>

> #JudgementDay14

> AI for CyberSecurity in the World of Encryption

> 06-11-19

>

>

>

>

> Petr Somol

> Head of Cognitive Research Team at Cisco Systems

> Research Fellow, Czech Academy of Sciences

>

> wget https://scholar.google.com/citations?user=&user=GYuMvRMAAAAJ

Team Background

- **Solved projects for**
  - U.S. Army – Network Security SW (Cognitive)
  - U.S. Navy – Network Security SW (Cognitive)
  - U.S. Air Force – Autonomous Flight Agents Cooperation (Univ. project)
- **10+ years experience in**
  - **Mathematics**
    - Optimization, Game Theory
  - **Computer Science and Artificial Intelligence**
    - Modeling, Statistical Recognition, Search Algorithms, Agent Systems
  - **Data Science**
    - Data Mining, Data Representation, Streaming Data Analysis!

Now a team of **~15 scientists** in engineering role with **~10 student interns**, addressing theoretical and practical problems in cybersecurity across Cisco ATS.

Threat prevalence we see

Economic activity and value creation is moving online. So is crime: **56% of fraud** incidents cyber related *(England&Wales, 2017)* · Cyber crime to hit **$6 trillion** in 2021, up from $3 trillion in 2015 · **$93B** spent on Defense in 2018

For sample report see

http://cognitive.cisco.com

ML in Network Security – Taxonomy

„**KNOWN-KNOWN**“ threats

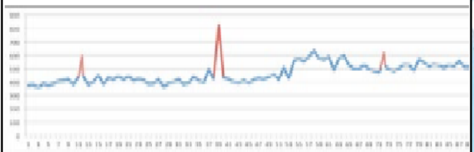
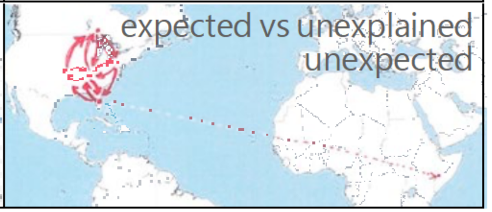
Detect the exactly known infections, as seen before

„**KNOWN-UNKNOWN**“ threats

Detect previously unseen variations of known threats, sub-families or related new threats

„**UNKNOWN-UNKNOWN**“ threats

Detect zero-days unrelated to any known malware

	Threat type vs suitable Detection technique				
	Static Signatures	**Dynamic Signatures**	**Behavioral Signatures**	**High-Level Patterns**	**Unsupervised Anomalies**
What it does	Exact matching of predef ned character- or numeric sequences. Def nitions human readable. Manual def nition, possibly tooling-assisted. *(Remark: form of extremely overtrained ML)*	Matching of predef ned rules. Def nitons human readable. Manual def nition, possibly tooling-assisted. *(Remark: form of strongly overtrained ML model.*	Matching of machine learned rules (e.g., regex) or recognition of machine learned behavioral patterns (vector representations of events) in transformed feature space. Applicable through Supervised machine learning.	Very high level patterns, machine learned to distinguish generic malicious behavior. (cf. signal discoverability). Great task for Semi-supervised machine learning.	Cases signif cantly distant to all known normal behavior (machine learned). Distance measures can be highly abstract. Unsupervised machine learning.
Expect	• Very High Precision. • No generalization (exact matching) • Good explainability • Does not scale • Requires manual def nition.	• Very High Precision • Generalization limited (variations exactly encoded) • Finds variations explicitly covered by the pattern • Good explainability • Requires manual def nition.	• High Precision • Generalizes based on similarity to known malware. Great to f nd previously unseen variations/ subfamilies of known infections. • Good explainability. • Learned (semi)auto from data.	• Good Precision. • High recall. Scales well. • Findings may be dif cult to attribute to known infections = explainability limited. • Good chance to f nd true 0-days	• Low Precision. • Possibly best recall. Best chance to f nd true zero-day. Scales well. • Explainability dif cult. • Learned from data
Example	domain name associated to trojan: • `server1.39slxu3bw.ru`	• `regex: .*/i[a-z]-(ready|rinoy|gnfoh)`	Redrom, -2 sample patterns • `hxxp://crazyerror.su/b/opt/8681BAE3DB3A2F9D446CD5E3` • `hxxp://50.63.147.69:8080/b/req/3D111E6B21F373015C646CA4`	generic suspicious traf c: 	

Technique Trade-Of

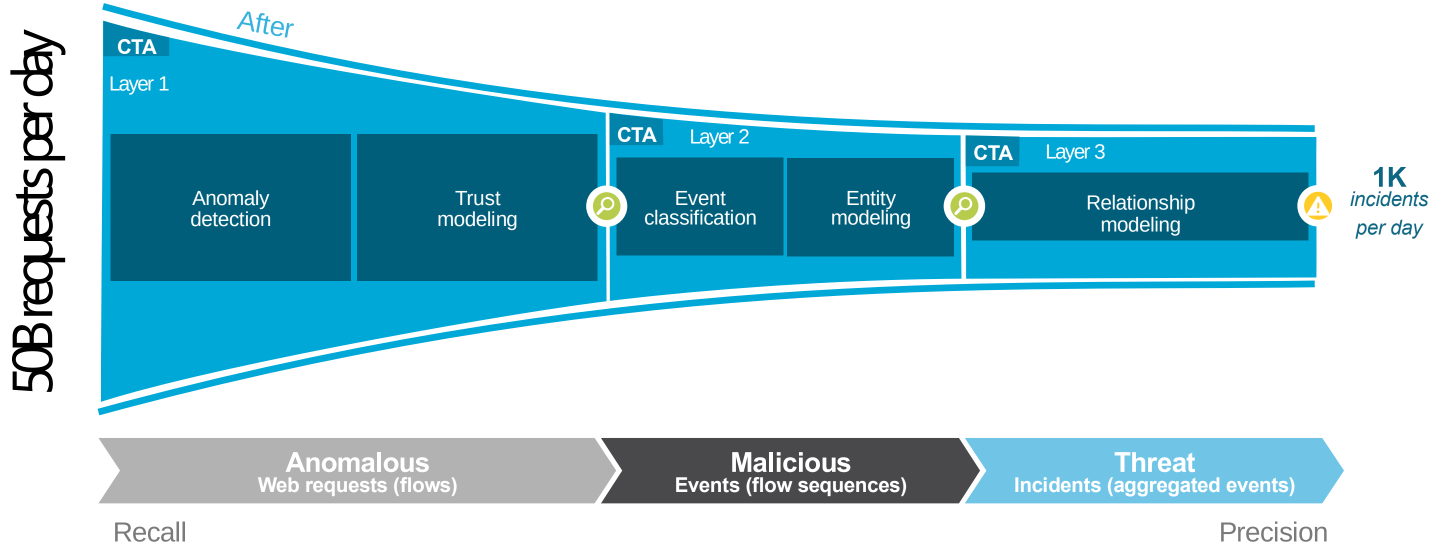
← Better Precision and Explainability, simplicity of Proof

