

50 Thousand Needles in 5 Million Haystacks

Understanding Old Malware Tricks to Find New Malware Families

Veronica Valeros, Karel Bartoš, Lukáš Machlica

{vvaleros, kbartos, lumachli}@cisco.com

Cognitive Threat Analytics

Cisco Systems, Inc.



Veronica Valeros

Malware Researcher
Threat Intel Analyst

Co-Founder MatesLab
Hackerspace (ARG)

@verovaleros



Karel Bartoš

Network Security
Researcher

PhD Candidate CS
ČVUT (CZ)

kbartos@cisco.com



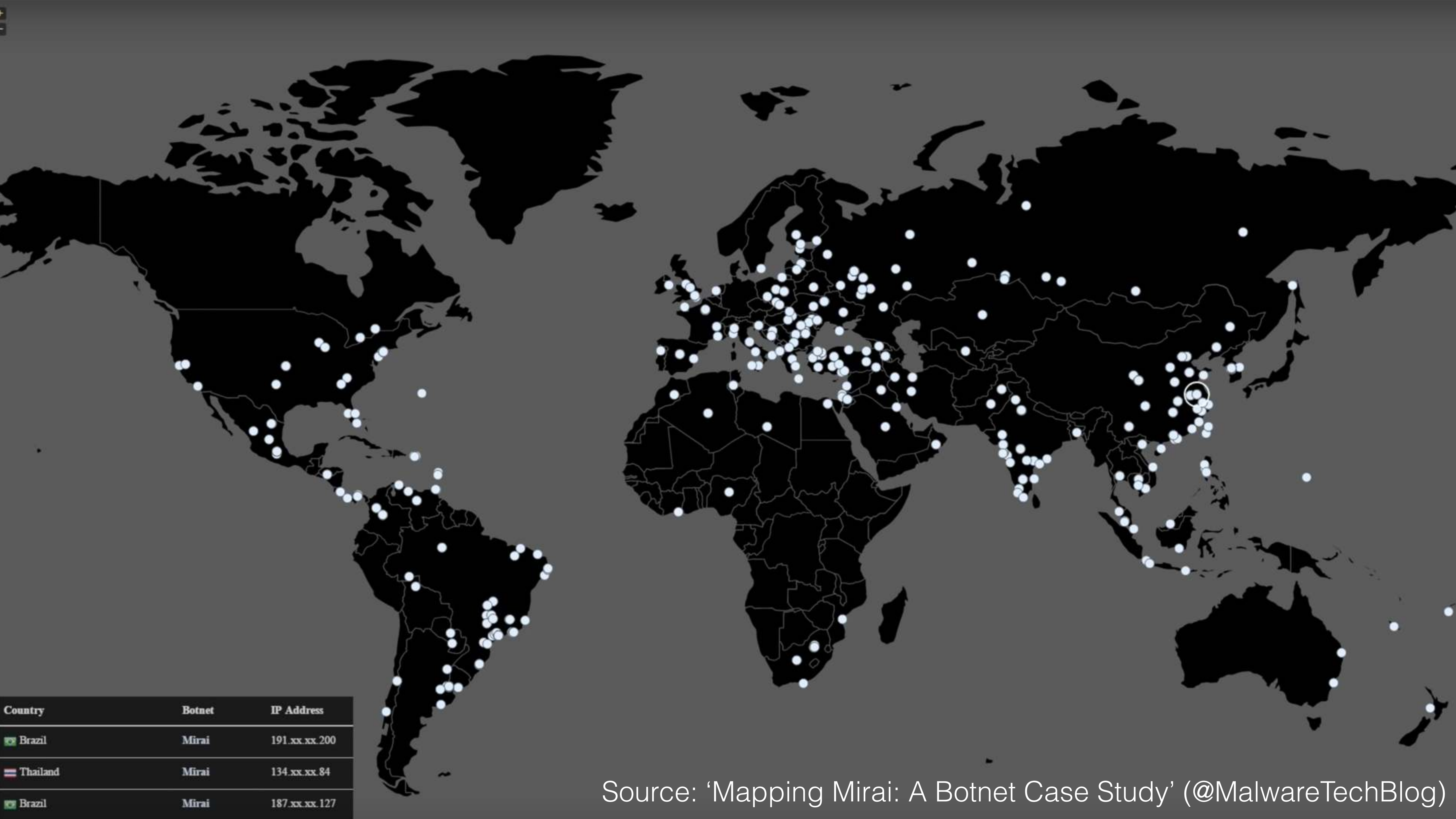
Lukáš Machlica

Network Security
Researcher

PhD in Cybernetics
ZCU (CZ)

lumachli@cisco.com





Country	Botnet	IP Address
 Brazil	Mirai	191.xx.xx.200
 Thailand	Mirai	134.xx.xx.84
 Brazil	Mirai	187.xx.xx.127

Source: 'Mapping Mirai: A Botnet Case Study' (@MalwareTechBlog)



admin:admin



Country	Botnet	IP Address
 Brazil	Mirai	191.xx.xx.200
 Thailand	Mirai	134.xx.xx.84
 Brazil	Mirai	187.xx.xx.127

Source: 'Mapping Mirai: A Botnet Case Study' (@MalwareTechBlog)

CONGRATULATIONS!

en chosen to receive a
away Desktop Computer!

m 4 Processor 2.66 GHz
R-SDRAM, 80GB HD, 48x CD-RW
or CRT Monitor (18-inch viewable)

o Claim Your FREE* Desktop Computer!

FREE!



Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel

Setting Started Features Contact Us Help In

ents

Black
Roule
Slot M

Internet

games live, for Fun or Real Money. Chat with Others. 25% Deposit Bo

Online Poker Room T... http://ads1.revenue....

AdWare Punisher

Scan Settings Privacy Recovery

Type	Item	Details
☒ Spyware	cashtoolbar.com	Spyware cookie - cashtoolbar.com
☒ Spyware	hitexchange.net	Spyware cookie - hitexchange.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	fastclick.net	Spyware cookie - fastclick.net
☒ Spyware	mediaplex.com	Spyware cookie - mediaplex.com

Save log Save susp. Select all Select

Checking IE cookies

Sun 4/12/2015 11:55 AM

Internal Revenue Service

[!!Spam KSE]Payment confirmation

To [REDACTED]

Attachments confirmation_75991792.doc (58 KB); AT

Dear taxpayer,

You are receiving this notification because your tax r
Please find attached a copy of the approved 1040A f
On the last page, you can also find the wire transfer

Transaction type : Tax Refund
Payment method : Wire transfer
Amount : \$7592
Status : Processed
Form : 1040A

Additional information regarding tax refunds can be
Please note that IRS will never ask you to disclose pe

Regards,
Internal Revenue Service
Address: 1111 Constitution Avenue, NW
Washington, DC 20224
Website: <http://www.irs.gov>
Phone: 1-800-829-1040

YOUR COMPUTER AND FILES ARE
YOU MUST PAY 0.2 BITCOINS TO UNLOCK
YOUR FILES HAVE BEEN MOVED TO A HIDDEN PART OF YOUR COMPUTER
ESSENTIAL PROGRAMS IN YOUR COMPUTER WILL NOT FUNCTION
AND YOUR COMPUTER WILL NOT FUNCTION
— 0 —
ONCE YOUR BITCOIN PAYMENT IS RECEIVED
FILES WILL BE RETURNED TO NORMAL



WARNING!

Your personal files are encrypted!

CRYPT
nts were encrypted!

YOUR BITCOIN PAYMENT ADDRESS
1G6tQeWw6TU1qu

[COPY THE ADDRESS]
[CONFIRM PAYMENT BELOW]
IF YOU DO NOT HAVE BITCOINS VISIT
IF YOU HAVE MADE THE BITCOIN PAYMENT CHECK

I MADE PAYMENT
PLEASE VERIFY
AND UNLOCK MY COMPUTER

BBC

BBC iD

Menu

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

University pays \$20,000 to ransomware ~~hackers~~ ACTORS

🕒 8 June 2016 | Technology

🔗 Share

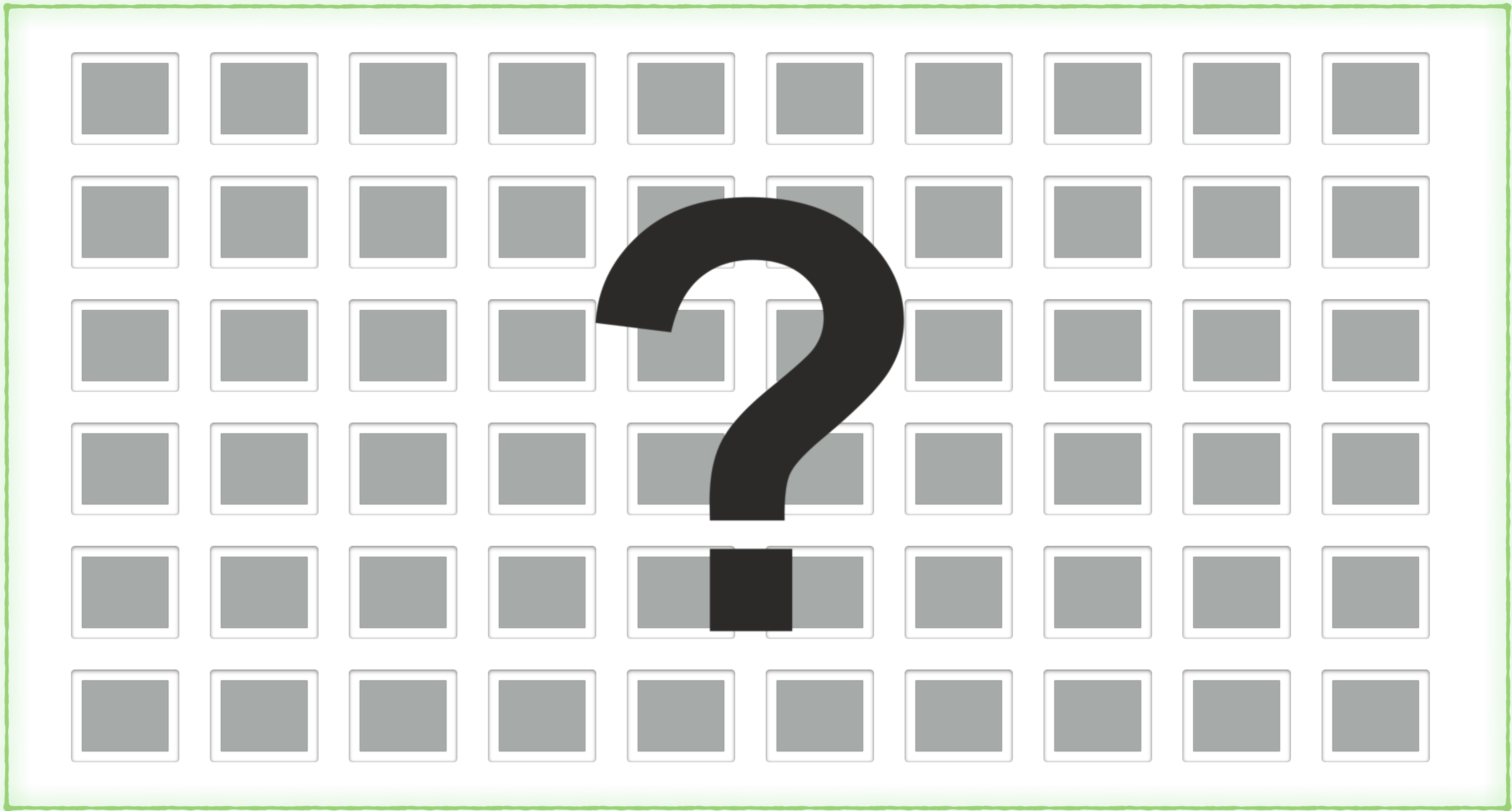
JIGSAW RANSOMWARE

-code!
our special

file.

encrypted forever)

destroy or damage your files!







“Need to communicate” > Our competitive advantage

“Need to communicate” > Our competitive advantage

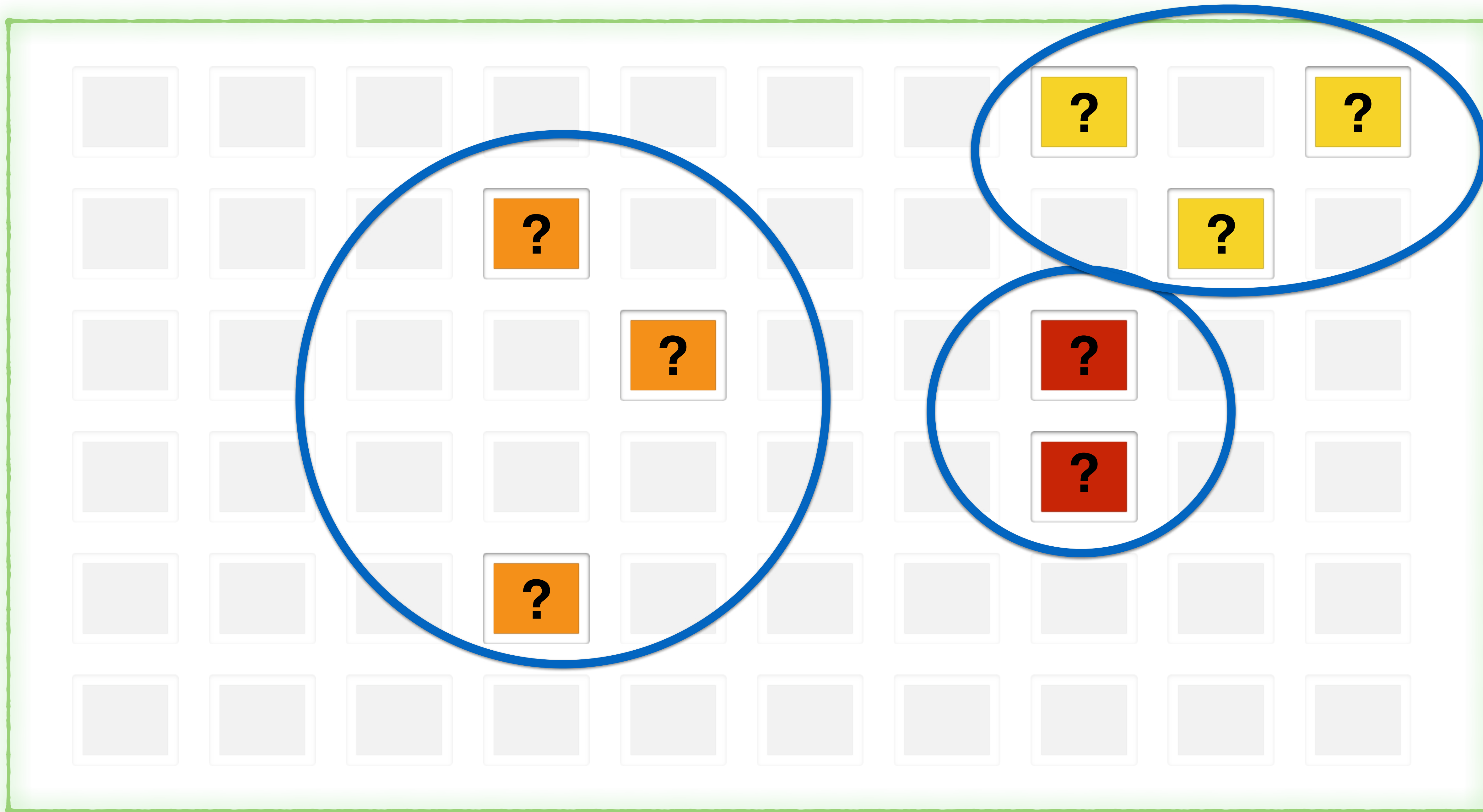
Big Data is no longer a problem nor a challenge

