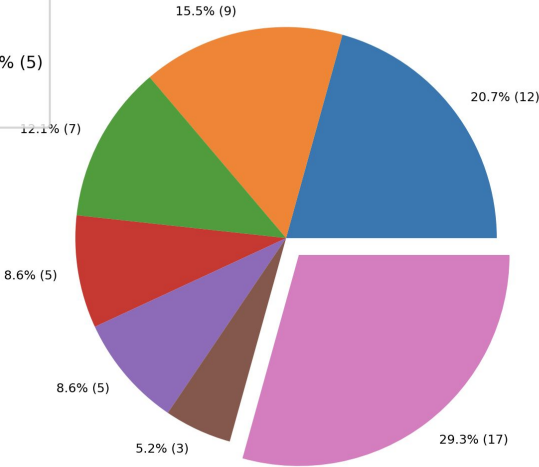


NVIDIA DIGITS

Percentage of nodes by continents

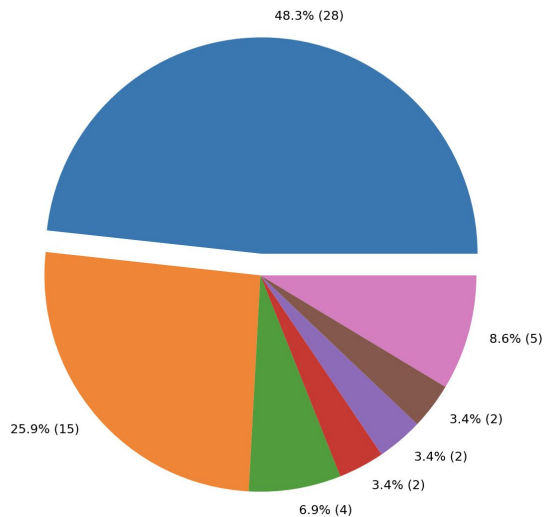
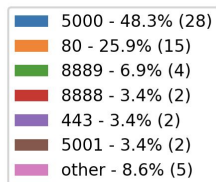


Percentage of nodes by countries

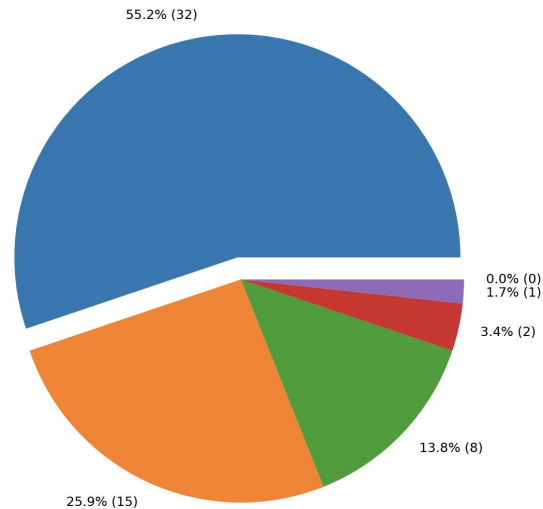
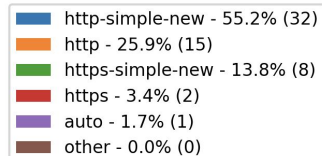