Better Recall, Scalablity, applicability to encrypted data, ability to detect Zero-days →

Cognitive Intelligence - Network Analytics Architecture

Proxy Logs *or NetFlows*

Features	Example Value
x-elapsed-time	1405089360000
c-ip	10.0.0.1
cs-username	jhonson
c-port	32000
s-ip	66.196.65.112
s-port	443
cs-url	https://s.yimg.com/zz/combo?yui:/3.12.0/yui/yui-min.js&/os/mit/td/a
cs-bytes	320
sc-bytes	436
sc-body-size	345
cs(User-Agent)	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
cs-mime-type	application/javascript; charset=utf-8
cs-method	GET
sc-http-status	200
cs(Referer)	https://uk.yahoo.com/?p=us
sc(Location)	

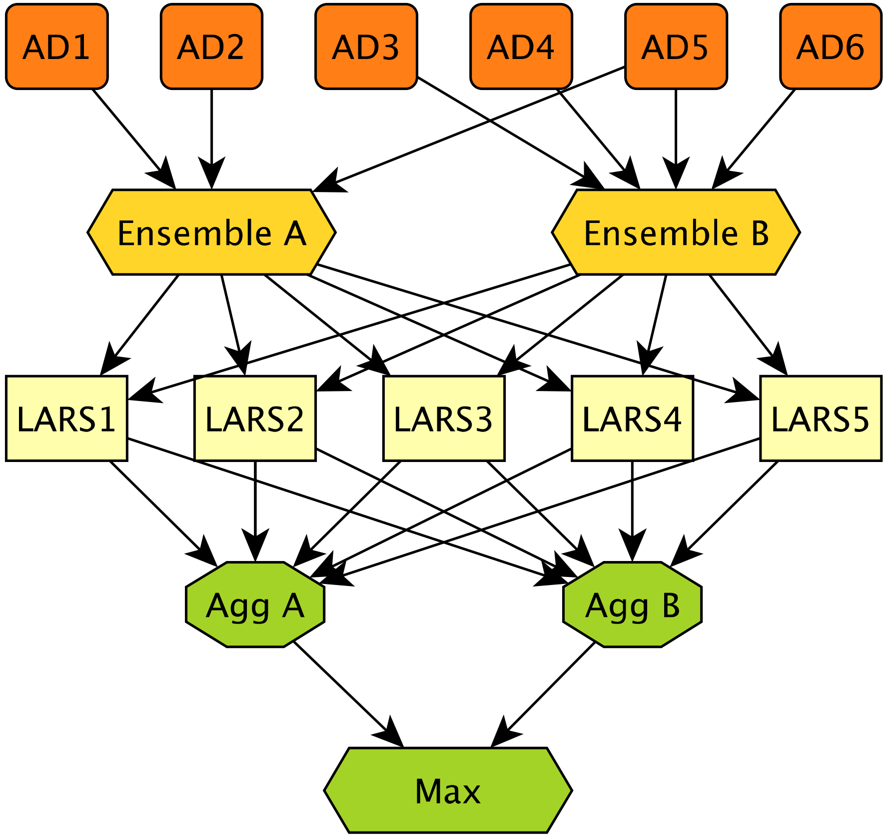


ML models w.r.t. whole Internet - speed over accuracy

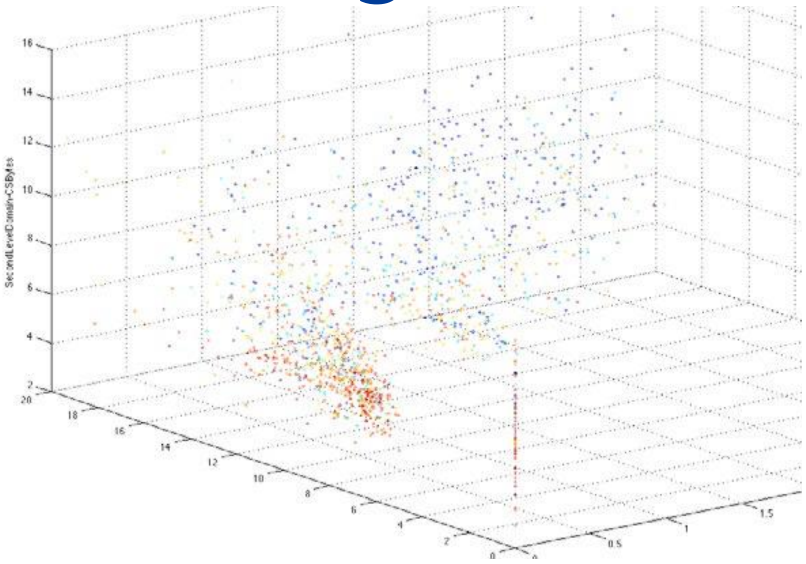
…

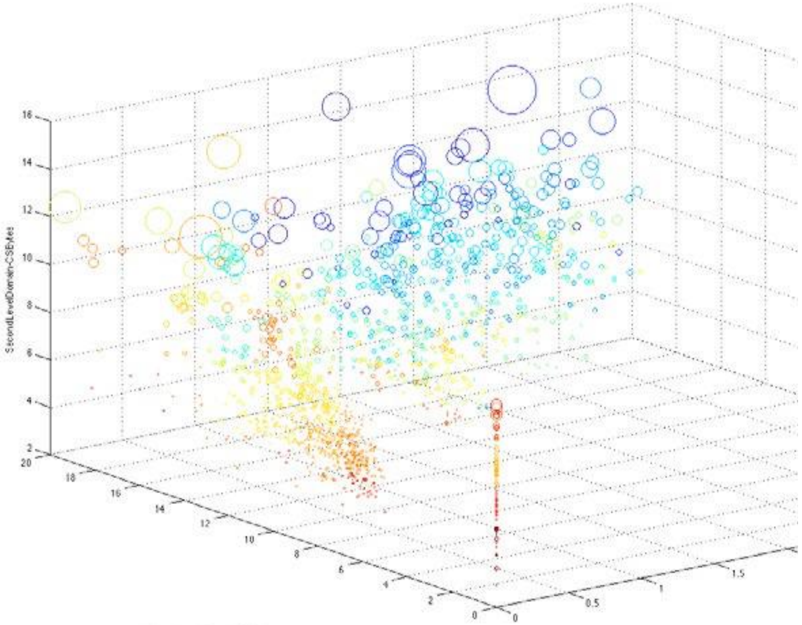
ML models on suspicious traffic - accuracy over speed

Anomaly Detection Architecture with Denoising

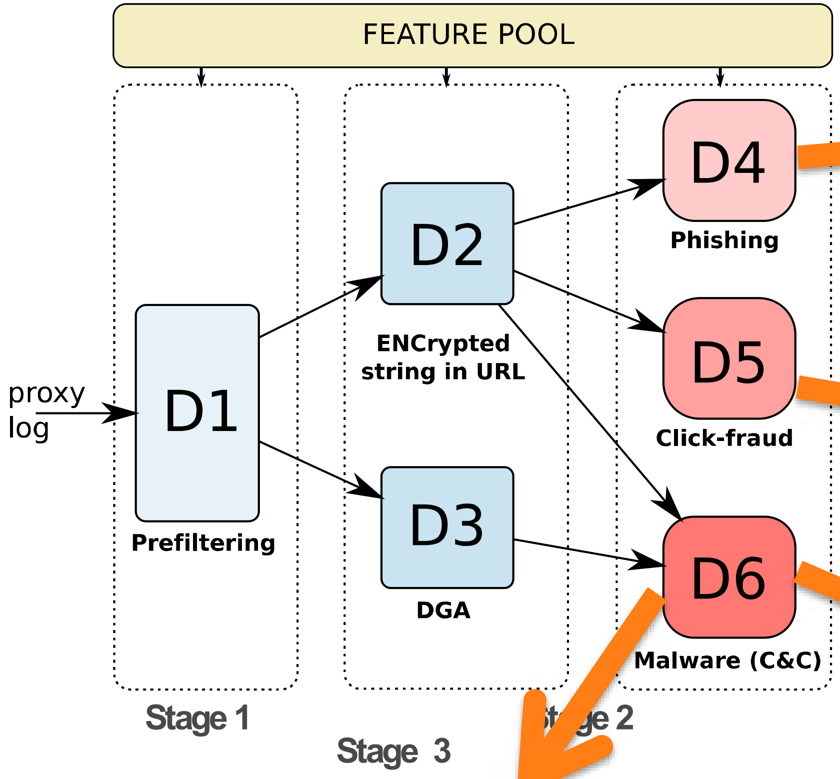


	AUC
Individual Anomaly Detectors	**0.72** (±0.27)
Individual Ensembles of Anomaly Detectors	**0.94** (±0.14)
Individual LARS Models	**0.96** (±0.07)