“Need to communicate” > Our competitive advantage

Big Data is no longer a problem nor a challenge

Machine Learning give us the perfect mechanism

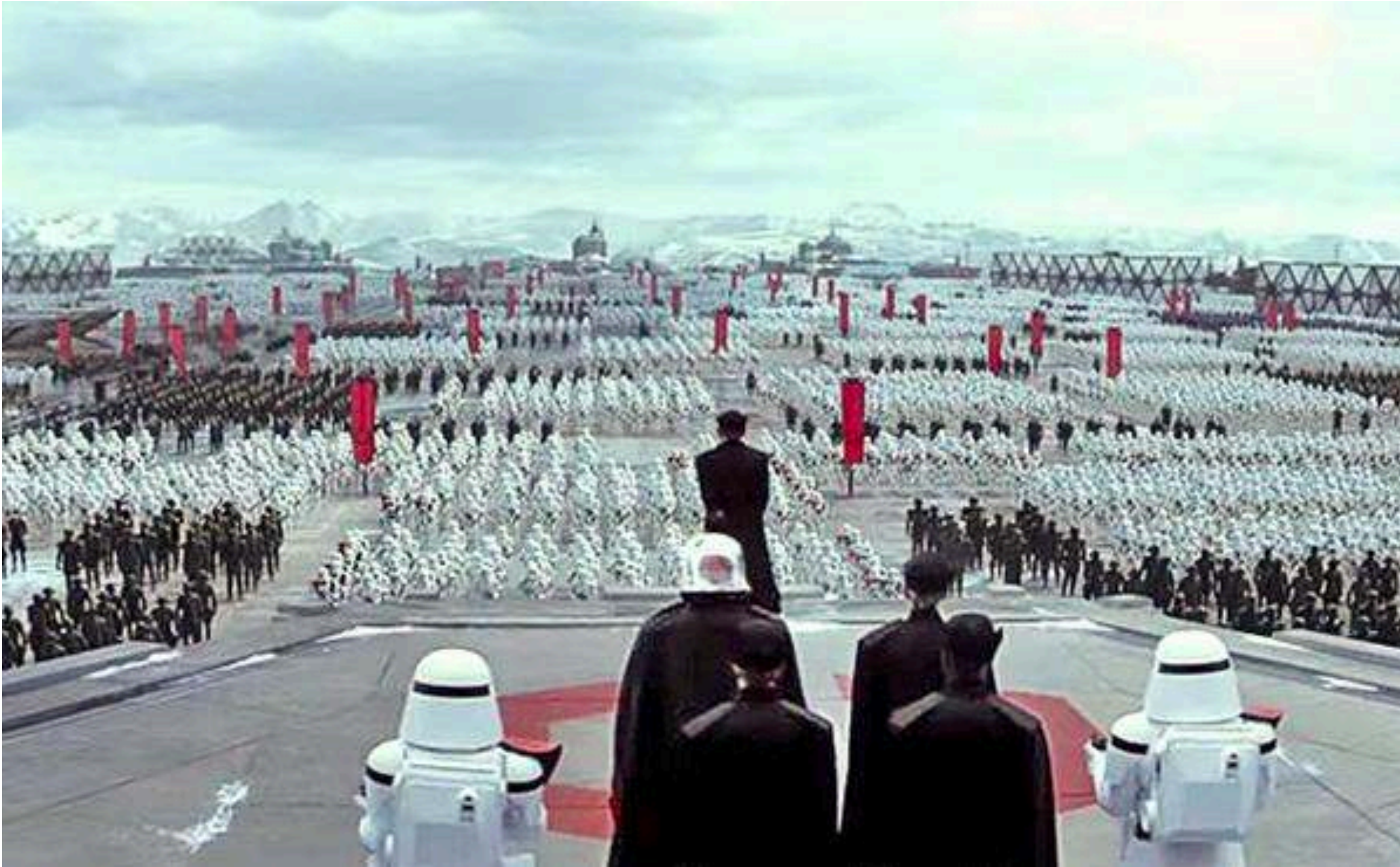
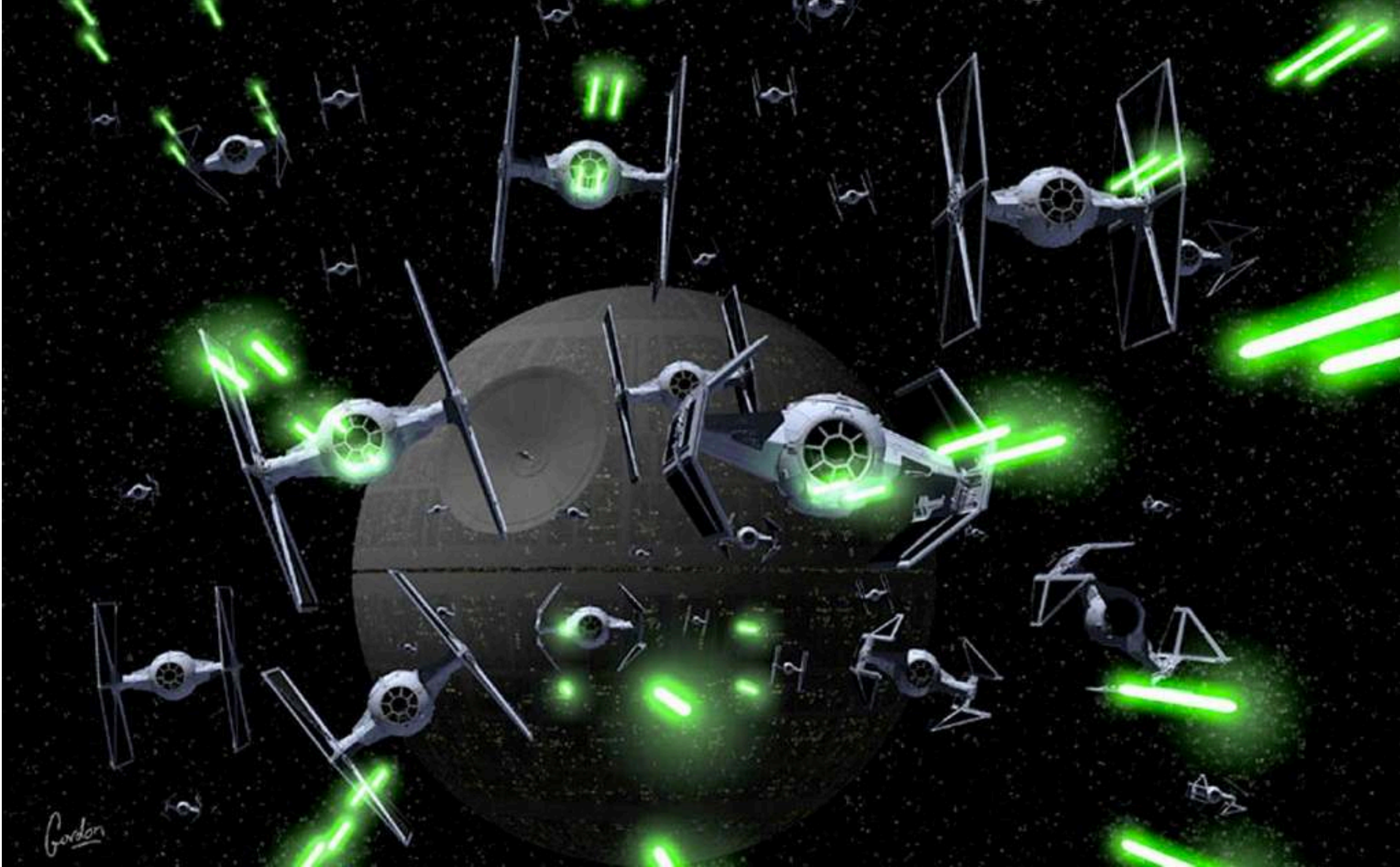