NVIDIA DIGITS

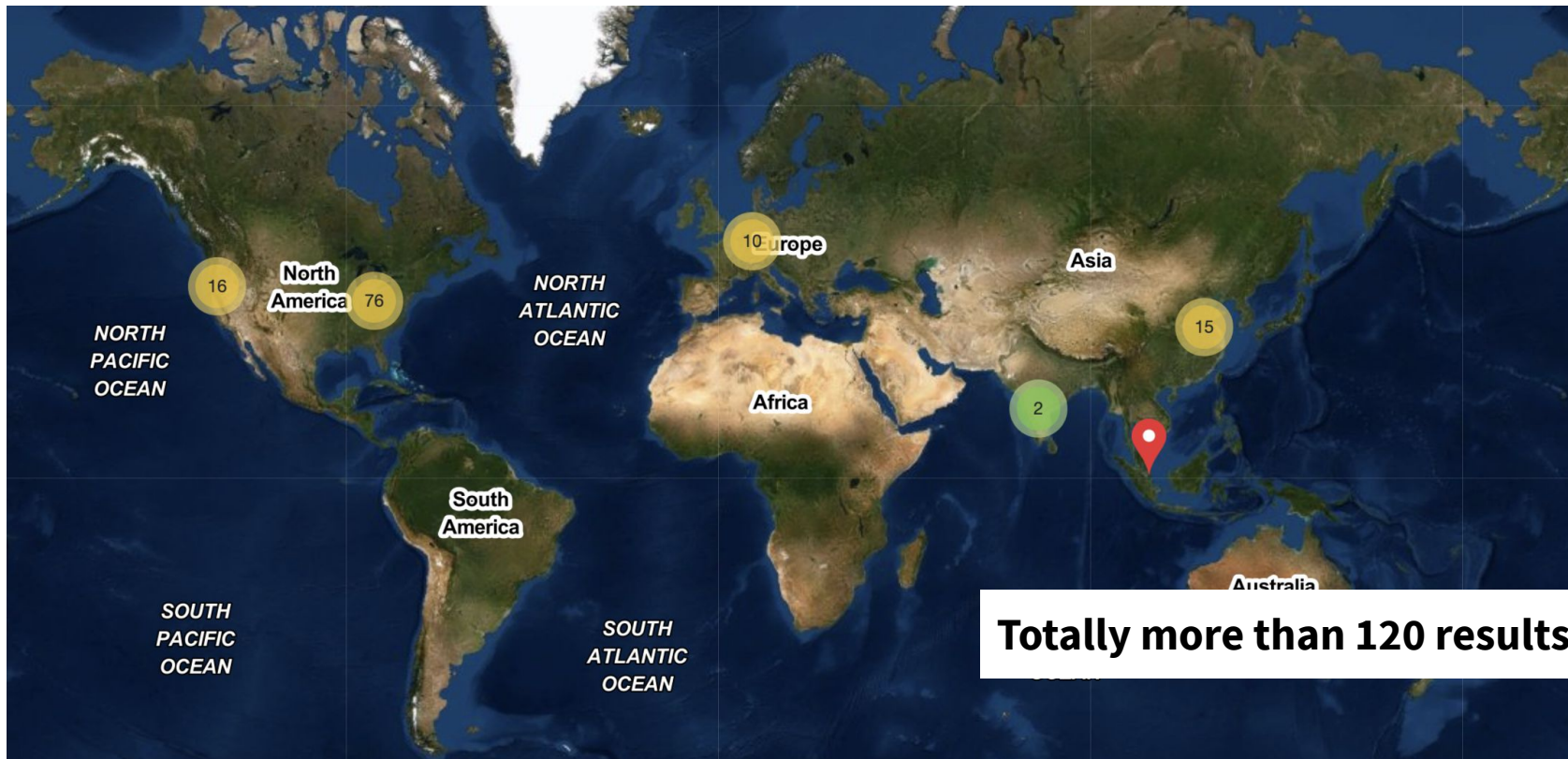
Percentage of nodes by ports



Percentage of nodes by protocols

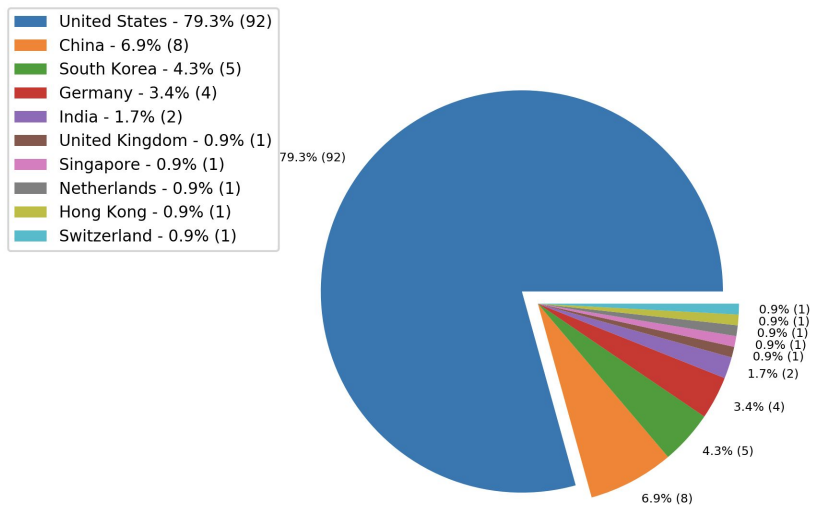


TensorBoard

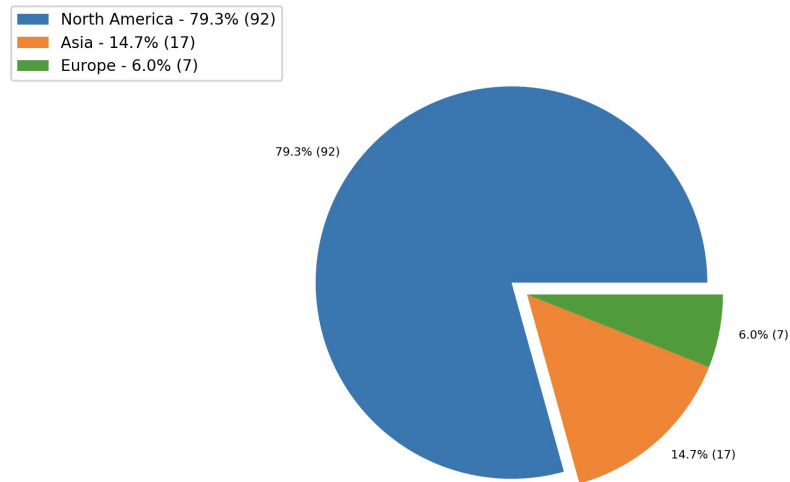


TensorBoard

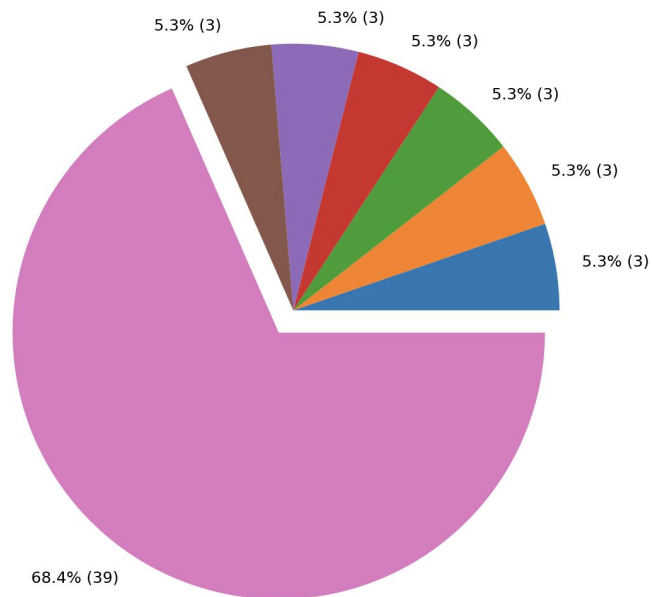
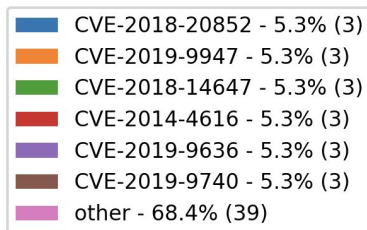
Percentage of nodes by countries



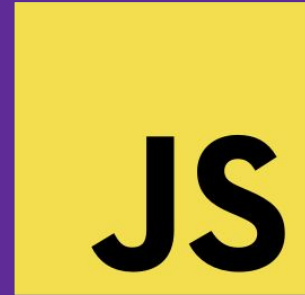
Percentage of nodes by continents



TensorBoard Vulnerabilities



JavaScript Applications

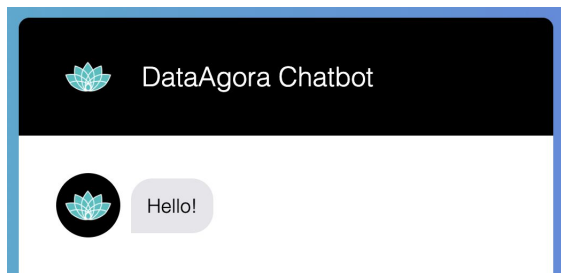


TensorFlow.js and Others

Welcome to TensorFlow.js

TensorFlow.js Object Detection

Выбрать файлы Файл не выбран



Real time Object Detection with Meraki camera

Model loaded - loading snapshot from Meraki MV camera

Your browser does not seem to support getUserMedia. 🙄 This will probably only work in Chrome or Firefox.