Final Aggregation	**0.98** (±0.04)





Data Driven Classif er Architecture



malicious
hxxp://cohostro[.]com/keyJjIjogMjM4MiwgImYiOiAwLCAibSI6IDI2M..
hxxp://coclouderx[.]com/peyJjIjogMjUyOCwgImYiOiAwLCAibSI6IDI3..
hxxp://adminxhost.com/8a766814986811e486083c4a92db07ce

malicious
hxxp://findreek[.]com/cen?ag=de6b7f fbf8a767e8bdecbb805143bca6-2..
hxxp://199.182.165[.]105/c.php?i=DFuwjK oDUiUNzF8Qnn%2F%2FQw..
hxxp://clickered[.]com/cex?si=94b2ba8b0b59787b4609c64514baa26c-81-0
hxxp://180.149.131[.]33/v.php?q=252043836&callback=jQuery11020...
hxxp://lookfunnel[.]com/lr?si=362edf9becb1bf79713d1cf131936afb-18-0

malicious
hxxp://lkckclckl1i1i[.]com/zKG2ZB1X6M5xt5c1Y2xrPTEuNyZiaWQ9..
hxxp://109.235.54[.]162/m/IbQEZVVjipFdkB0KHeNkNuGBabgSr2z3..
hxxp://78.140.164[.]160/jjlqXpP/ ← GIja7A3q/KqRSx+1s8kNC=/%2BsI..
hxxp://masterproweb[.]net/images2/BD3006FB490CADF111E40696D3..
legitimate
http://www.thespec.com/DependencyHandler.axd/L0Rlc2t0b3BNb2R1b..
http://www.degruyter.com/assets/virtual/H4sIAAAAAAAAAKWSwUo..
http://www.1001pneus.fr/ls/YToxNzp7czo0OiJwYWdlIjtzOjY6InNlYX..