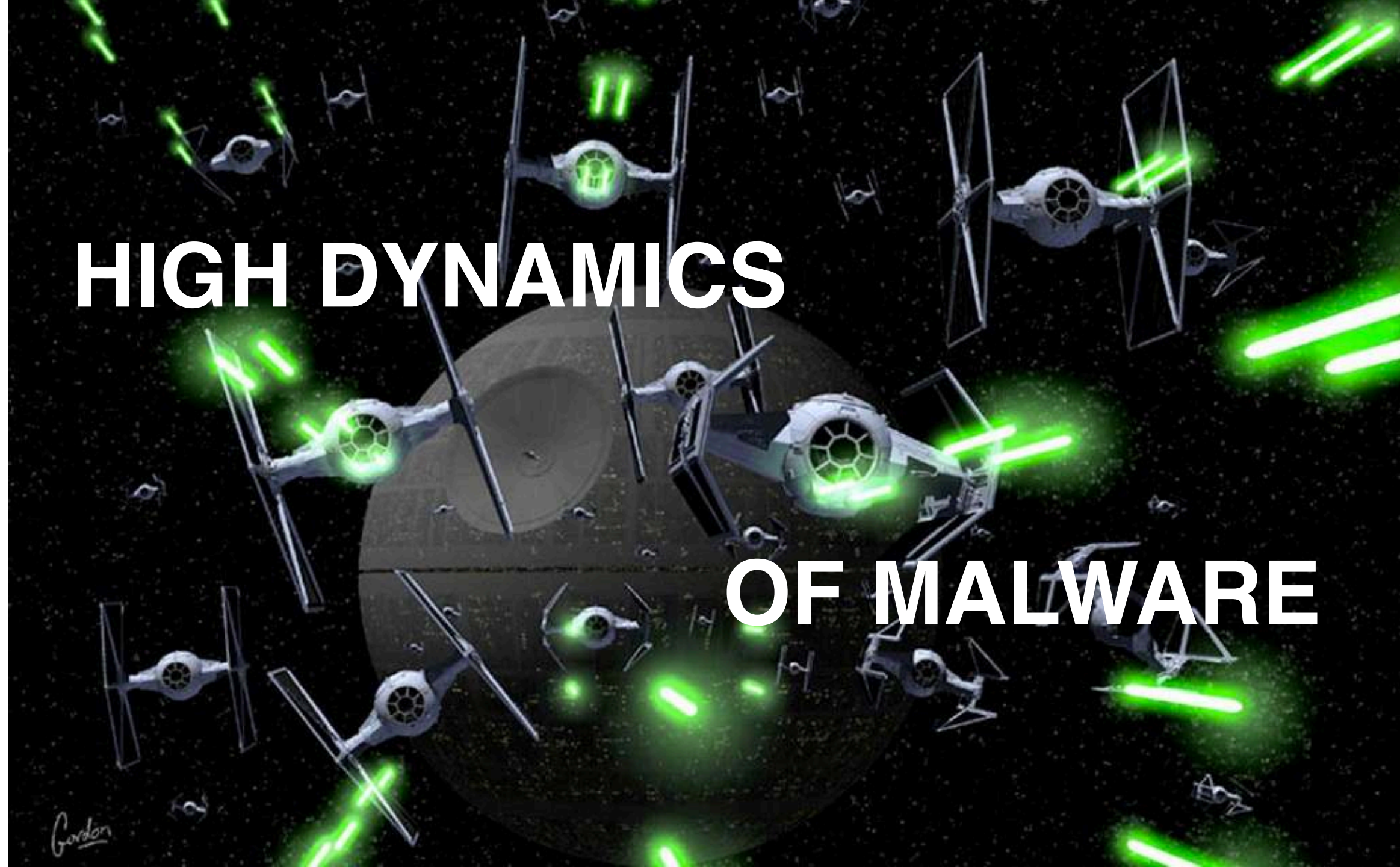


Transparency + Collaboration

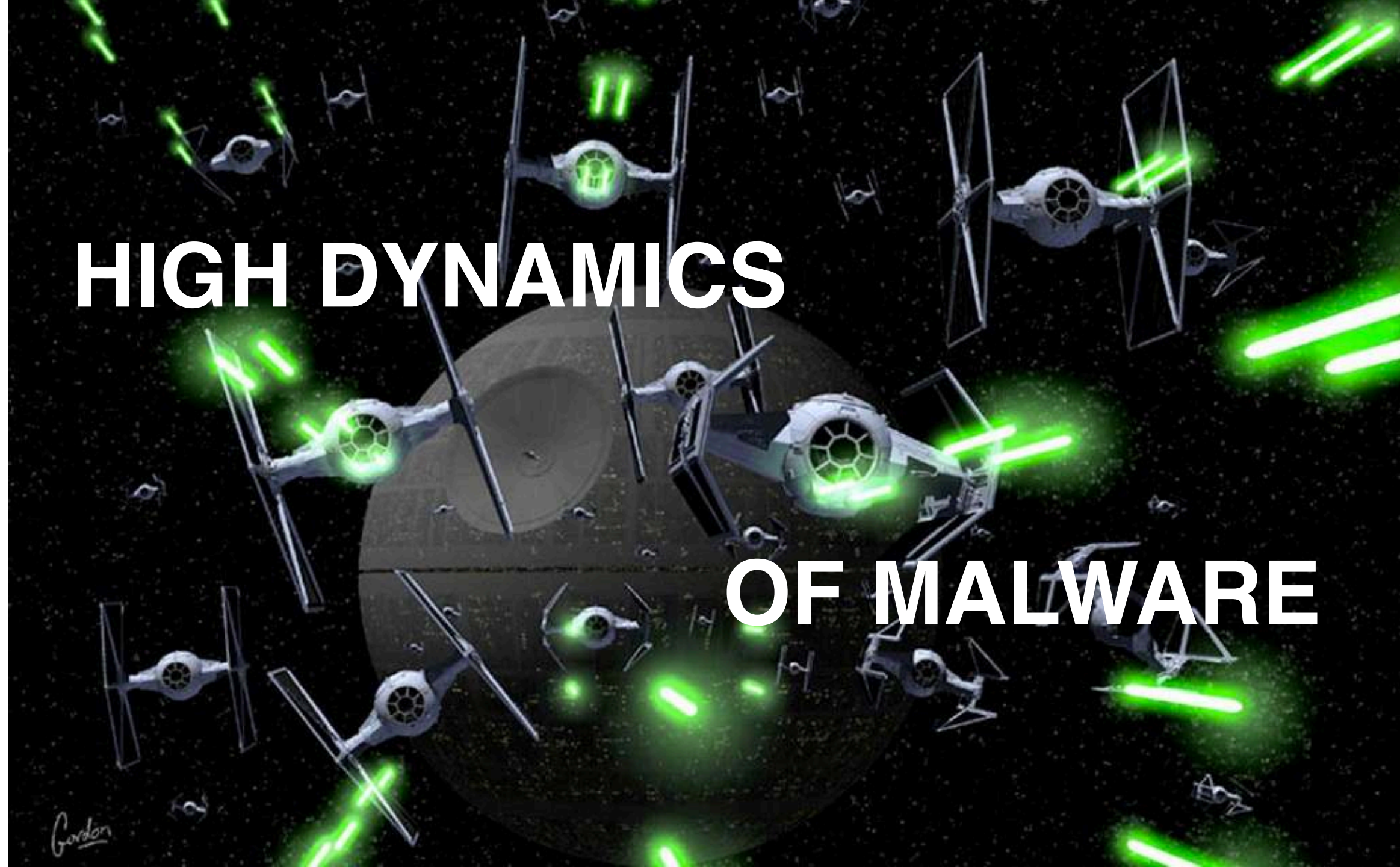
4 CHALLENGES



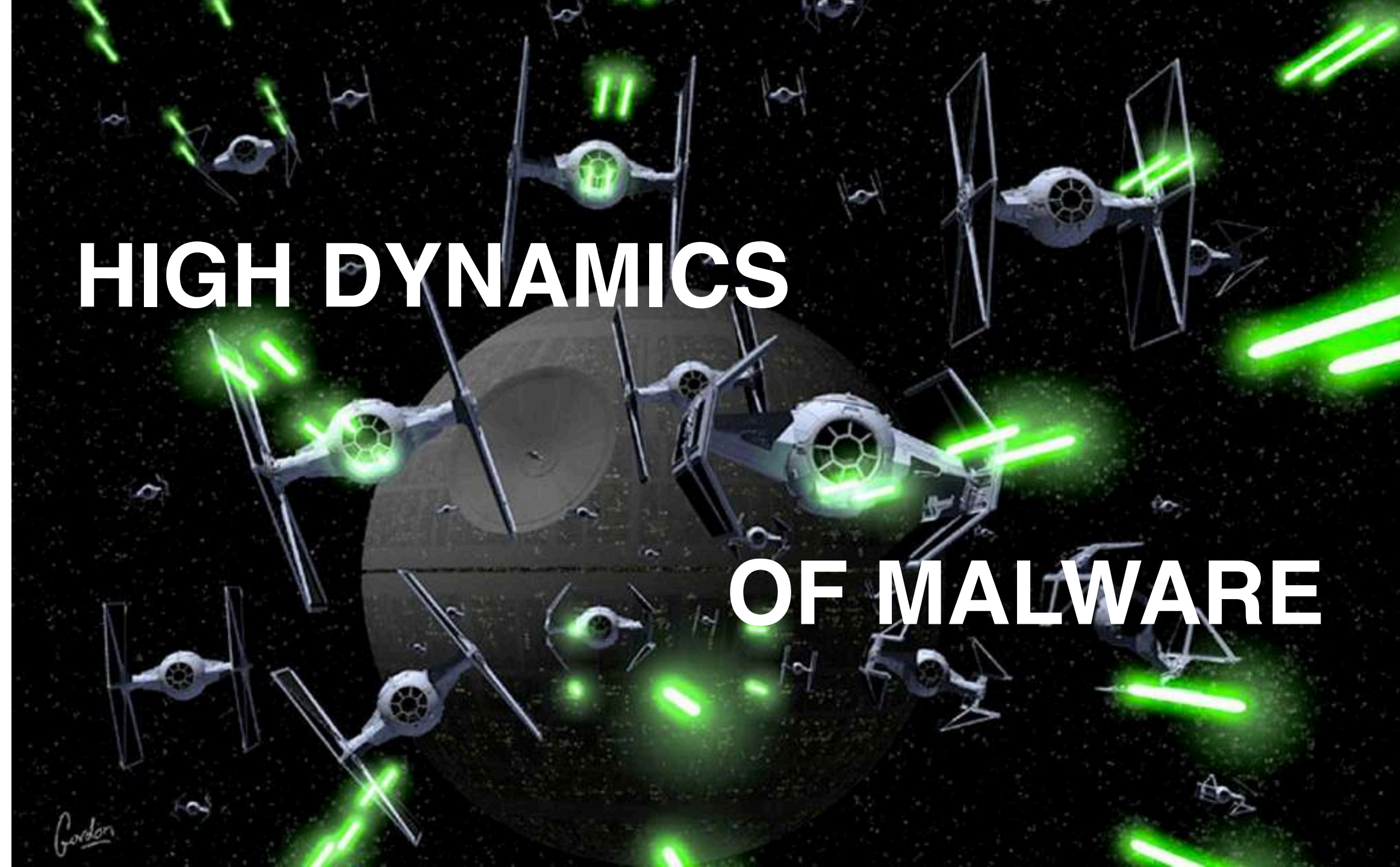
4 CHALLENGES



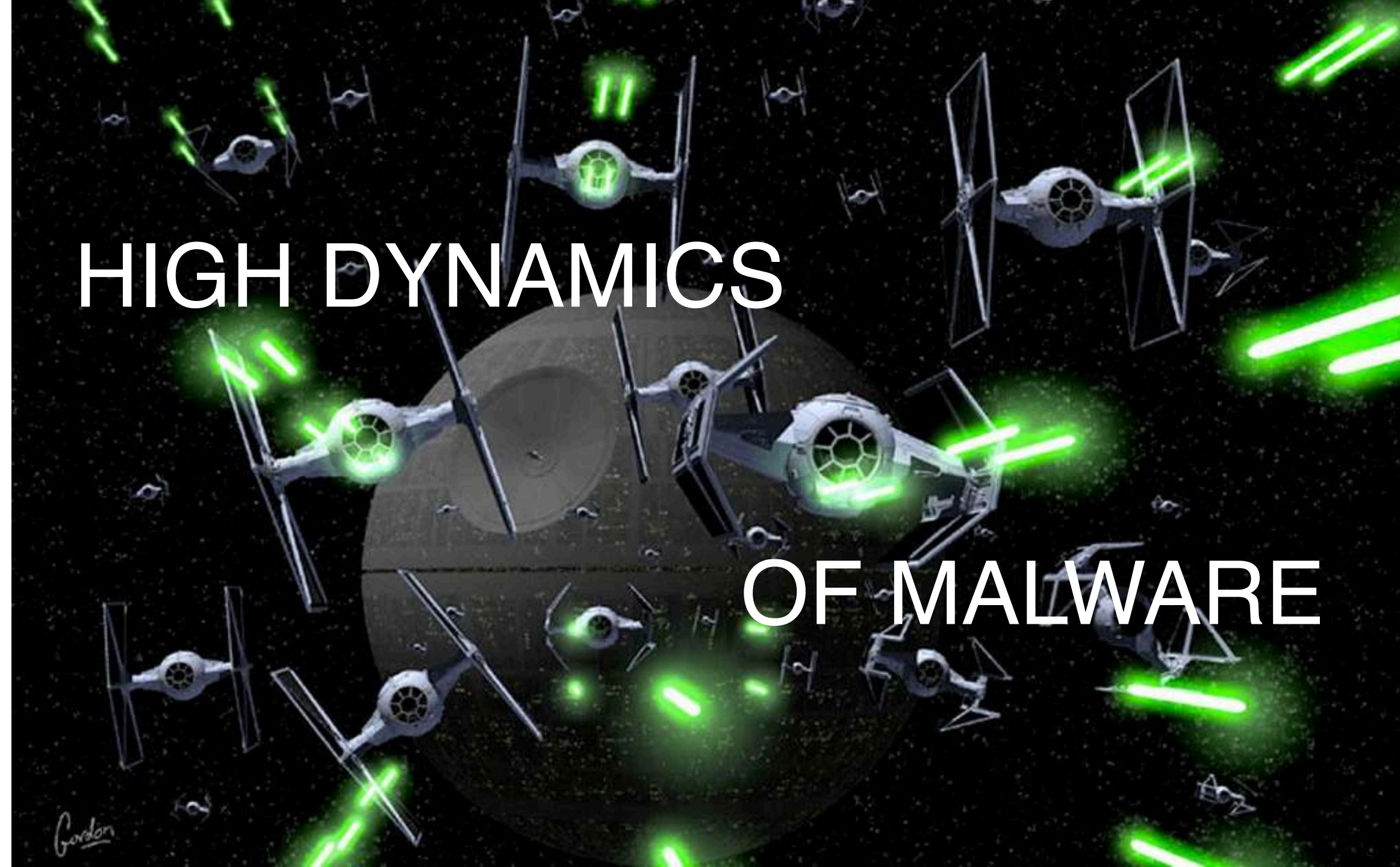
4 CHALLENGES

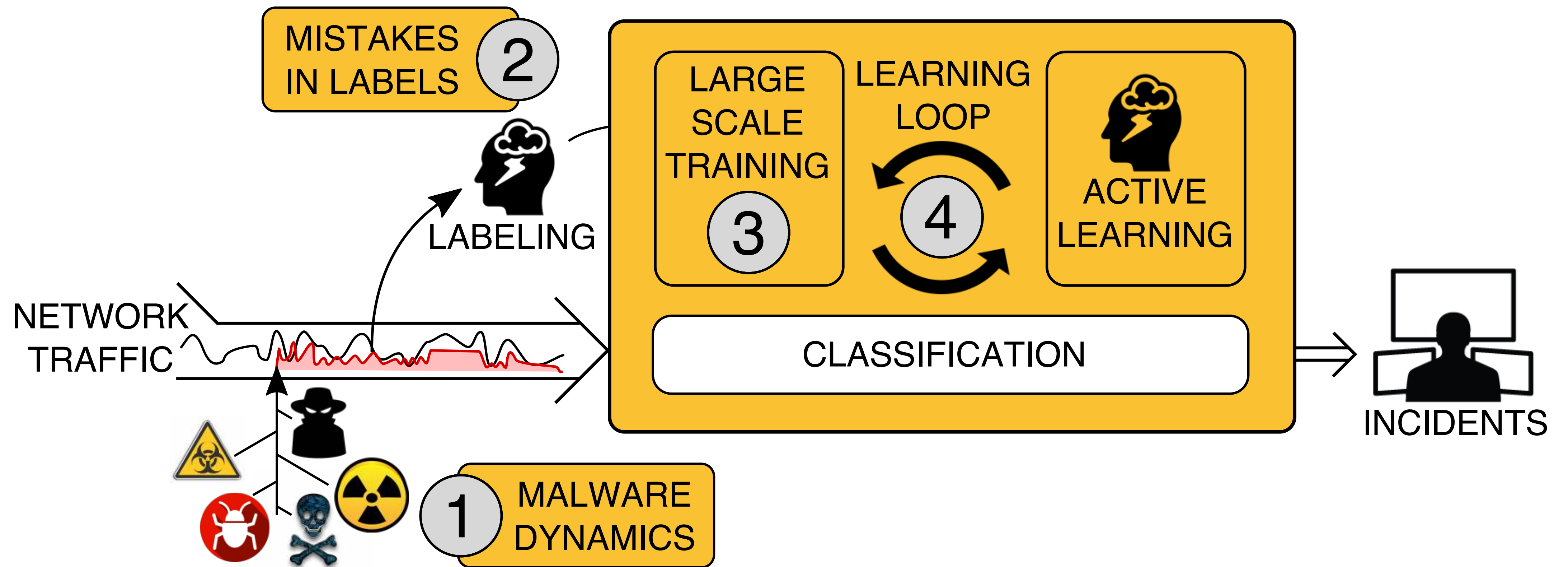


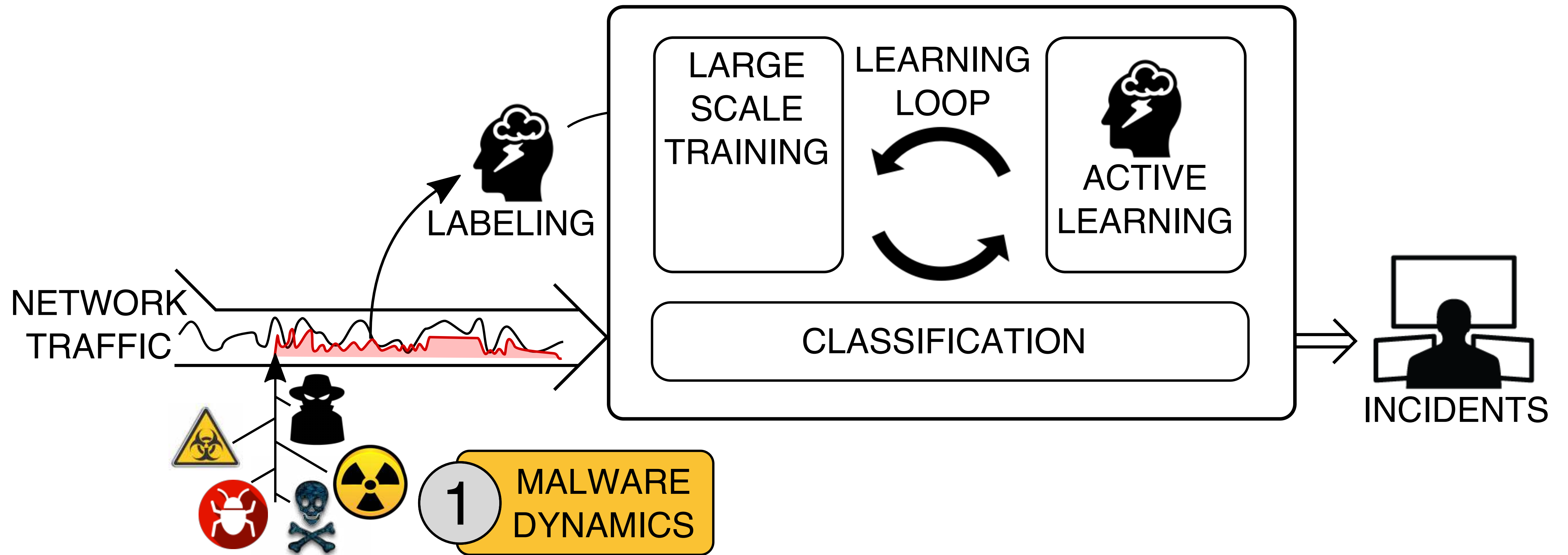
4 CHALLENGES



4 CHALLENGES



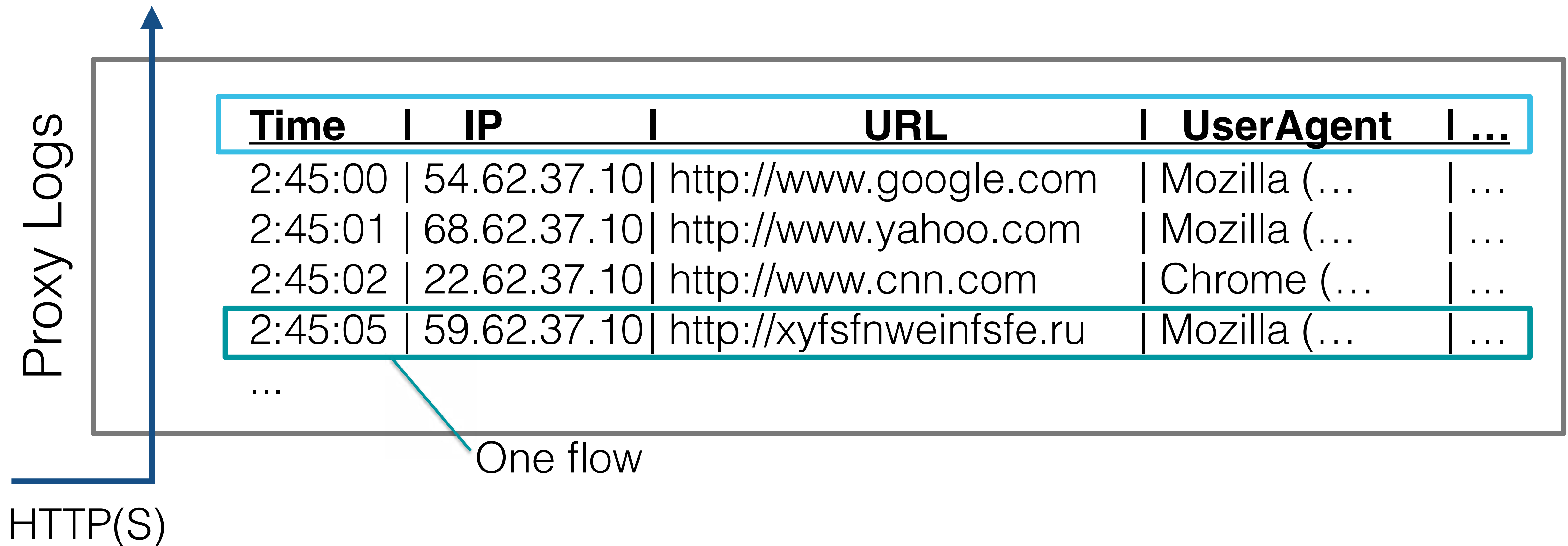




Change in Malicious Code or Payload

```
tion(a); })); $("#User_logged"); function  
if (0 == a.length) { return  
a.replace(/+(?= )/g, ""), a = a.split  
0 == r(a[c], b) ||  
length; c++) {  
for (var a = $("#  
tion h() {  
""), a = a.split(  
push(a[c])
```


Countermeasure – Proxy Log Records



Network Traffic Variability

Thinking Time	Server IP Address	Hostname	URL Path/ Resource/ Parameters
02:45:01	185.163.200.15		http://chgk.ge/logo.gif?a99b4ded=-1449439763
02:45:04	52.28.249.128		http://gim8.pl/images/logos.gif?ed13fa9b=-1269831060
02:45:09	195.157.15.100		http://althawry.org/images/logosa.gif?ed13e406=-1587317730
02:48:59	192.185.190.9		http://www.bijibali.com/images/logof.gif?2f18696=148149186
02:49:04	178.162.203.226		http://kukustrustnet987.info/home.gif?228c09=9056292
02:49:07	173.193.19.14		http://173.193.19.14/images/xs.jpg?250695=9706068

Extracted Features

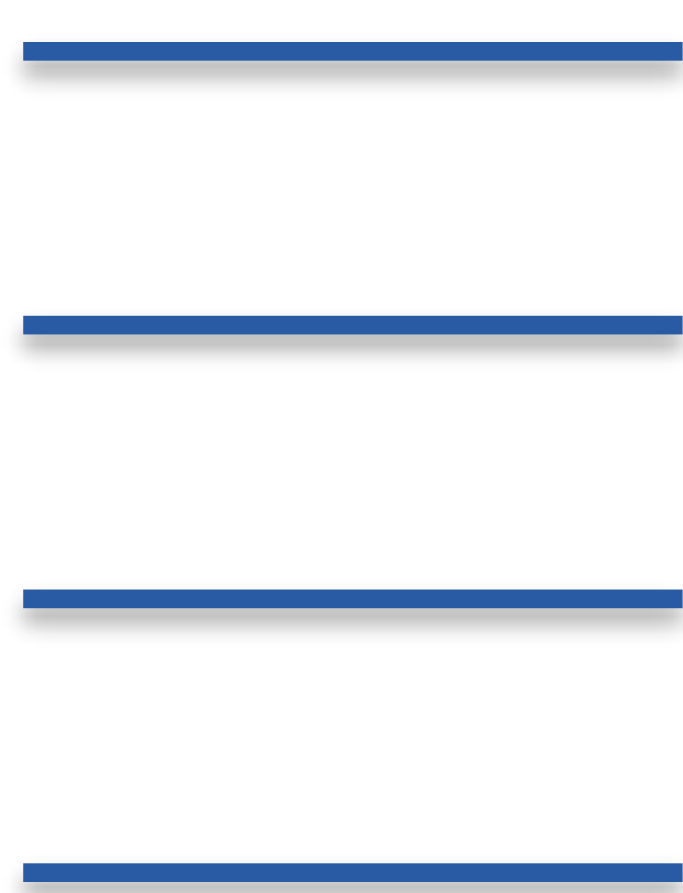
HTTP(S) based (~600):

- URL based – Related to n-grams of letters, distribution of characters, ...
- HTTP(s) request based – HTTP status, Ports, Up/Down Bytes, Referrer, User Agent, Mime Type, ...

Offline per domain/IP (~20):

- Global stats – user-domain popularity, ...
- External sources – domain age (WHOIS), ...

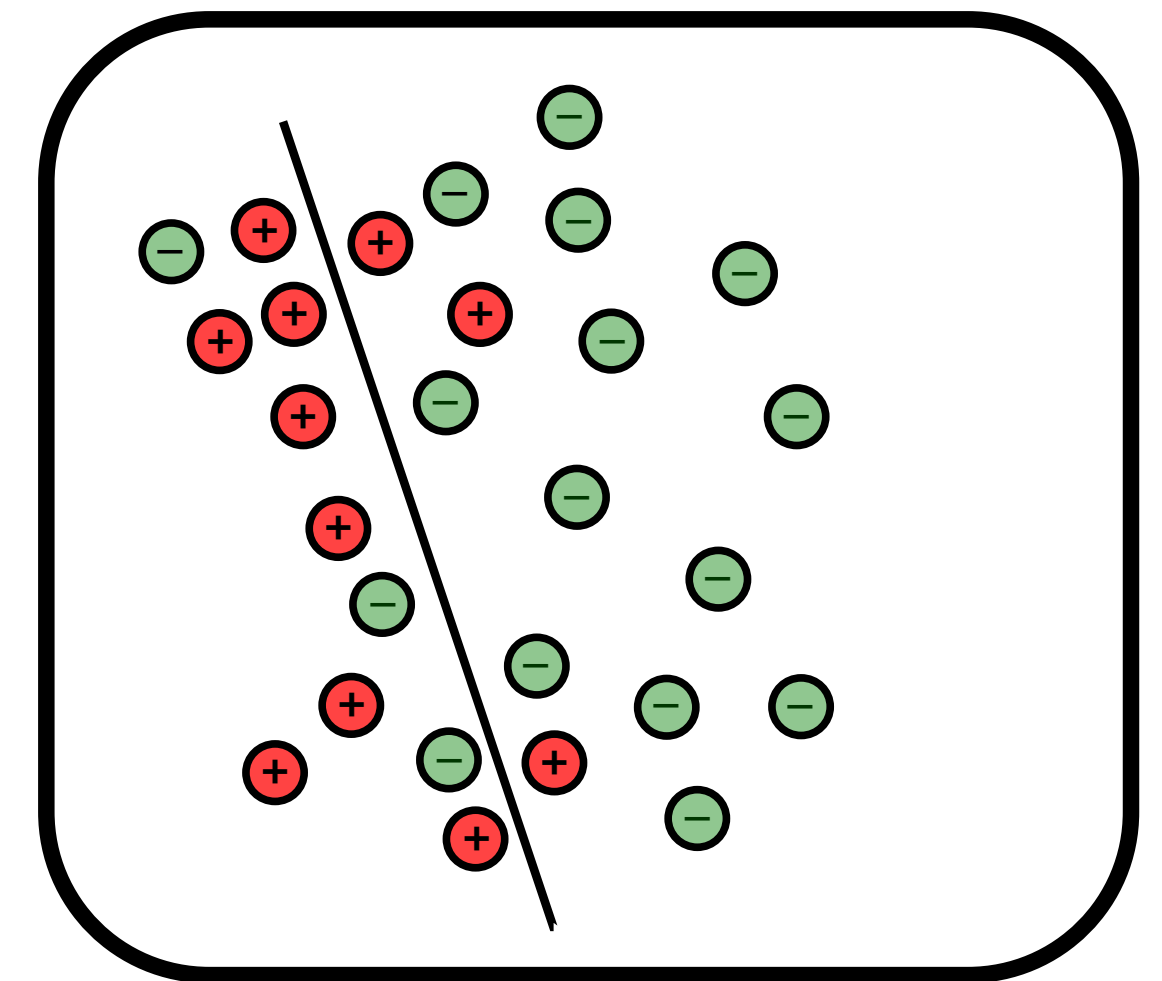
Legacy Approach



Network connection
(flow)