Totally more than 1.000 different results were found

MoAir 微信小程序版

Sorry! An error occurred while loading the model 🙄
If you're on an iPhone, please try using Safari.

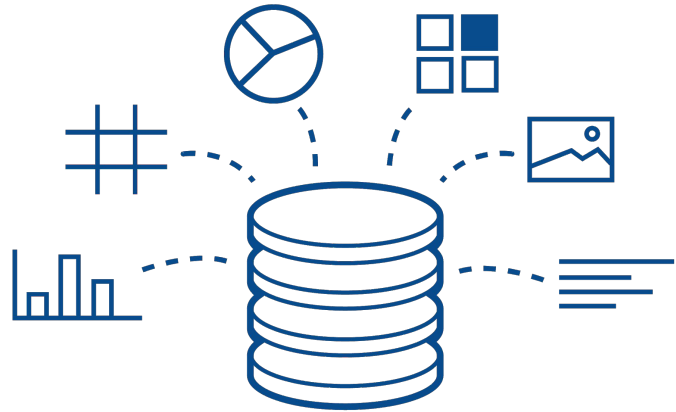
Тренировочные данные	0
Валидационные данные	0
Эпох обучено	0
Ошибка на тренировочных данных	?
Ошибка на валидационных данных	?
Начать тренировку	Стереть модель и начать заново
Нарисовать heatmap	Очистить Heatmap
Скачать датасет с данными	Загрузить датасет

Open Databases with ML Data



Possible Impact

Sensitive Information Leakage: An attacker can gain full access to sensitive information about the system, infrastructure, processes, and system paths. Moreover, the logs may contain personal and private information.



Possible Impact

Information Theft: an attacker can gain access to datasets, tags, and labels with different databases and collections