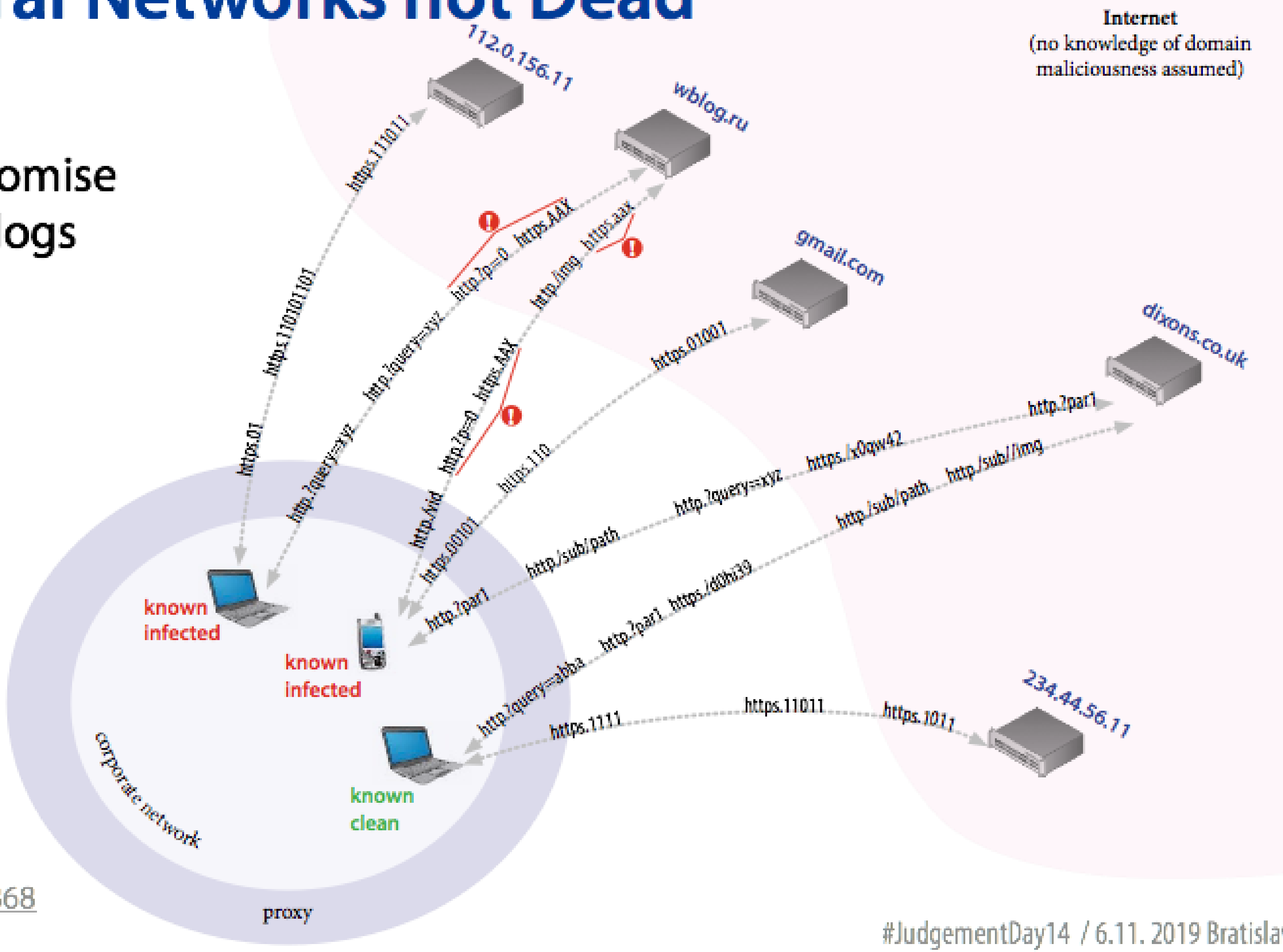
malicious
hzmksreiuojy[.]in, b9qmjjys3z[.]com, jaoohqvqda[.]ru, oqjiwef12egre6erg6qwefg312qrgqretg132[.]com, lkckclckl1i1i[.]com, xjpakmdcfuqe[.]nl, reqblcsh[.]net, cilavocofer[.]eu
legitimate
skhhtcss.edu.hk, edkowalczyk.com, blkdmnds.com, watdoejijbijbrand.nl, kdnlrklb.com, abcdefgtfddf2223.com, llanfairpwllgwyngyllgogerychwyrndrobwll-llantysiliogogogoch.com