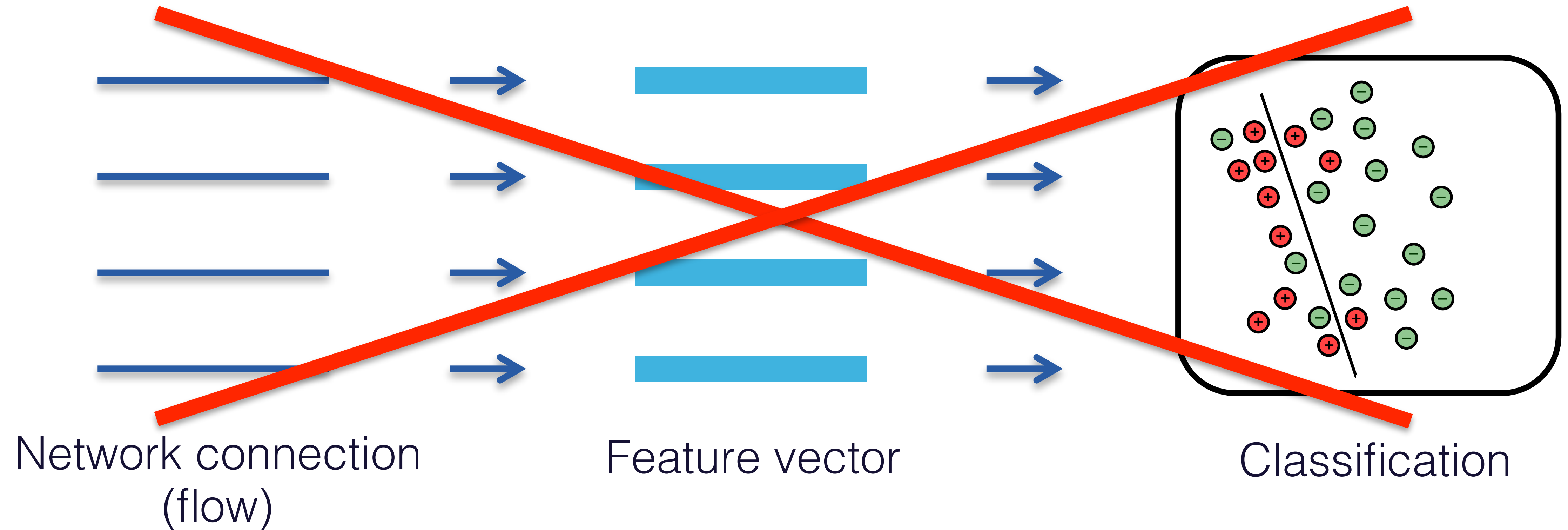


Feature vector

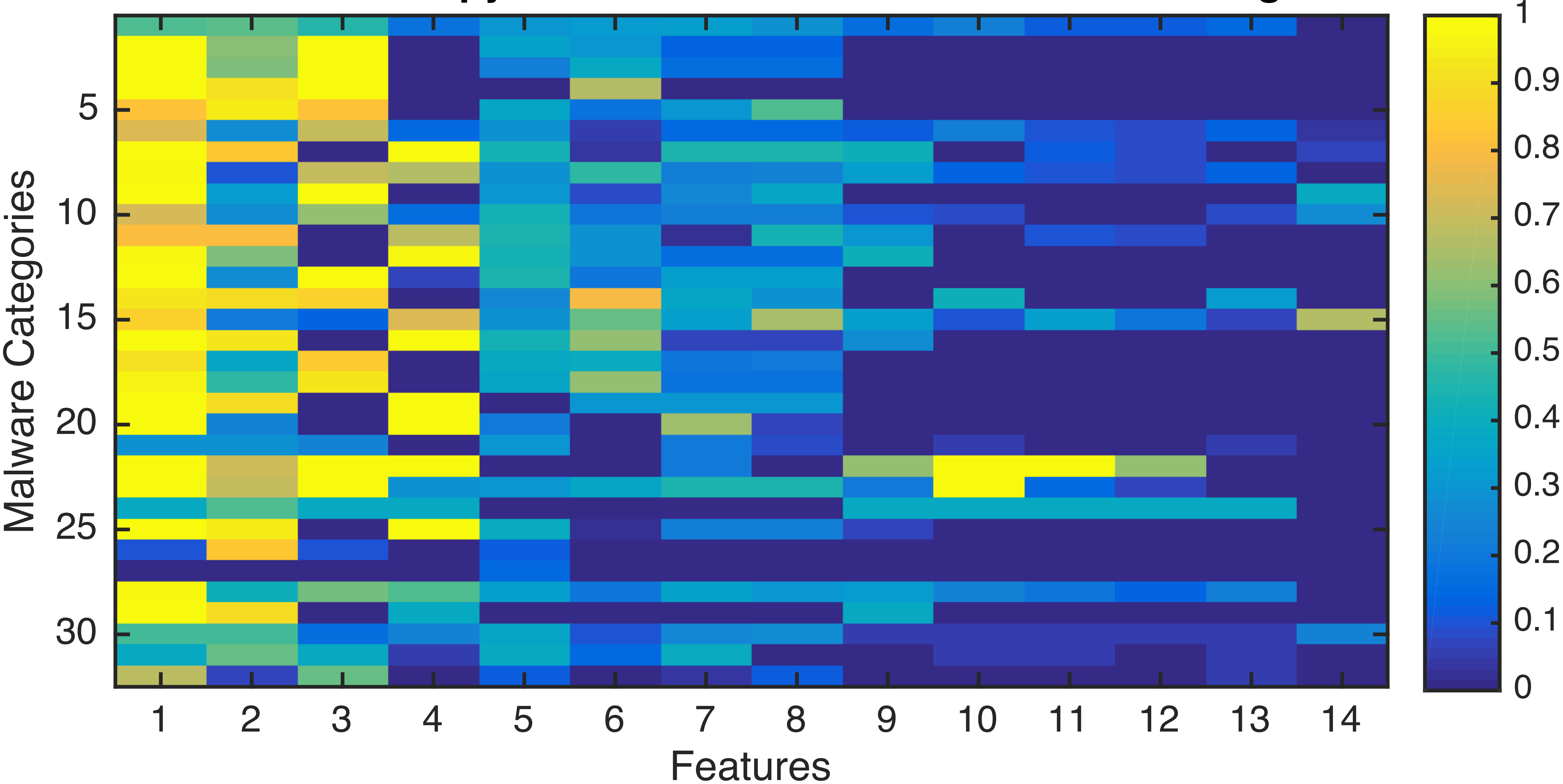


Classification

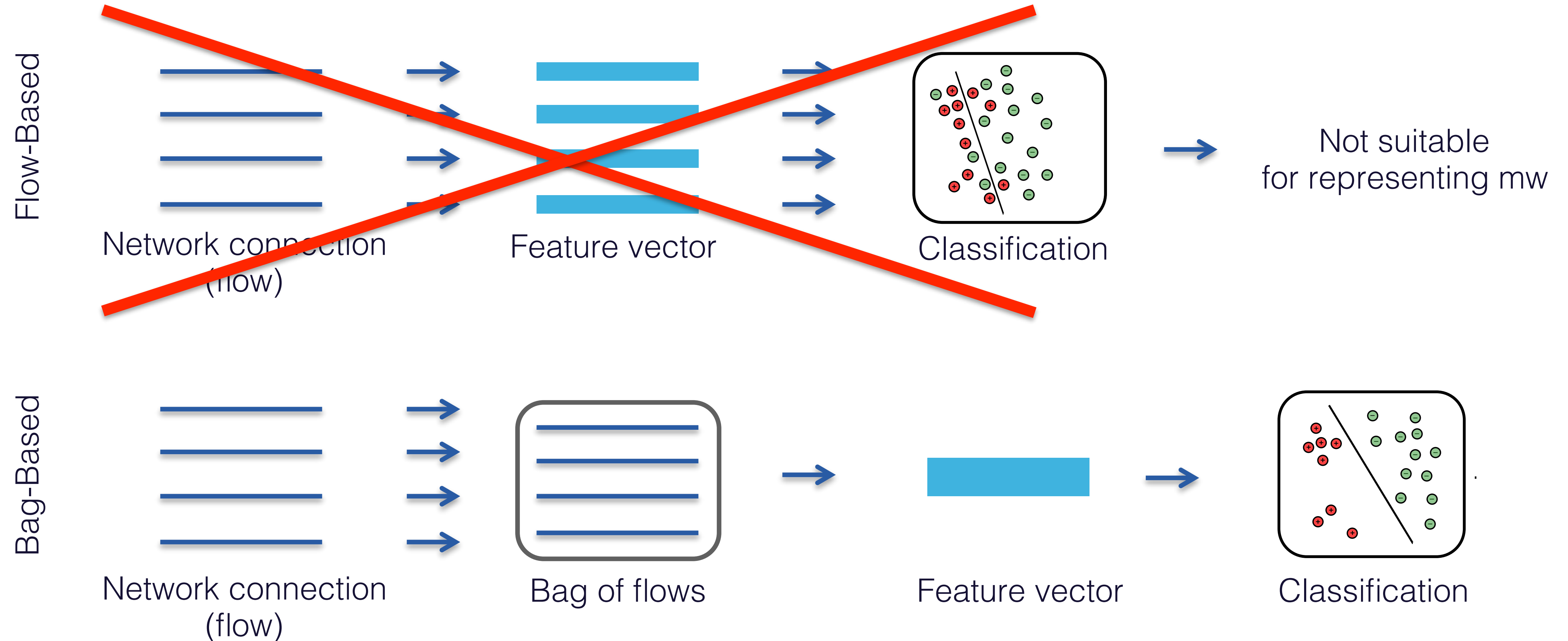
Legacy Approach



Normalized Entropy of Feature Values for 32 Malware Categories



Legacy vs. Proposed Bag Representation

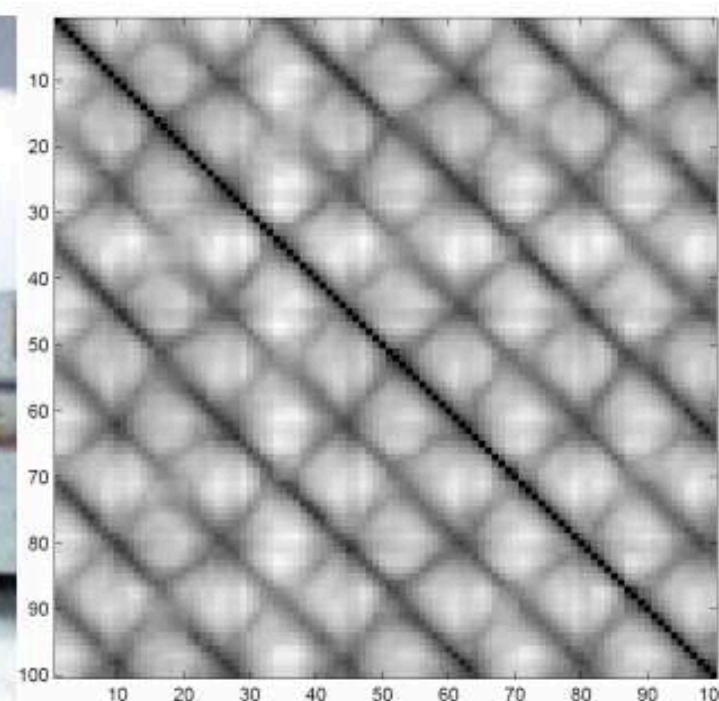
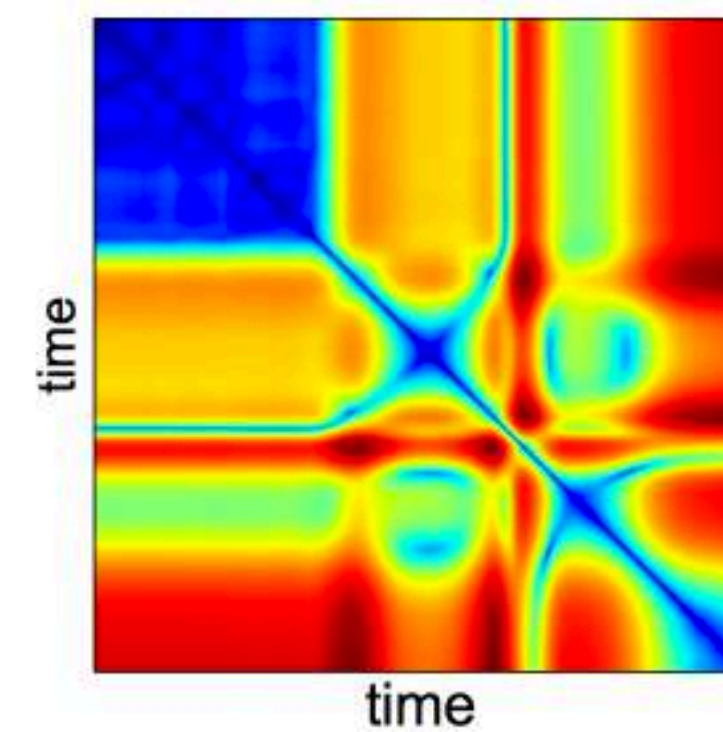
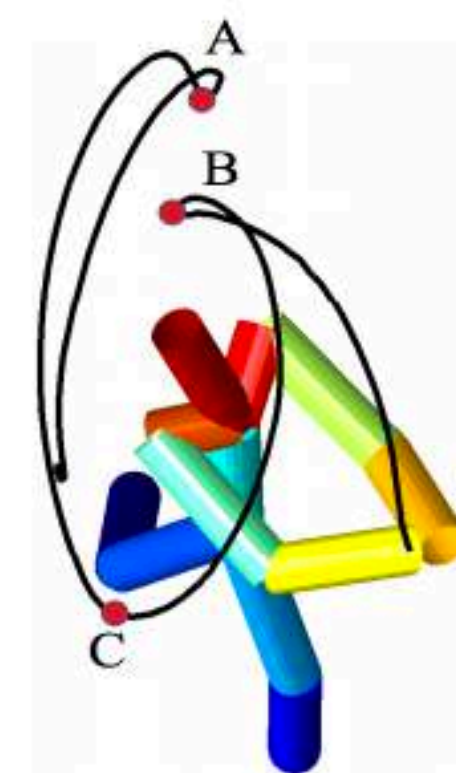
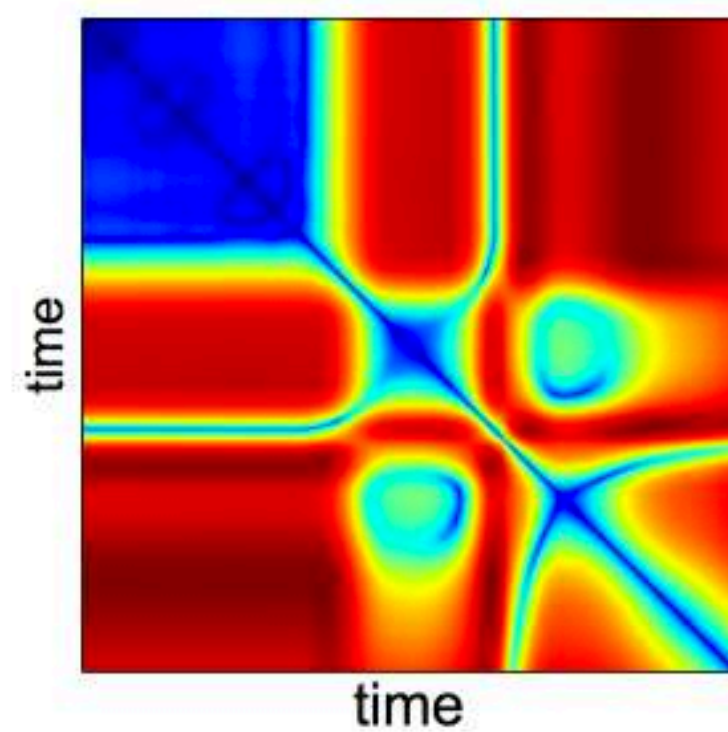
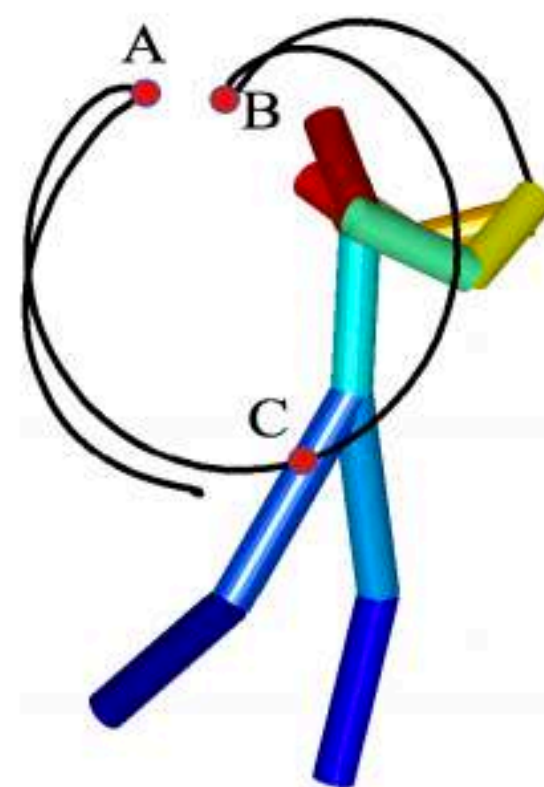