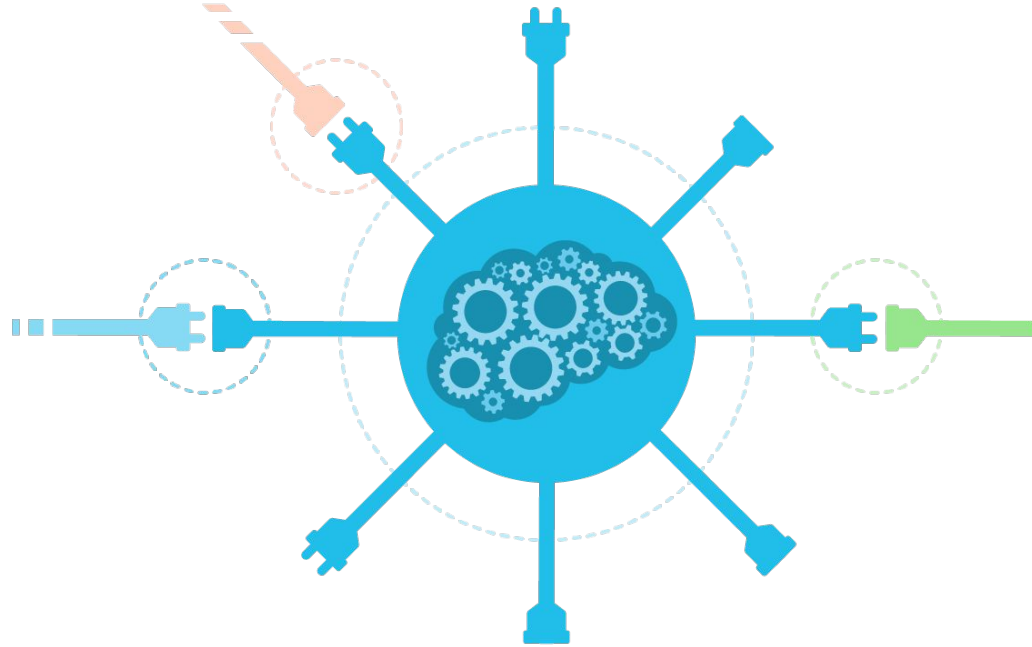


Running Containers

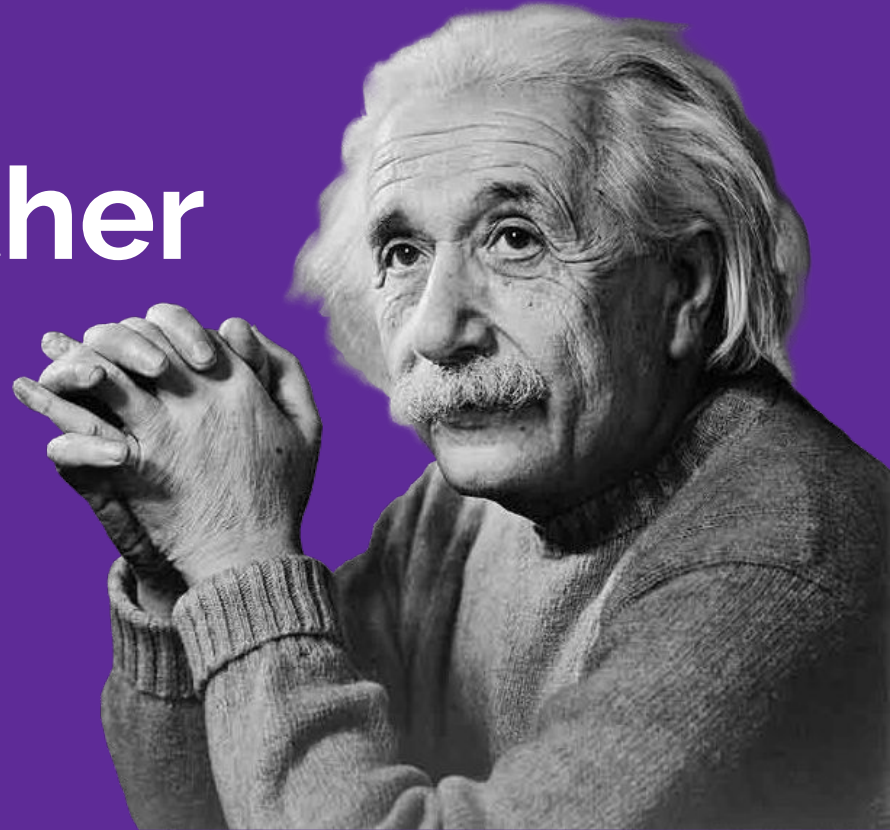


Possible Impact

API Mechanisms Exposure: an attacker can manage remote containers and images; run, delete or stop them

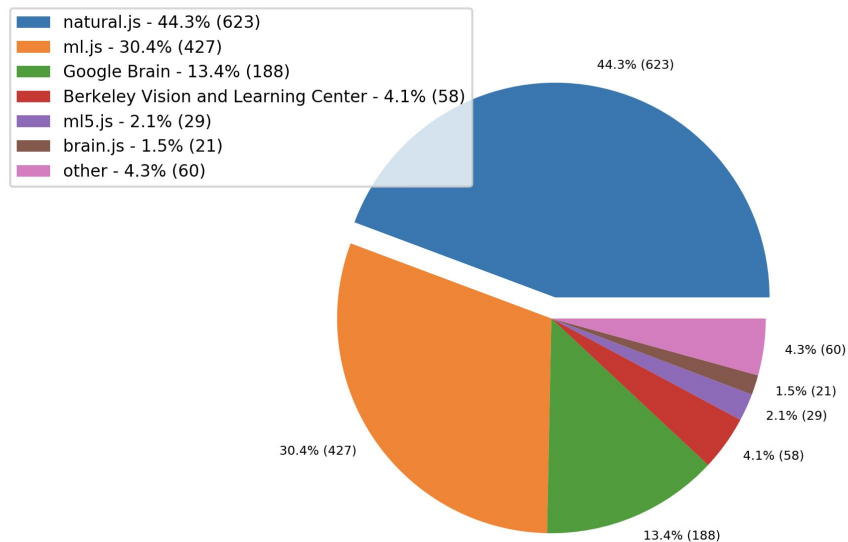


What About Other Applications?