Shallow Neural Networks not Dead

Learning behavioral
Indicators of Compromise
from HTTP(s) proxy logs

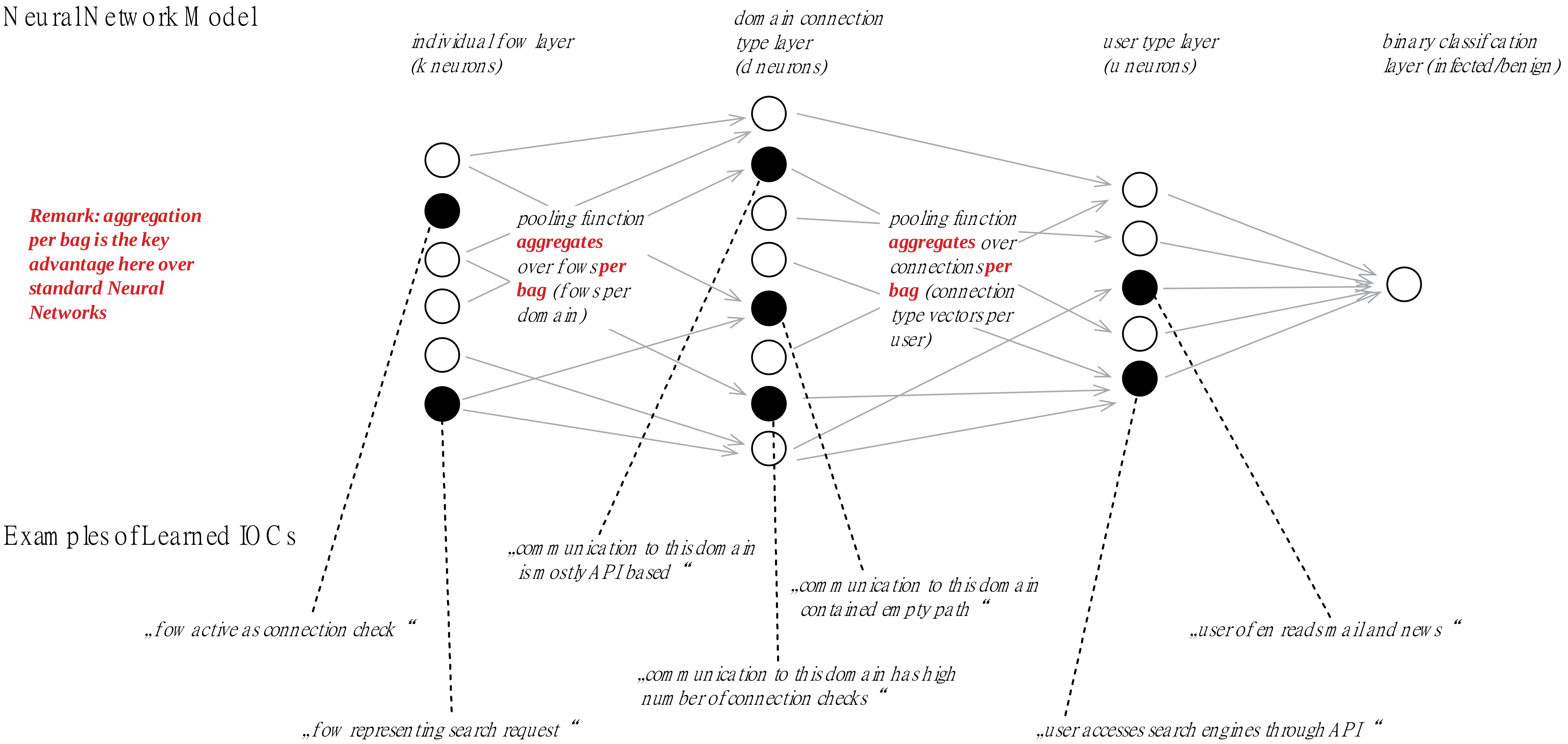
using

Multiple Instance
Learning (MIL)
Neural Networks



cf. Tomas Pevny:
https://arxiv.org/abs/1703.02868

Shallow Neural Networks not Dead (cont.)



Remark: interpretation of learned neuron is possible in afer-learning phase through subsequent analysis of fows on which learned neurons excite the most.

MIL Neural Network - Learned IoC Examples

HTTPs connections to raw IP addresses like

- hxxps://62.249.33.21/

DGA domains like

- hxxp://ivdyxgqtwqsztopjrijlnhqwcnbtk.com,
- hxxp://pojxofukqskfhajvizdhmdxwwghq.biz
- hxxp://twwkgihmmvspblrnzpnjnhexcqgtkrk.com

HTTPs connections to live.com domain like

- hxxps://roaming.officeapps.live.com/

Download of images like

- hxxp://www.biglots.com/images/aprimo/common/holiday_header/110714-04.gif

Malware-specific traffic

- hxxp://95.211.188.129/ZsSgh+/IjxG@wJQuQs/_y%24Z@B&kc
- hxxp://76.119.58.221/ts1V+V6g44Q/sL8PMB/hml+%2D/s%24@9LQI7%24
- hxxp://78.129.153.15/W3S.T7JgR+/S+~@R/SNV%7EL%7E+/p%2C
- hxxp://195.162.107.7/02s1S+5m/s%266/K@wxE/LCeg/0SlQ
- hxxp://165.124.106.26/H3+9UsS/QW1_rI/8JPn_qQgS.@/%26NScFY

Seemingly legitimate traffic like

- hxxp://banners.itunes.apple.com/js/banner-main-built.js
- hxxp://www.slfn.co.uk/today_matchsheet.php

Detection Dif culty High and Growing

- Internet-size scale learning… model robustness still a problem where labels are scarce
- Privacy vs. security trade-of chellenge

data size

- *known learning methods do not scale enough. (we now process 50TB/day, need Feature Selection on 400k-dim etc)*
- *we routinely break well-known ML &BigData libraries by sheer data size on massive CPU-pools*

visibility

- *encyption · TLS 1.3 · GDPR*
- *Application-level encryption*
- *DNS over HTTPS or TLS*
- *use of ML by malicious actors – ease of obfuscation, hiding, evasion…*
- *evolution of attack vectors (eg f leless..) - past knowledge quickly obsolete*

Way Forward - the Power of Complementarity

Content / Files / Memory

endpoint system activity · execution patterns · phishing · ransomware · patterns in disassembled structure…

Telemetry + Enhanced Analytics techniques (ETA)

f leless attacks · c&c activity · data exf ltration · phishing · attribution by association · malicious infrastructure discovery…

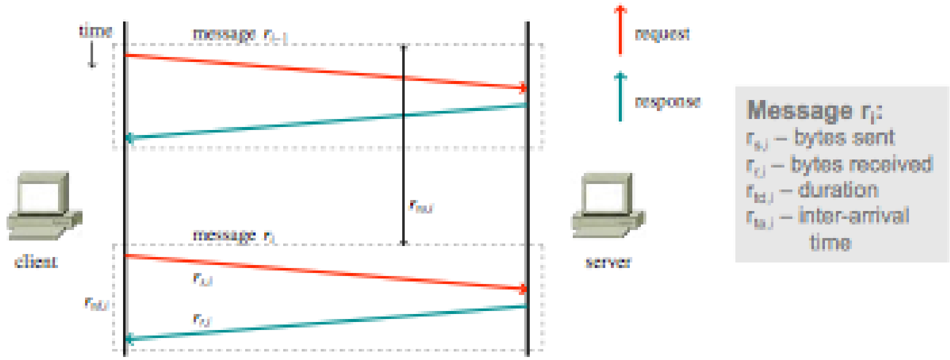
Asynchronous Intel

sandboxing · shared intel platforms · global stats · RiskMaps (e.g. WhoIs inference)…