Asterope
hxxp://194.165.16.146:8080/pgt/?ver=1.3.3398&id=126&r=12739868&os=6.1—2—8.0.7601.18571&res=4—1921—466&f=1
hxxp://194.165.16.146:8080/pgt/?ver=1.3.3398&id=126&r=15425581&os=6.1—2—8.0.7601.18571&res=4—1921—516&f=1
hxxp://194.165.16.146:8080/pgt/?ver=1.3.3398&id=126&r=27423103&os=6.1—2—8.0.7601.18571&res=4—1921—342&f=1
hxxp://194.165.16.146:8080/pgt/?ver=1.3.3753&id=126&r=8955018&os=6.1—2—8.0.7601.18571&res=4—1921—319&f=1
Click-fraud, malvertising-related botnet
hxxp://directcashfunds.com/opntrk.php?tkey=024f9730e23f8553c3e5342568a70300&Email=name.surname@company.com
hxxp://directcashfunds.com/opntrk.php?tkey=c1b6e3d50632d4f5c0ae13a52d3c4d8d&Email=name.surname@company.com
hxxp://directcashfunds.com/opntrk.php?tkey=7c9a843ce18126900c46dbe4be3b6425&Email=name.surname@company.com
hxxp://directcashfunds.com/opntrk.php?tkey=c1b6e3d50632d4f5c0ae13a52d3c4d8d&Email=name.surname@company.com
Poweliks
hxxp://31.184.194.39/query?version=1.7&sid=793&builddate=114&q=nitric+oxide+side+effects&ua=Mozilla%2F5 ... &lr=7&ls=0
hxxp://31.184.194.39/query?version=1.7&sid=793&builddate=114&q=weight+loss+success+stories&ua=Mozilla%2F5 ... &lr=0&ls=0
hxxp://31.184.194.39/query?version=1.7&sid=793&builddate=114&q=shoulder+pain&ua=Mozilla%2F5 ... &lr=7&ls=2
hxxp://31.184.194.39/query?version=1.7&sid=793&builddate=114&q=cheap+car+insurance&ua=Mozilla%2F5 ... &lr=7&ls=2
Zeus
hxxp://130.185.106.28/m/IbQFdXVjiriLva4KHeNpWCmThrJBn3f34HNwsLVVsUmLXtsumSSPe/zzXtlu9SzwjI9zKlxdE ... 3RqvGzKN5
hxxp://130.185.106.28/m/IbQJFUVjgZn4vx4KHeNpWCmThrJBn3f34HNwsLVVsUmLfkoPaSS+S+zzXtlu9SzwjI9zKlxdE ... 3vKwmk0oUi
hxxp://130.185.106.28/m/IbQJFUVjiJwJBX4KHeNpWCmThrJBn3f34HNwsLVVsUmKH7ue2STvSkzzXtlu9SzwjI9zKlxdE ... 3vKwmk0oUi
hxxp://130.185.106.28/m/IbQNtVVji5/7Yp4KHeNpWCmThrJBn3f34HNwsLVVsUmLz4sO6YRvOjzzXtlu9SzwjI9zKlxdE ... 3zB9057quqv
Legitimate traffic 1
hxxp://www.cnn.com/.element/ssi/auto/4.0/sect/MAIN/markets_wsod_expansion.html
hxxp://www.cnn.com/.a/1.73.0/assets/sprite-s1dced3ff2b.png
hxxp://www.cnn.com/.element/widget/video/videoapi/api/latest/js/CNNVideoBootstrapper.js
hxxp://www.cnn.com/jsonp/video/nowPlayingSchedule.json?callback=nowPlayingScheduleCallbackWrapper&_=1422885578476

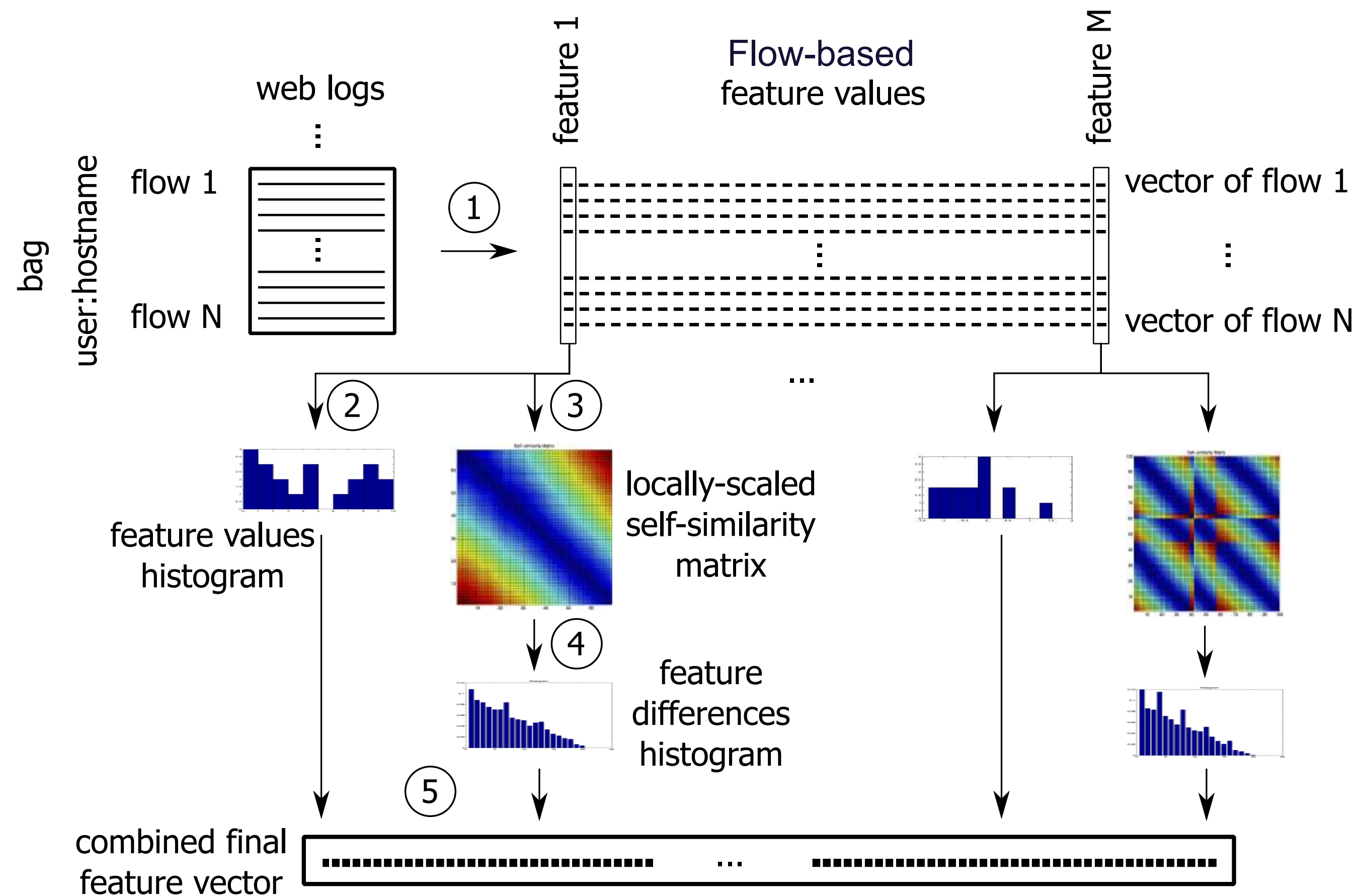
MALICIOUS
BAGS

LEGITIMATE
BAG

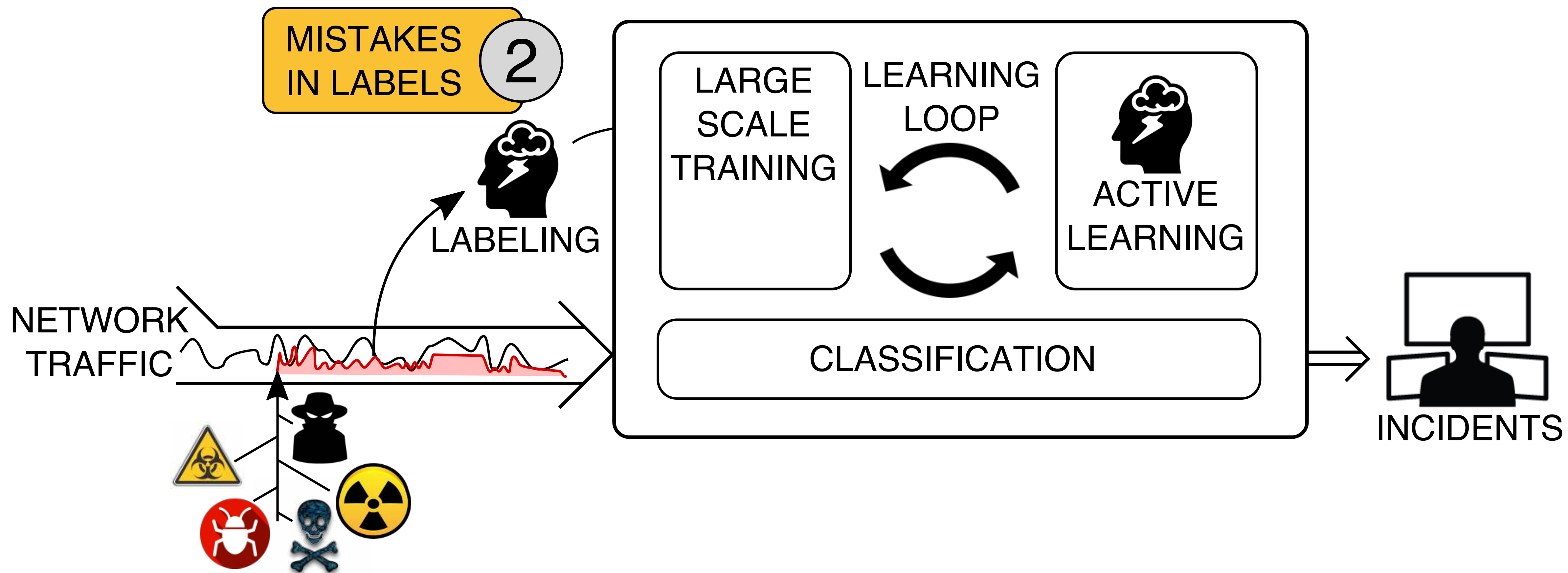
Parallel to Action Recognition



Invariant Representation* – Overview



- 1 – create bag
+ extract flow-based feature vectors
- 2 – create feature values histogram
- 3 – create self-similarity matrix
- 4 – create feature differences histogram
- 5 – combine into final feature vector



Week Labels for Training?

Small amount of reliable labels



Week Labels for Training?

Large amount of week labels (blacklists, feeds)

Can we use them for training? Mistakes?

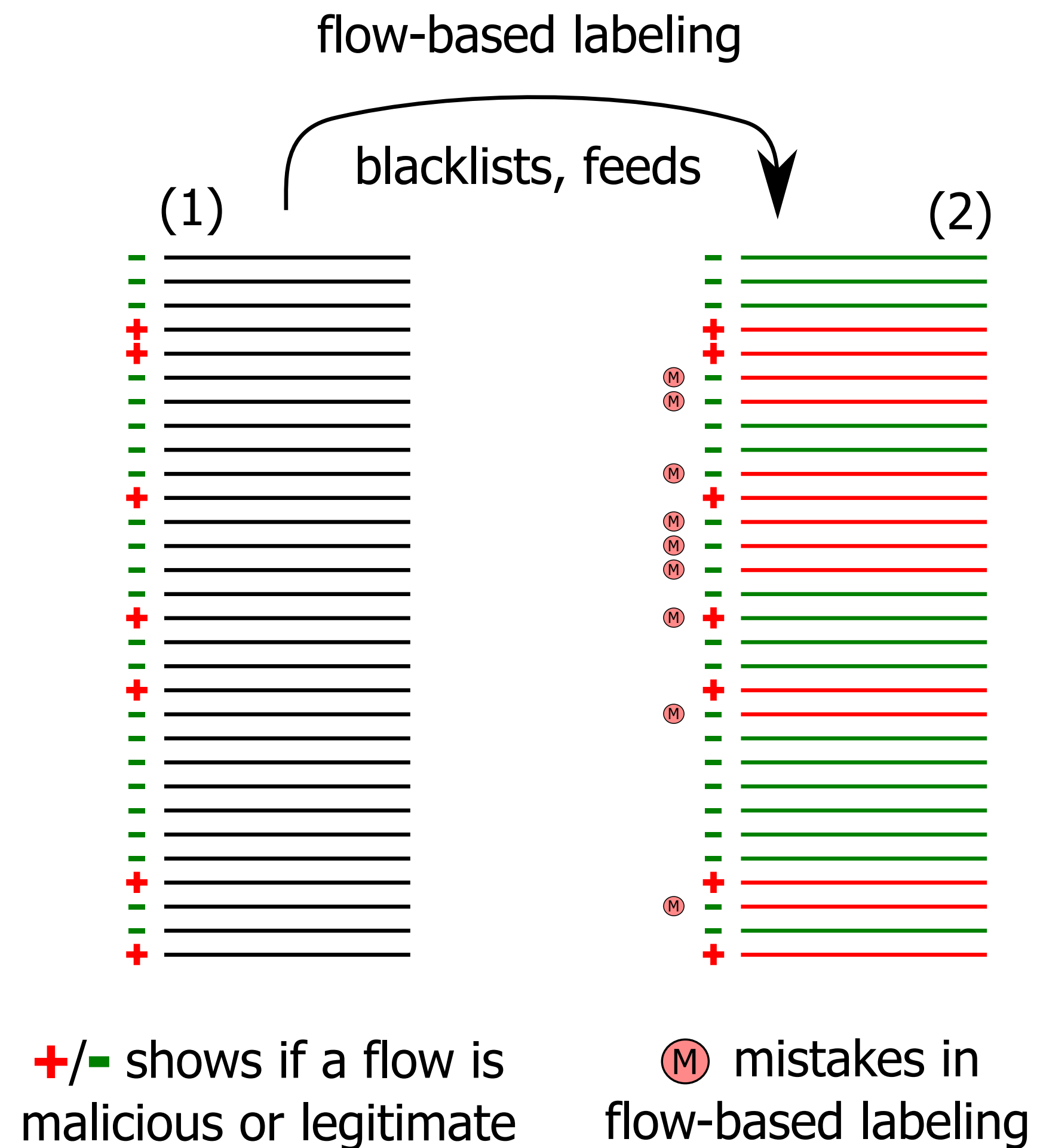


Multiple Instance Learning (MIL)