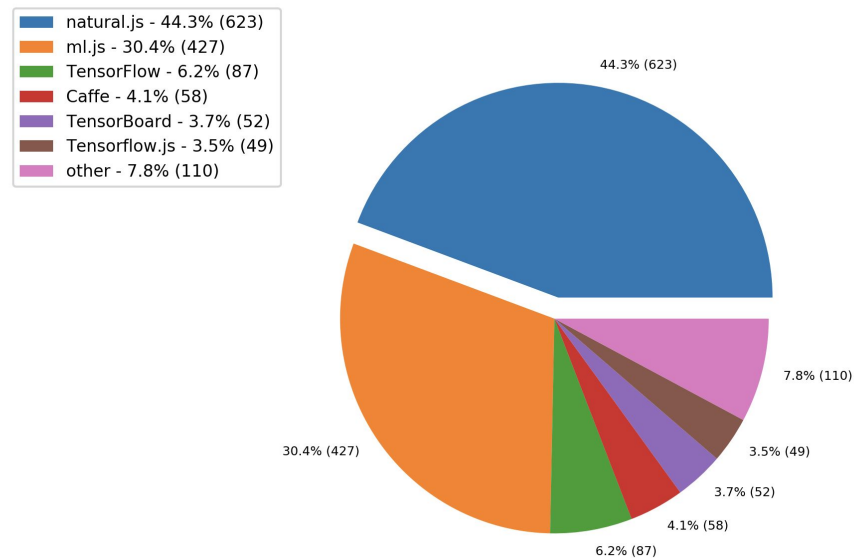


Results (July 2019)

Percentage of nodes by vendors

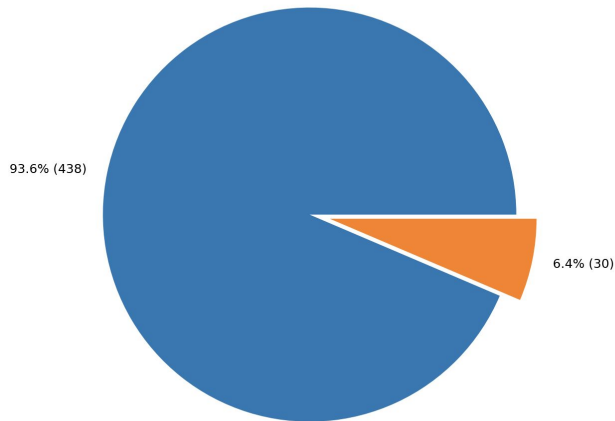
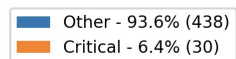


Percentage of nodes by products

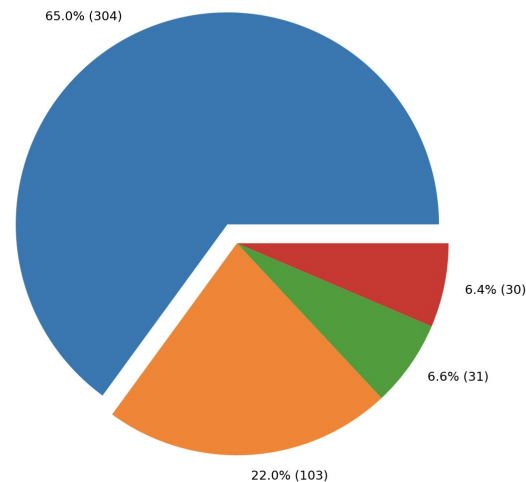


Vulnerabilities (July 2019)