Analytics on Weak / Encrypted Signal

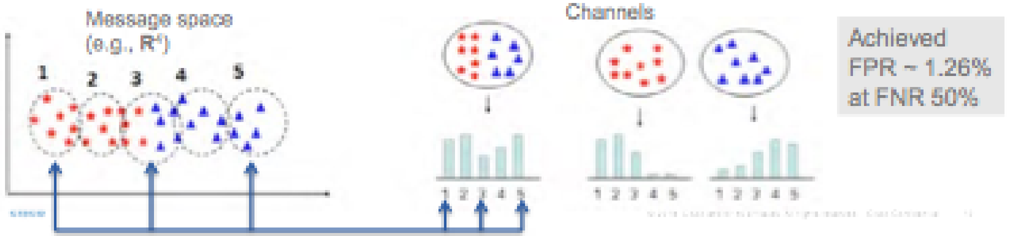
NetFlow only

Modeling Communication Channels



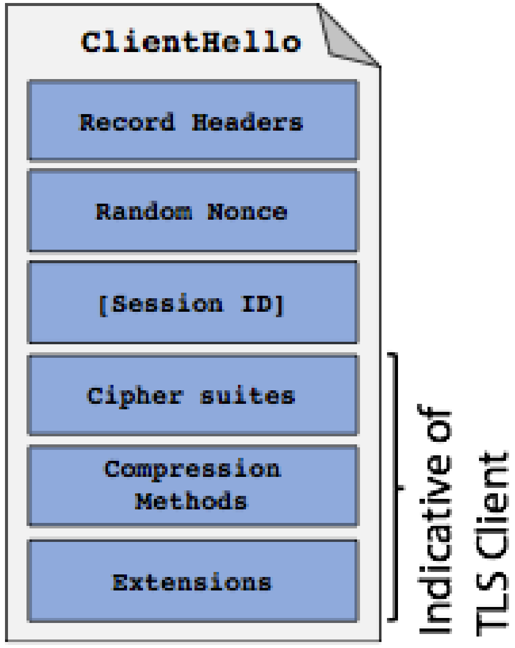
GMMs - Bag of Prototypes (Tomas Komarek)

- Find prototypes of messages in the original feature space
  - components of the GM model
- Prototypes found using Gaussian Mixture Models and EM algorithm
- Channel represented by histogram of used prototypes



NetFlow + Encrypted Threat Analytics

- Initial Data Packet
- TLS Objects
- Sequences of Packet/App Lengths + Byte Distr.

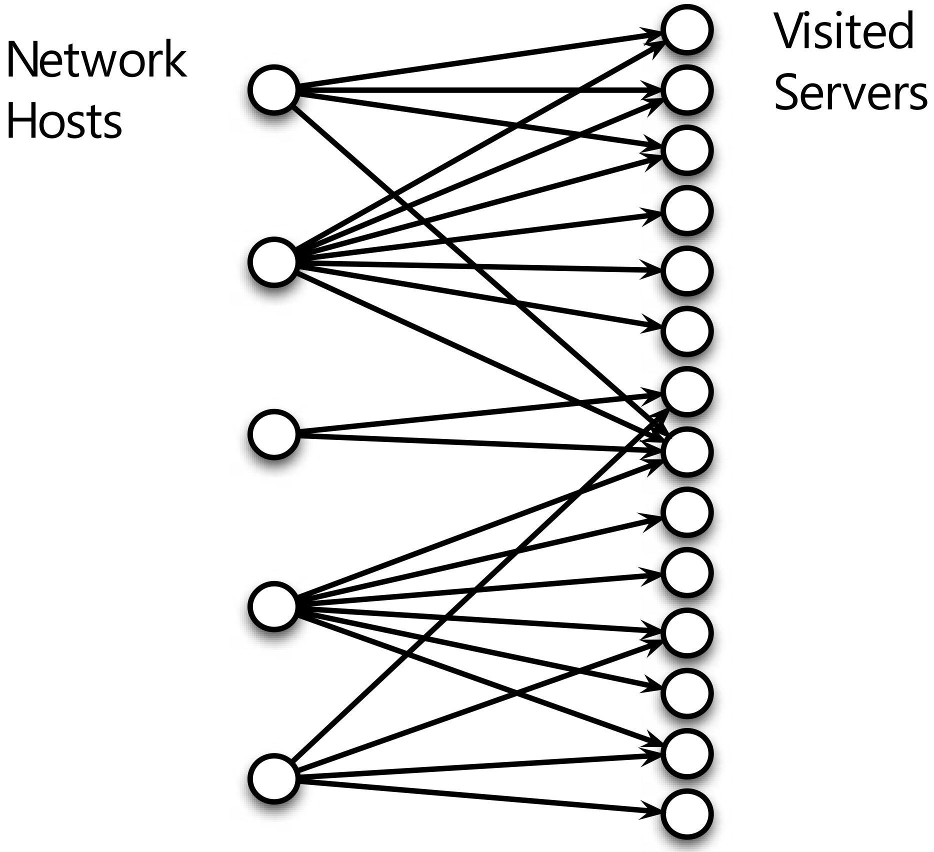


courtesy Blake Anderson

TLS Fingerprinting

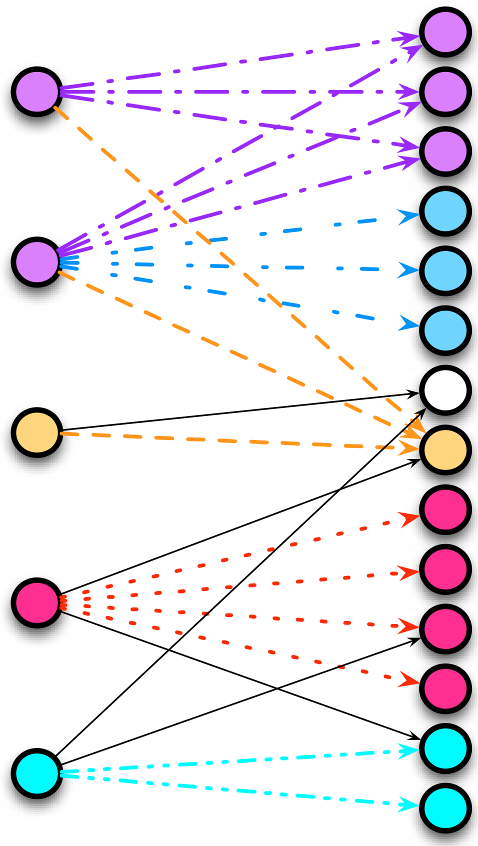
- map TLS traffic to applicaton/lib - connect endpoint and network intel
- utilize global data
- enrich features for learning preditors