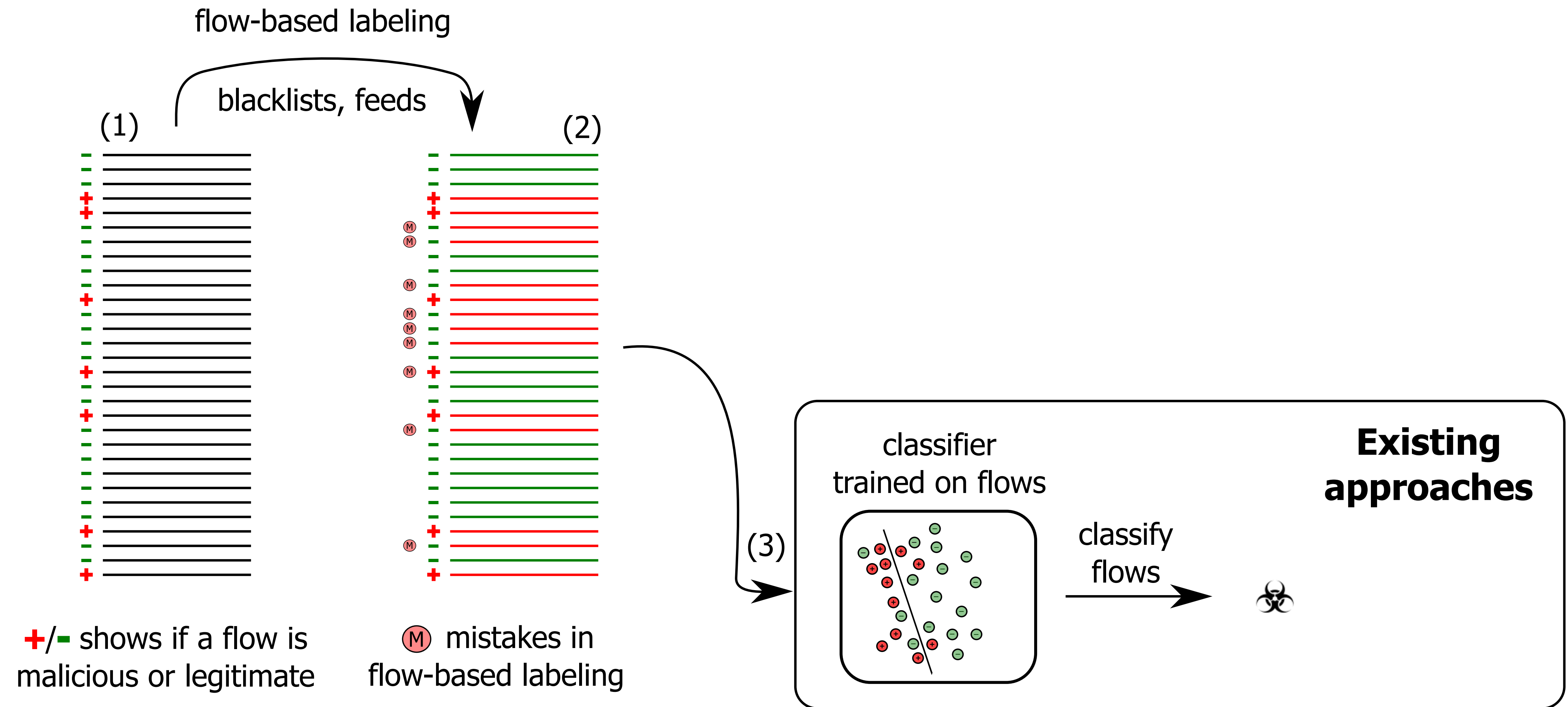


+/- shows if a flow is
malicious or legitimate

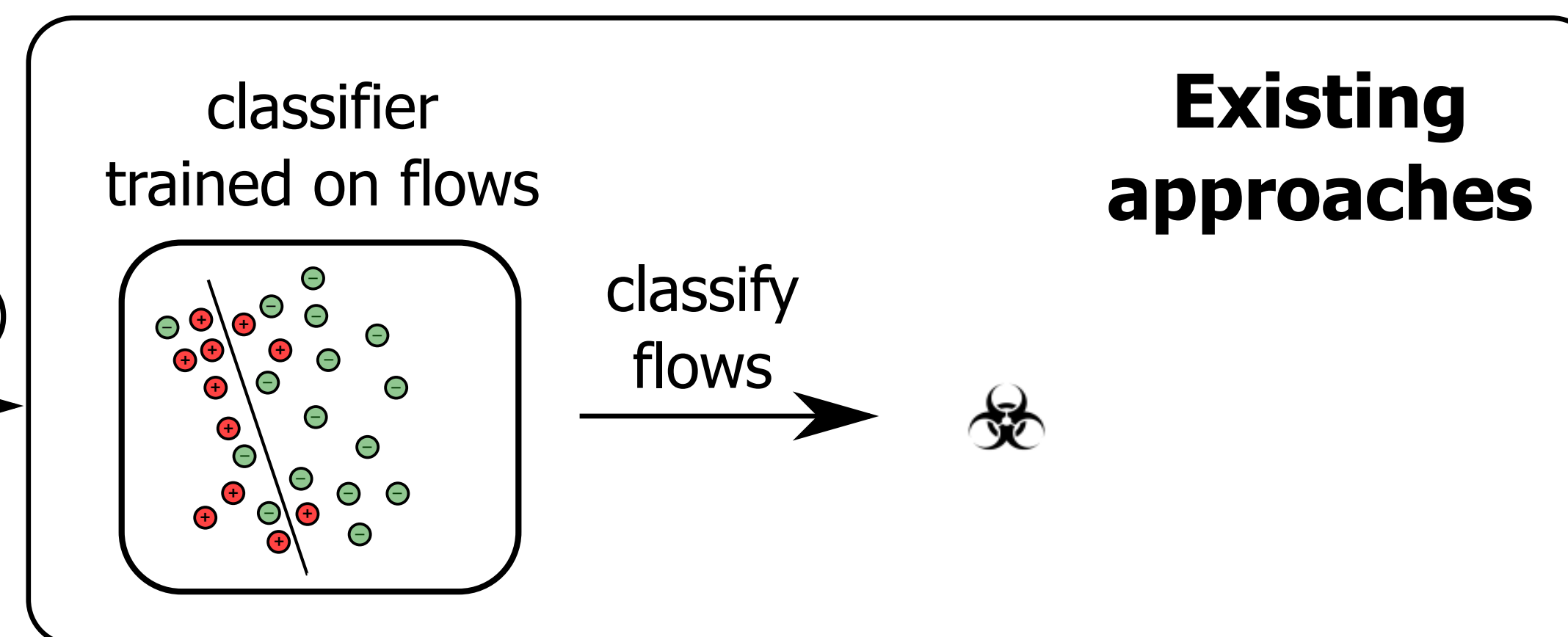
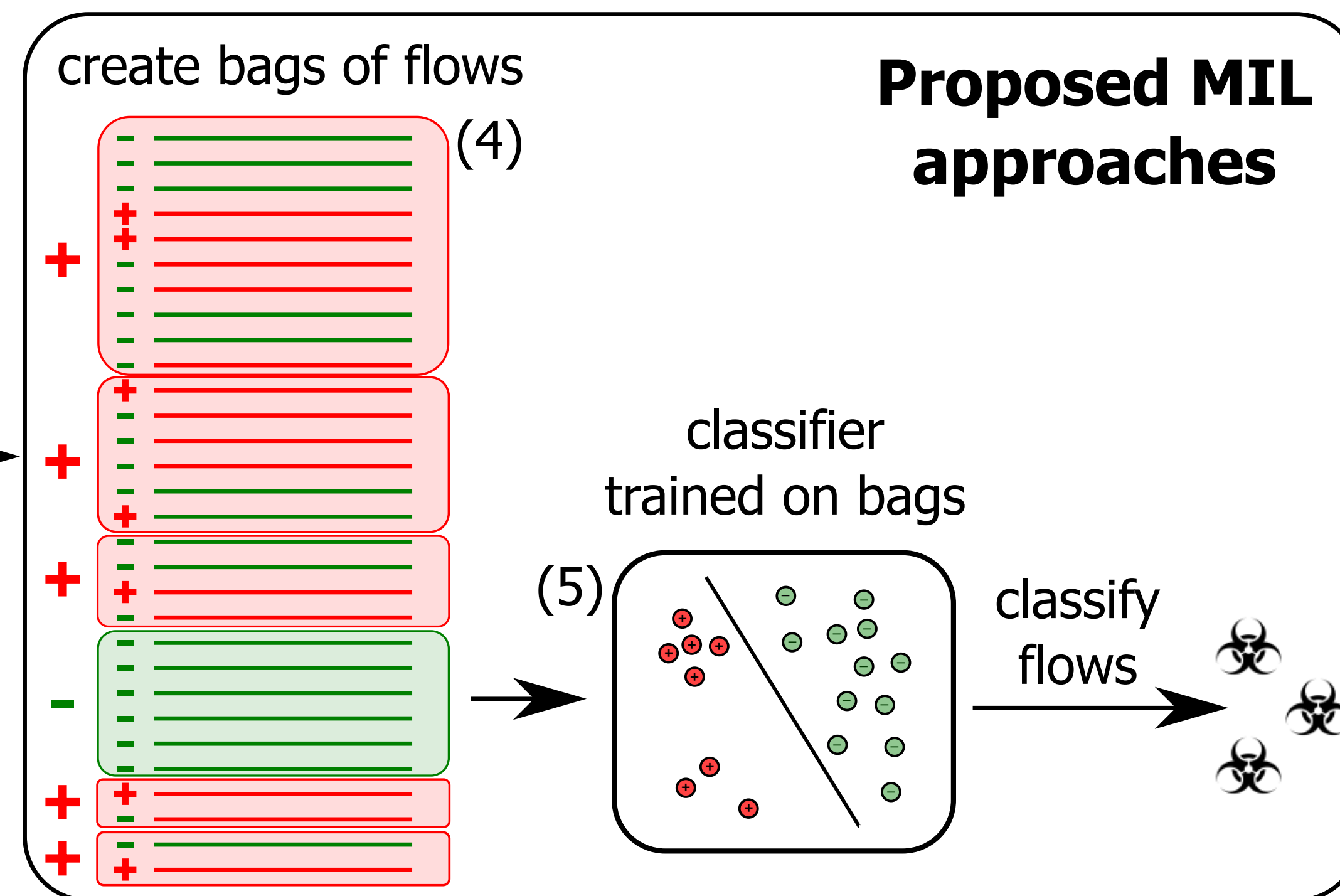
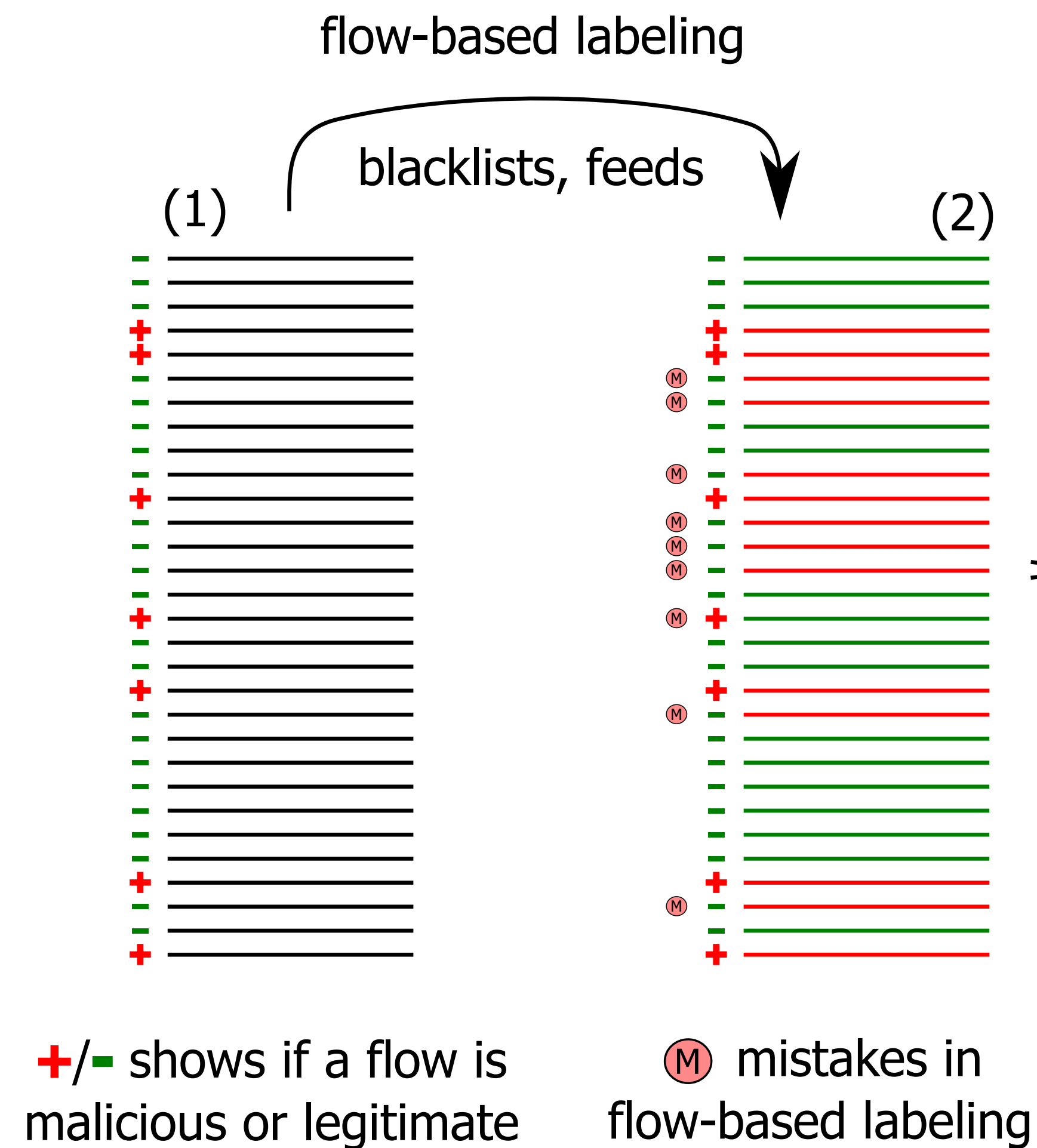
Multiple Instance Learning (MIL)



Multiple Instance Learning (MIL)



MIL*



Wide Classification Capability

Cryptowall

<http://zerosumstudio.com/img5.php?z=smnk91cpnmd>

<http://zerosumstudio.com/img5.php?z=sd04vutaog>

<http://zerosumstudio.com/img5.php?z=snmofp2ye0x>

Goznym Banking Trojan

<http://carvezine.com/chdcm.php?gvo=miovlbwds&pbhpuo=03625369&oo...>

<http://carvezine.com/nnlgz.php?pmgl=wynnckyuok&nlm=vzhuhjachy&nptr...>

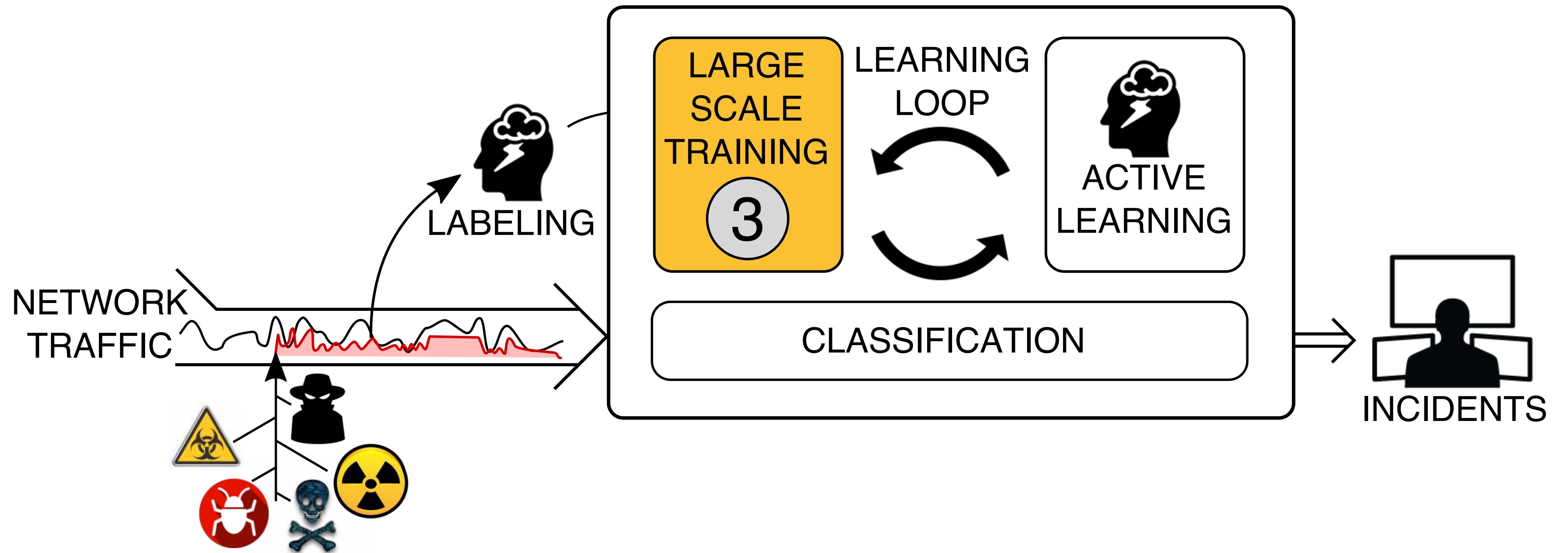
<http://carvezine.com/syajsg.php?lmtzkhhj=xmilzwgox&djax=1PhY8FI2NioY...>

Rig Exploit Kit

<http://ds.revivefl.org/?x3qJc7iZLBrGAoc=13SKfPrfJxzFGMSUb-nJDa9BMEX...>

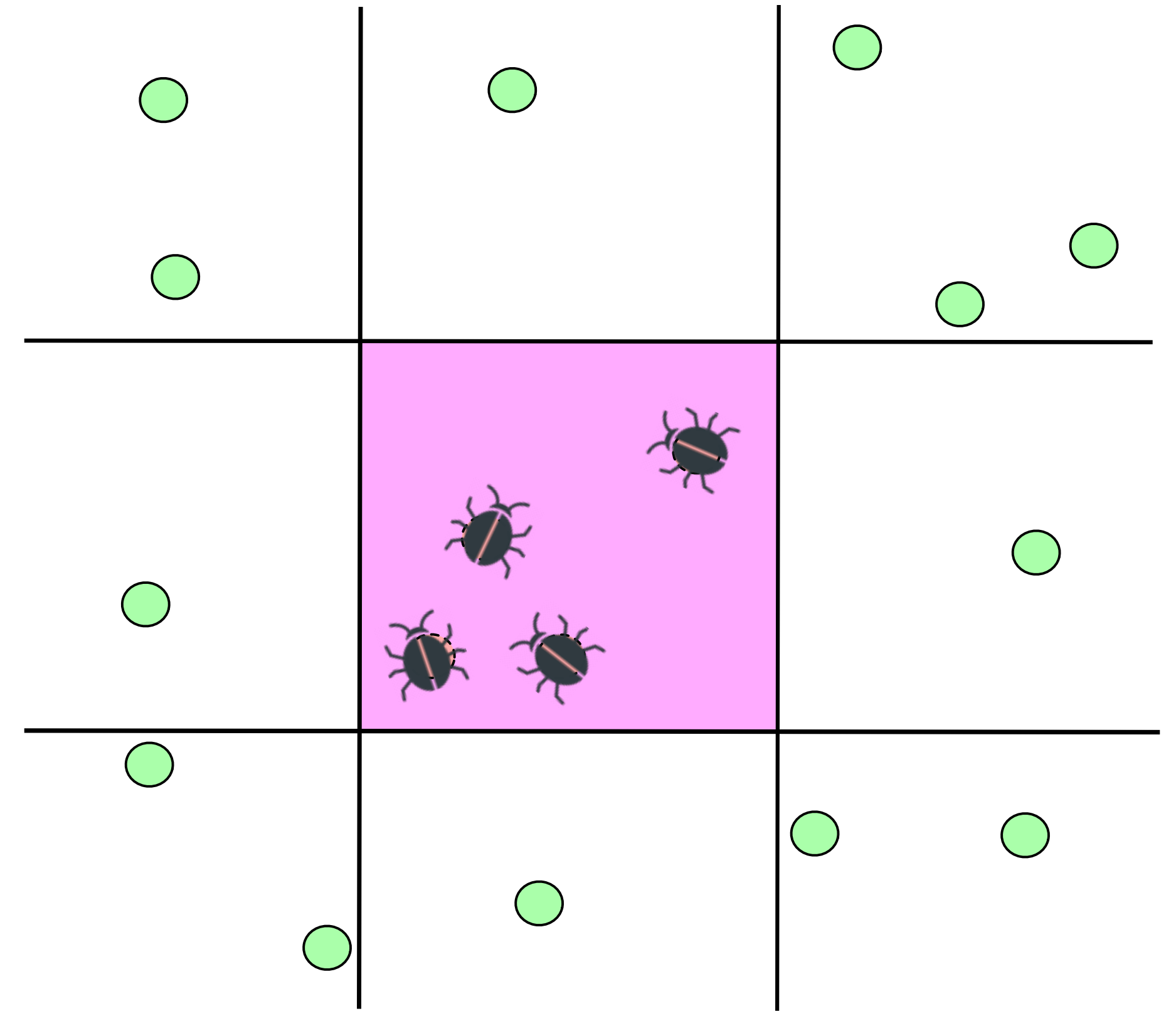
<http://ds.revivefl.org/index.php?x3qJc7iZLBrGAoc=13SKfPrfJxzFGMSUb-nJ...>

http://ds.revivefl.org/index.php?h4SGhKrXCJ-ofSih17OIFxzsmTu2KV_Opqxv...