Percentage of critical vulnerabilities

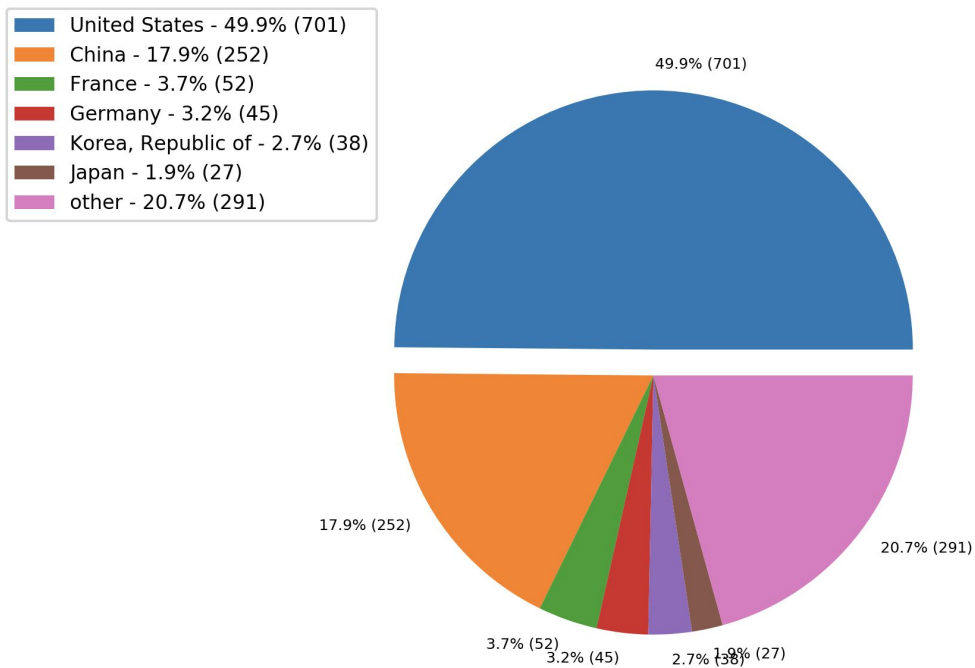


Percentage of vulnerabilities by CVSS v3.0 rating



Distribution by Countries

Percentage of nodes by countries



Results Map



AlFinger Project

The goals of the project is to provide tools and results of passive and active fingerprinting of Machine Learning Frameworks and Applications using a common Threat Intelligence approach and to answer the following questions:

- How to detect ML backend systems on the Internet and Enterprise network?
- Are ML apps secure at Internet scale?
- What is ML apps security level in a general sense at the present time?
- How long does it take to patch vulnerabilities, apply security updates to the ML backend systems deployed on the Internet?



sdnewhop.github.io/AlSec/



github.com/sdnewhop/AlSec

Contributors:

- Sergey Gordeychik
- Anton Nikolaev
- Denis Kolegov
- Maria Nedyak

AlFinger Project Coverage

- Frameworks
 - TensorFlow
 - NVIDIA DIGITS
 - Caffe
 - TensorBoard
 - Tensorflow.js
 - brain.js
 - Predict.js
 - ml5.js
 - Keras.js
 - Figue.js
 - Natural.js
 - neataptic.js
 - ml.js
 - Clusterfck.js
 - Neuro.js
 - Deeplearn.js
 - Convnet.js
 - Synaptic.js
 - Apache mxnet
 - Databases with ML Content
 - Elasticsearch with ML data
 - MongoDB with ML data
 - Docker API with ML data
 - Databases
 - Elasticsearch
 - Kibana (Elasticsearch Visualization Plugin)
 - Gitlab
 - Samba
 - Rsync
 - Riak
 - Redis
 - Redmon (Redis Web UI)
 - Cassandra
 - Memcached
 - MongoDB
 - PostgreSQL
 - MySQL
 - Docker API
 - CouchDB
 - Job and Message Queues
 - Alibaba Group Holding AI Inference
 - Apache Kafka Consumer Offset Monitor
 - Apache Kafka Manager
 - Apache Kafka Message Broker
 - RabbitMQ Message Broker
 - Celery Distributed Task Queue
 - Gearman Job Queue Monitor
 - Interactive Voice Response (IVR)
 - ResponsiveVoice.JS
 - Inference Solutions
 - Speech Recognition
 - Speech.js
 - dictate.js
 - p5.speech.js
 - artyom.js
 - SpeechKITT
 - annyang
- ... and many more

Thanks for Attention. Got Questions?



@dnkolegov



@manmoleculo



github.com/sdnewhop/grinder



sdnewhop.github.io/AISec/