Modeling „Social" Relationships



Modeling „Social“ Relationships

Infected Hosts detected by CTA



Servers featuring anomalous activity

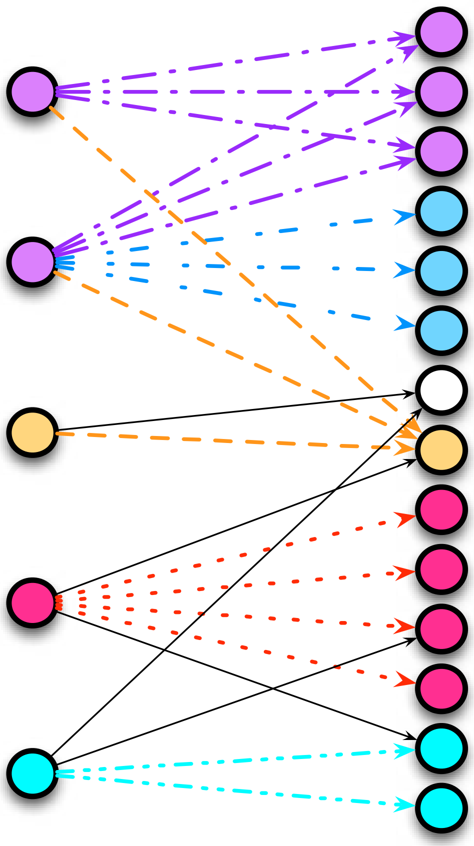
Hundreds of thousand of second level domains (many more servers)

Billions of requests towards these servers

Servers can be grouped into thousands of behavioral clusters

Modeling „Social“ Relationships

Infected Hosts detected by CTA

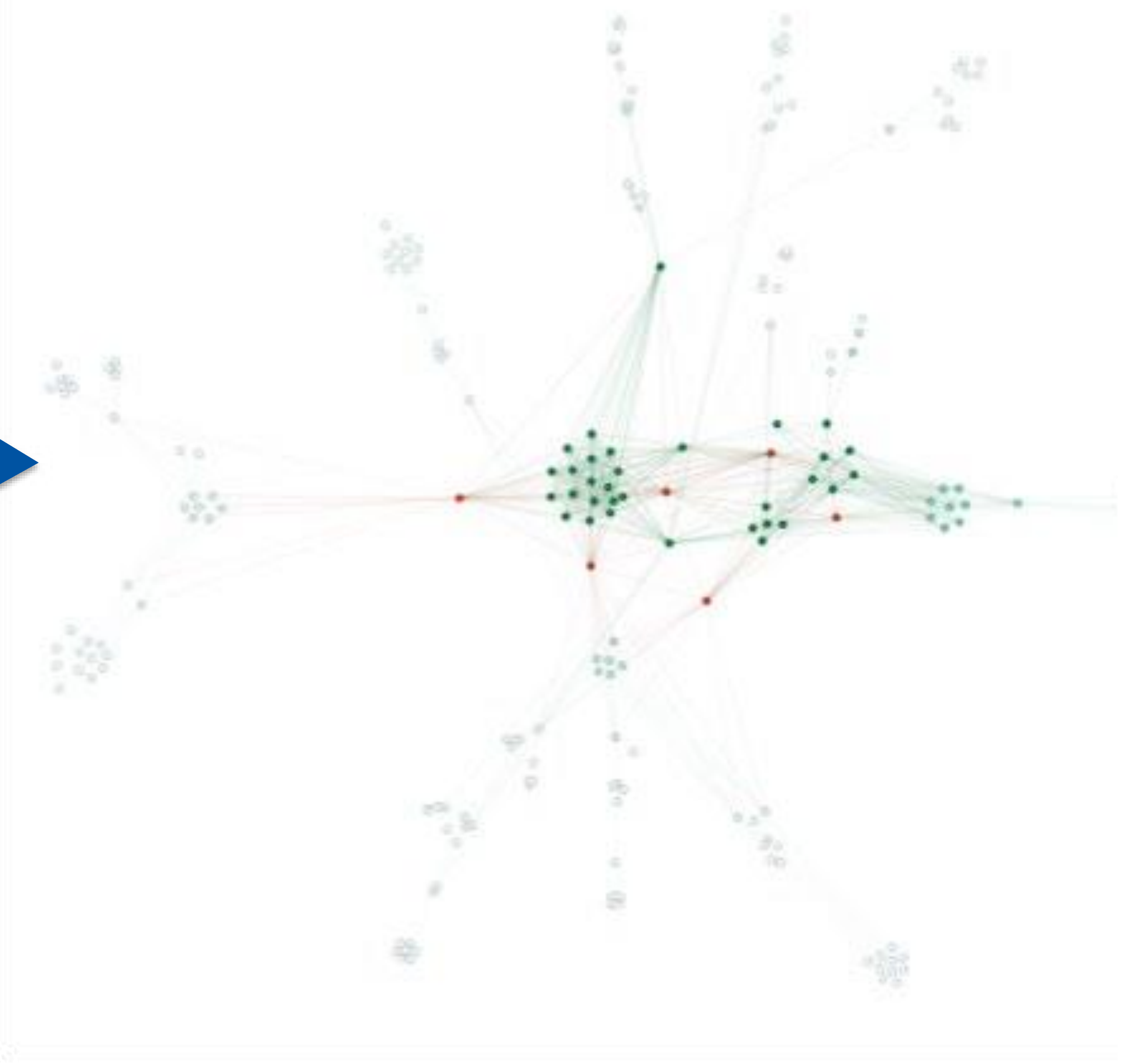


Servers featuring anomalous activity

Hundreds of thousand of second level domains (many more servers)

Billions of requests towards these servers

Servers can be grouped into thousands of behavioral clusters



Global Risk Map

- Behavioral statistics for millions of servers on the Internet
- Tracking servers likely becoming part of an attack
- Risk prof ling