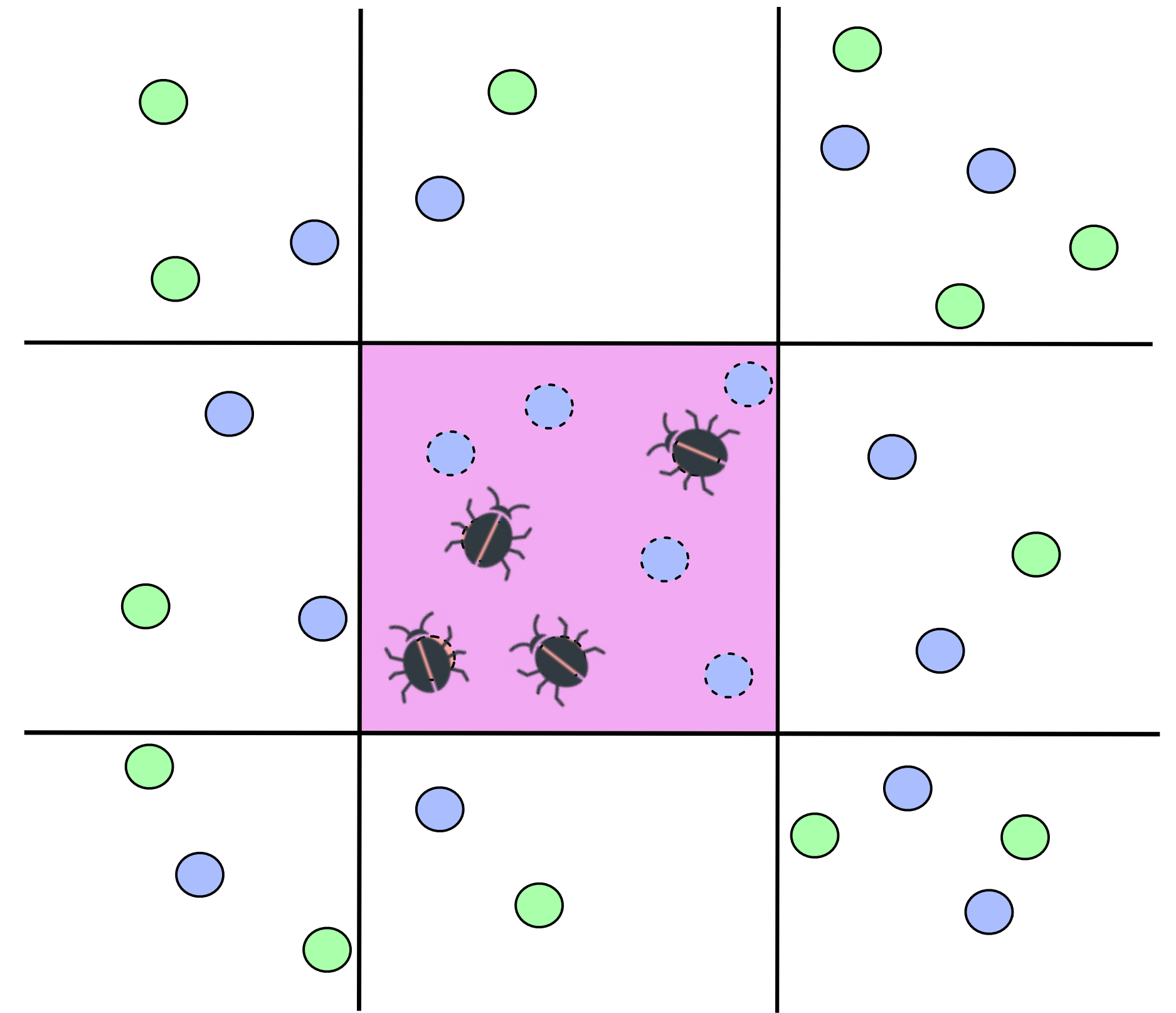
How to Sample Training Data

1 day = +10 billion requests
(millions of users and devices)



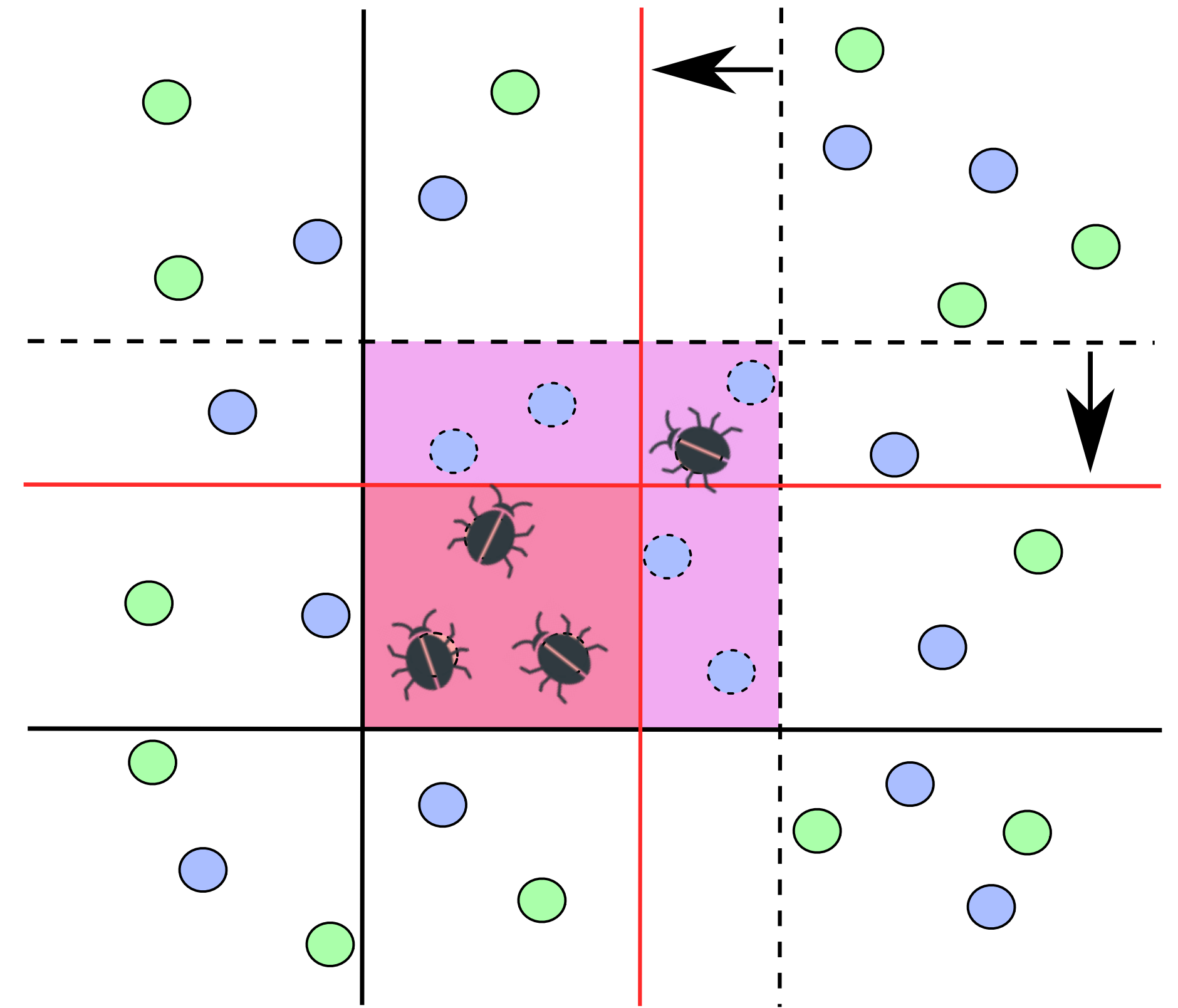
How to Sample Training Data

1 day = +10 billion requests
(millions of users and devices)



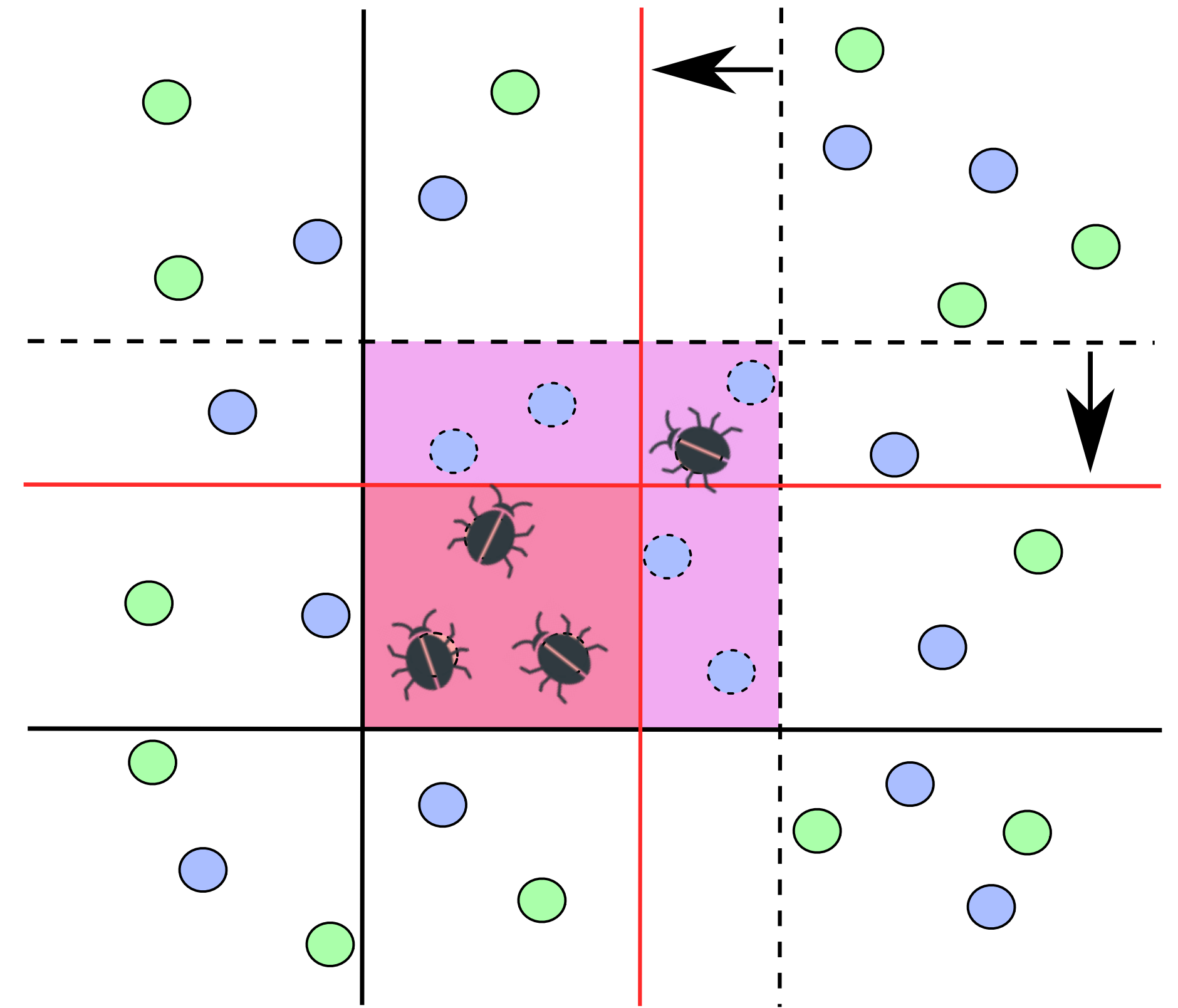
How to Sample Training Data

1. **RANK** the traffic according to the **SCORE** of statistical classifiers
2. Take only **TOP-N** samples as the **NEGATIVES**
3. **COLLECT** samples across longer time period



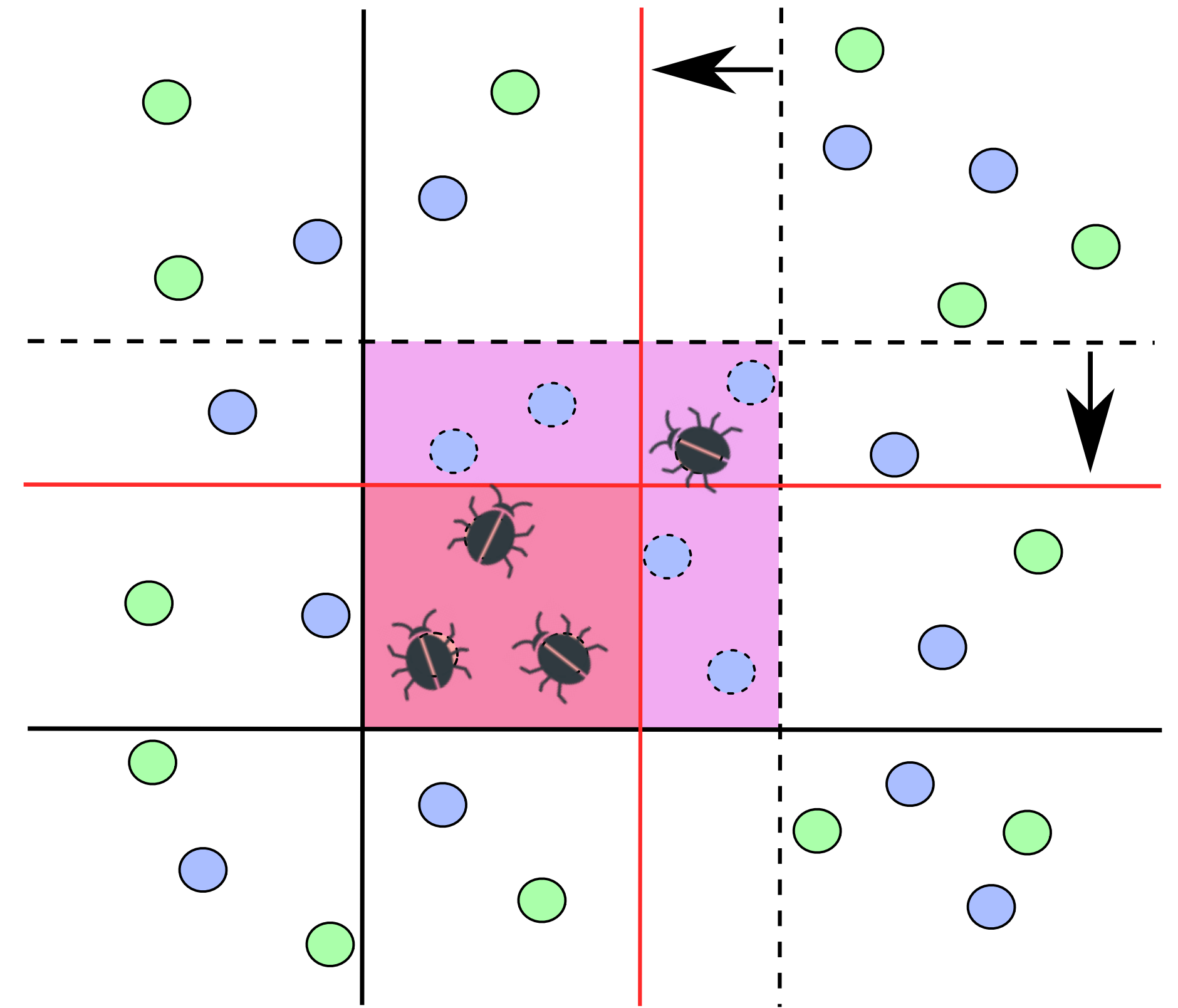
How to Sample Training Data

1. **RANK** the traffic according to the **SCORE** of statistical classifiers
2. Take only **TOP-N** samples as the **NEGATIVES**
3. **COLLECT** samples across longer time period



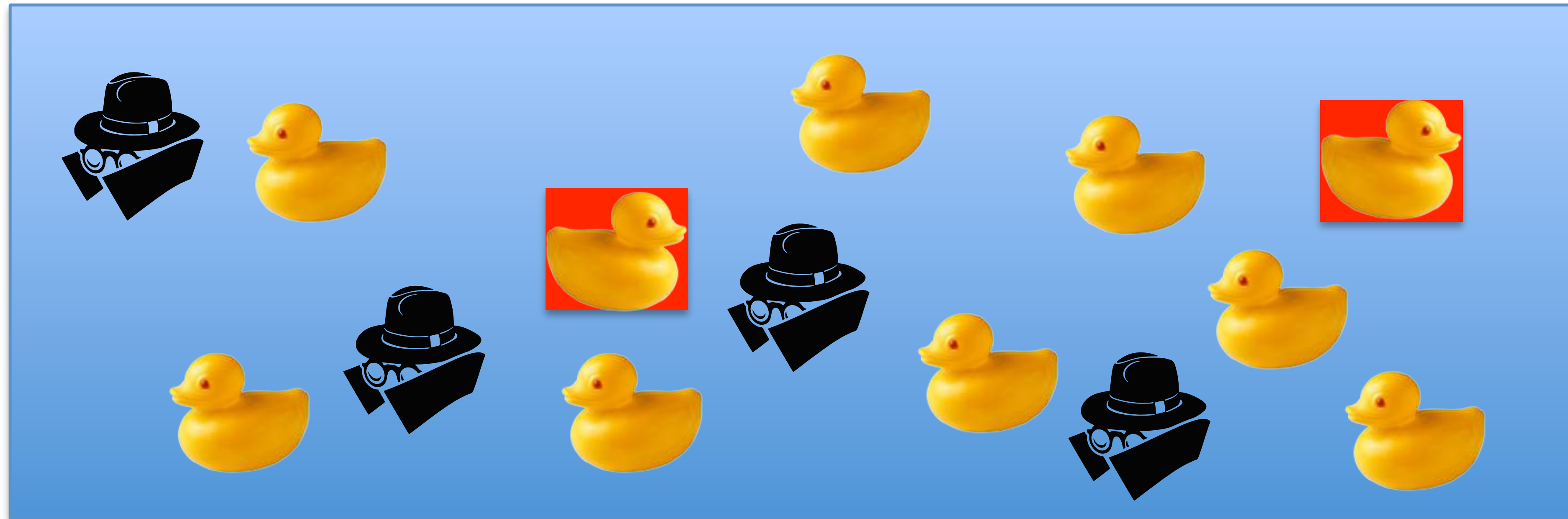
How to Sample Training Data

1. **RANK** the traffic according to the **SCORE** of statistical classifiers
2. Take only **TOP-N** samples as the **NEGATIVES**
3. **COLLECT** samples across longer time period