Unlike reputation DBs may not be interpretable easily - designed as input for learned predictors that combine many weak indicators

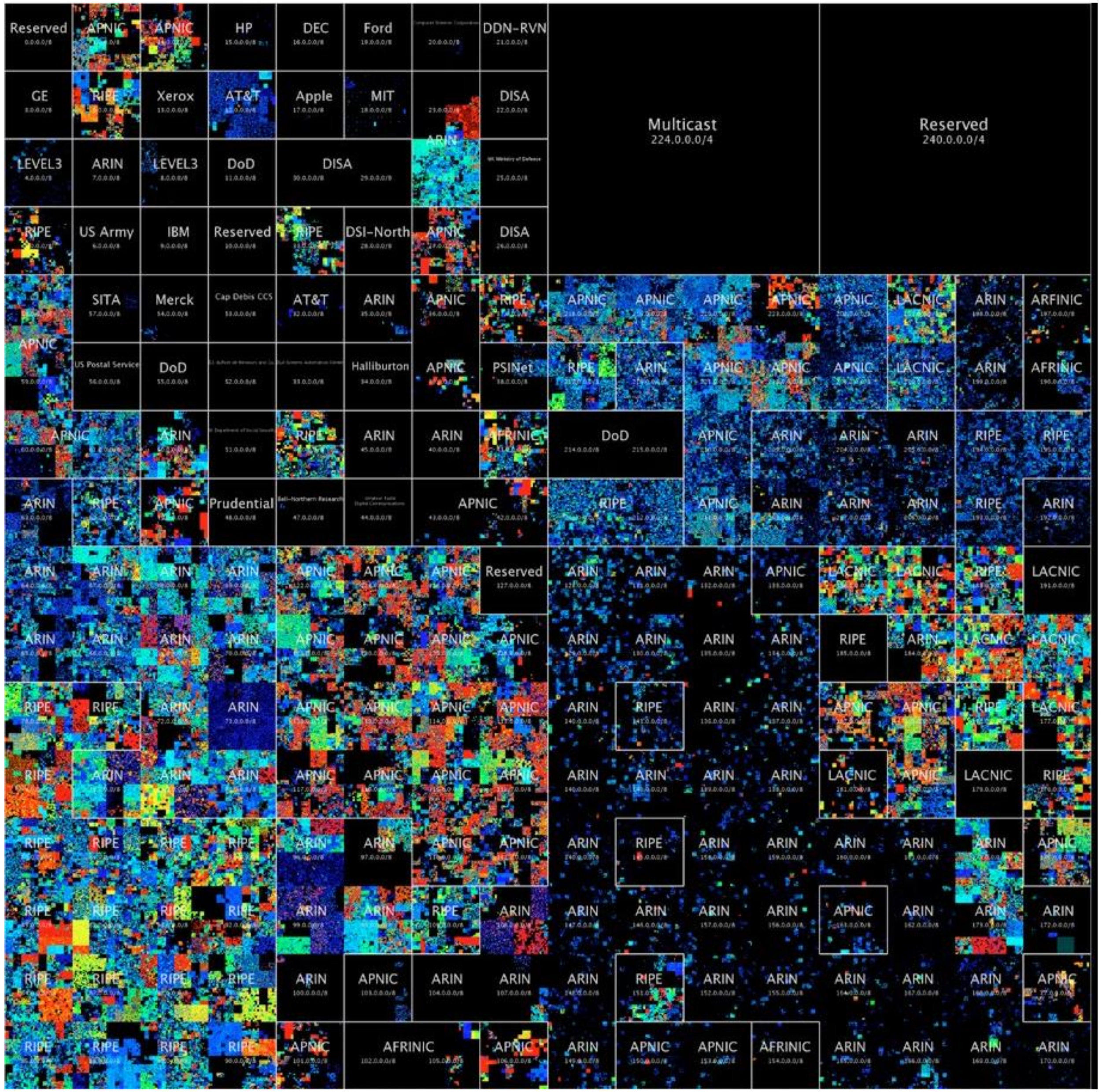


Image: http://census2012.sourceforge.net/images.html

Where We Are

- per-product working solutions, now integrating to boost detection capabilities...

StealthWatch

ETA switches, routers

Cognitive Intelligence

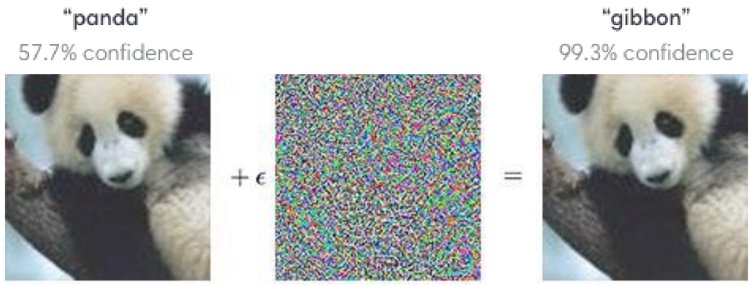
Cisco Threat Response (CTR)

AMP portfolio

ThreatGrid

Tetration

- abundance of open problems across industry



https://blog.openai.com/adversarial-example-research/

adversarial learning

advanced anti-evasion

privacy-preserving learning

concept drift

representation learning

Tech Resources
(sample)

- Package for capturing and analyzing network f ow data: https://github.com/cisco/joy
- Library for learning from massive data: https://github.com/cisco/oraf

- Encypted Telemetry Analytics Technology Overview: https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html
- Behavior Disovery in Encrypted Traf c: http://agents.fel.cvut.cz/stegodata/pdfs/Pev15-ICASSP.pdf, https://arxiv.org/pdf/1607.01639.pdf, US Patent US 2019 / 0230095 A1, etc.
- MIL Neural Networks for CyberSec: https://arxiv.org/abs/1703.02868
- CNN and LSTM Neural Networks in CyberSec: https://arxiv.org/pdf/1906.09084.pdf
- Preventive Blacklisting from WhoIs: http://www.approximateinference.org/accepted/LetalEtAl2015.pdf

Thank you

Q & A