Positive-Unlabeled Training*

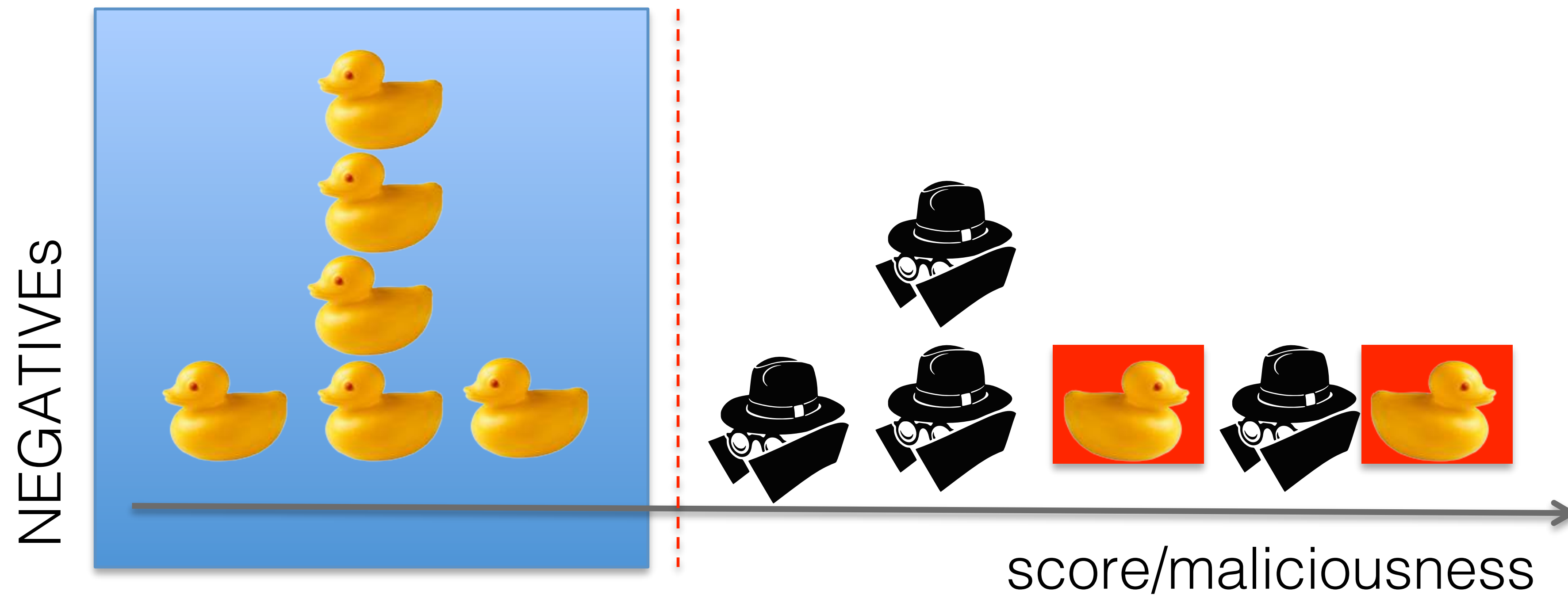
POOL OF NEGATIVES



 = spy/known positive  = malicious duck  = benign duck

* X. Li, B. Liu, S.K. Ng: Negative Training Data can be Harmful to Text Classification, 2010, EMNLP

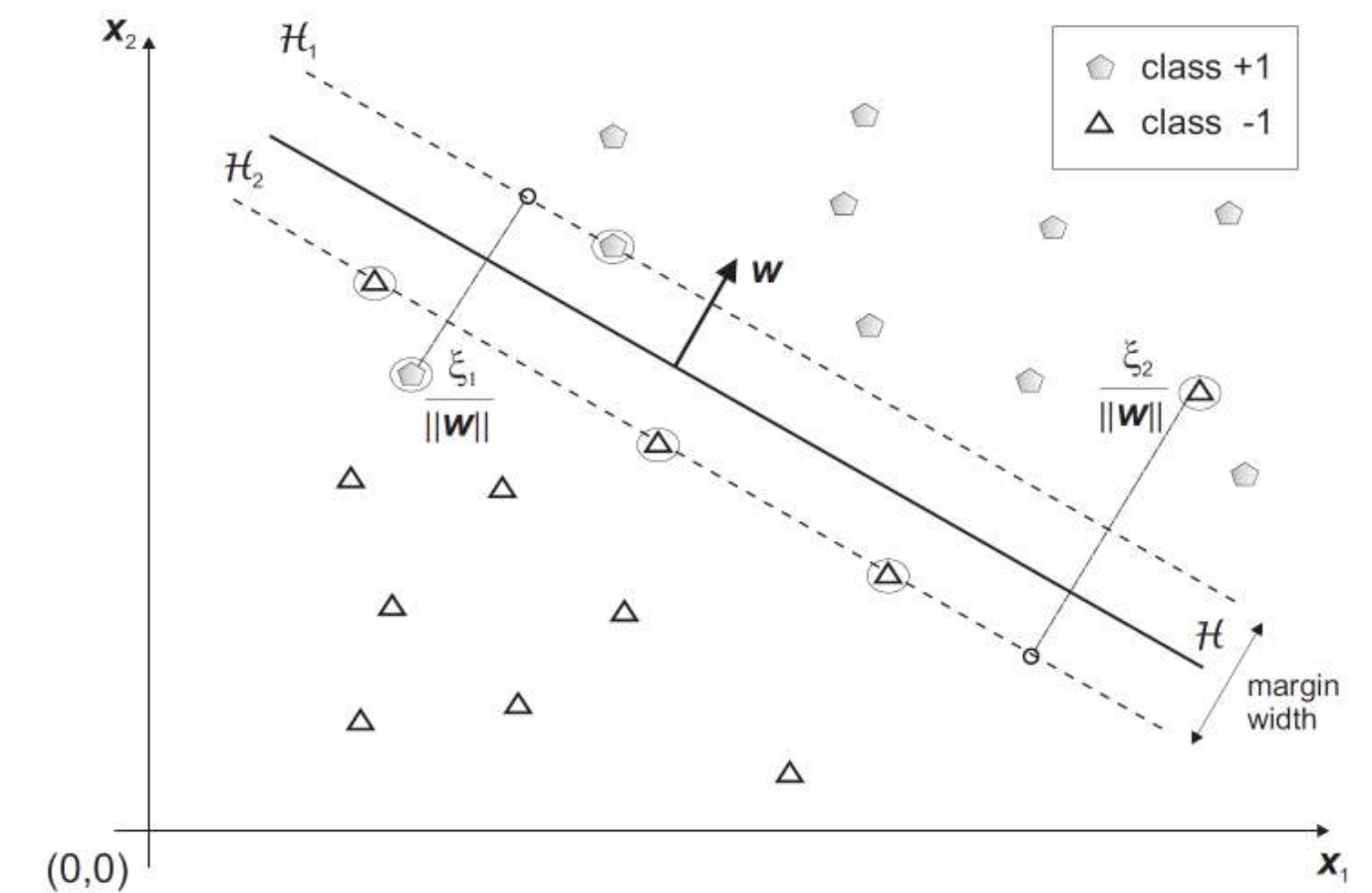
Positive-Unlabeled Training^{*}



^{*} X. Li, B. Liu, S.K. Ng: Negative Training Data can be Harmful to Text Classification, 2010, EMNLP

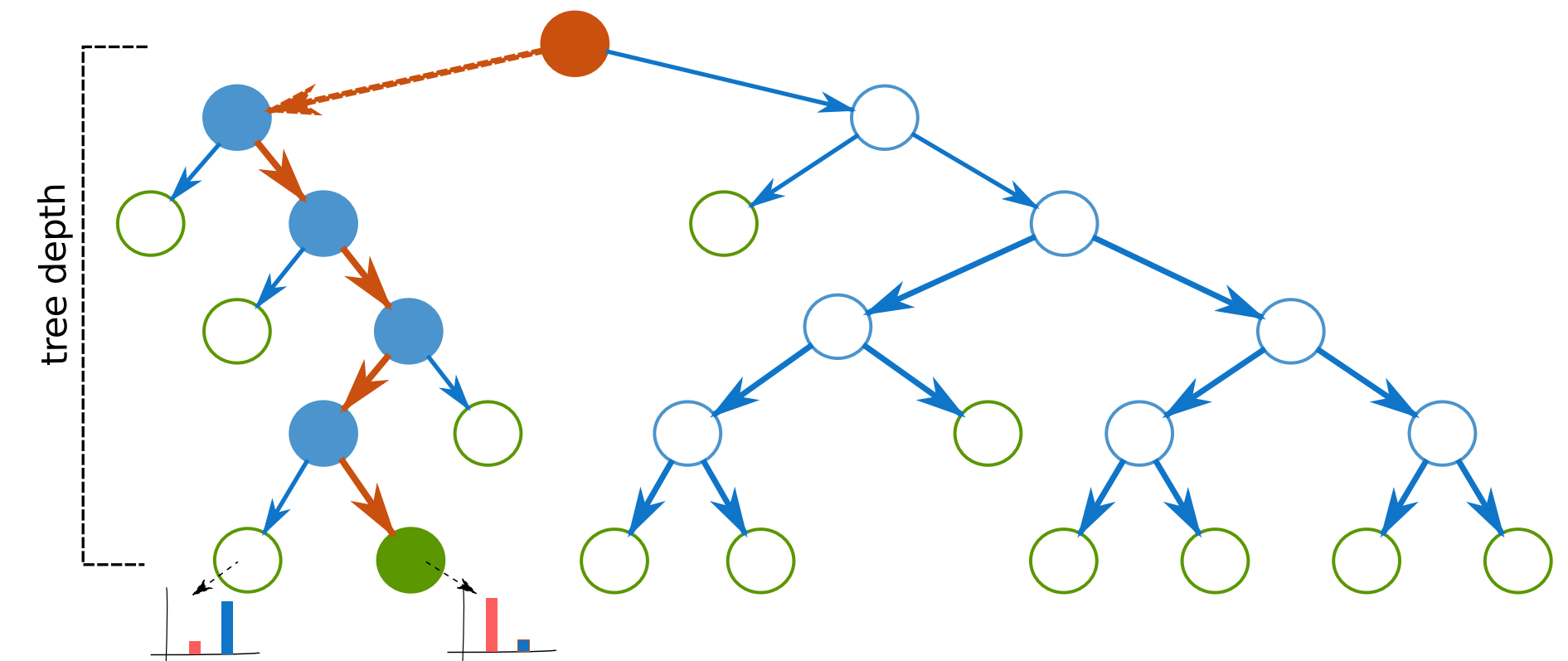
Classifiers

- **SVM alternative** – MIL representations: Challenge #1



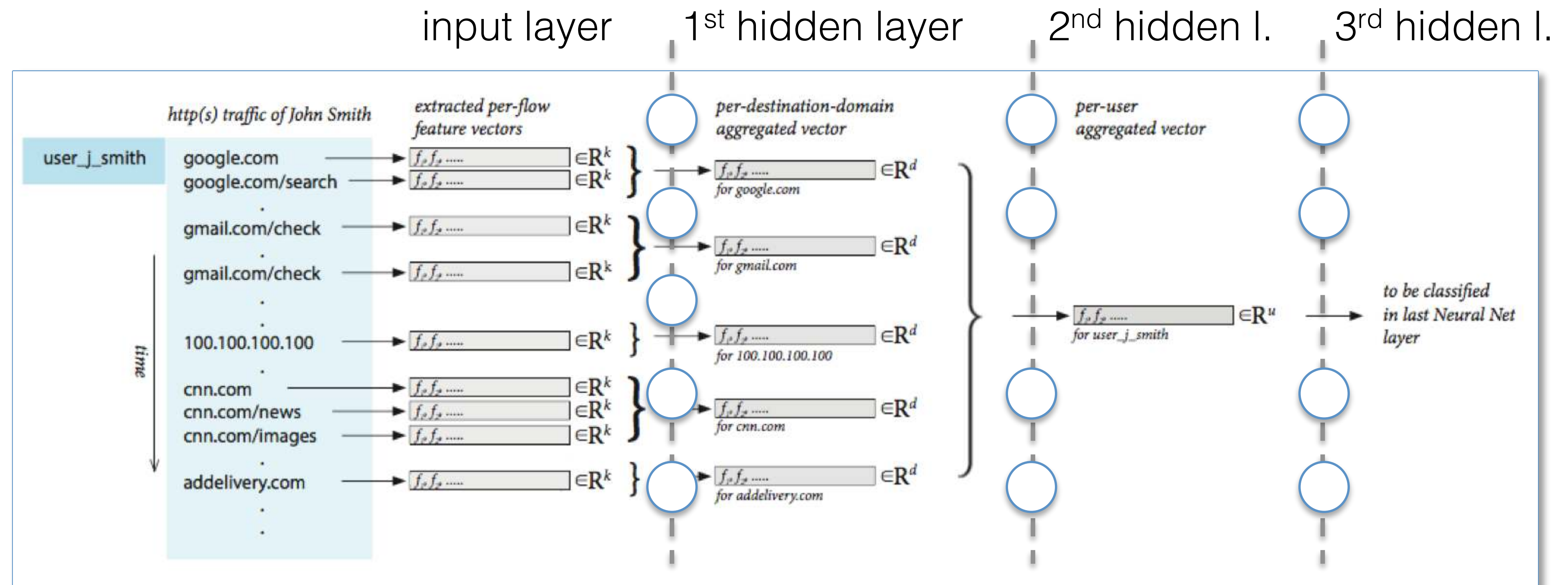
- **Random Forests**

- Randomness involved = more robust against evasion
- Multi-class classification
- Easy to train and run efficiently on big data
- Used prevalently for per-vector classification

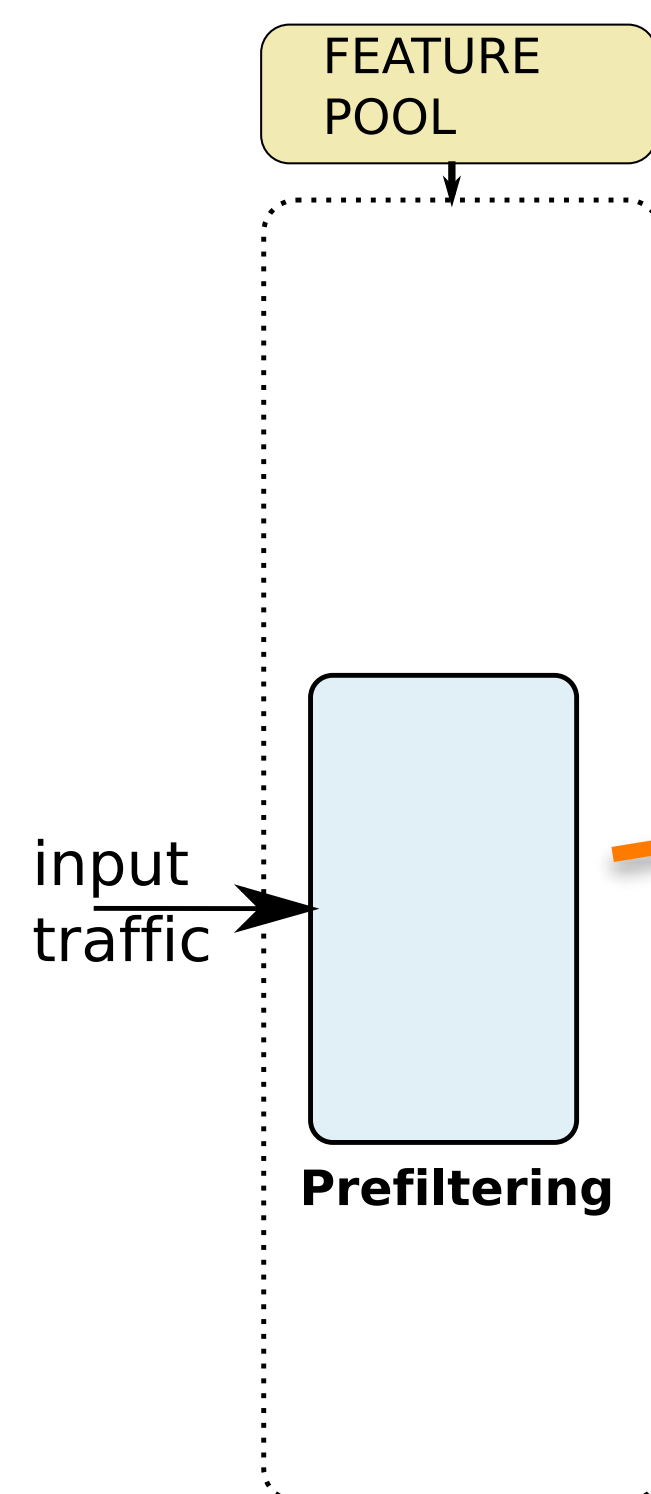


Neural Networks*

Used to classify the traffic on the level of users

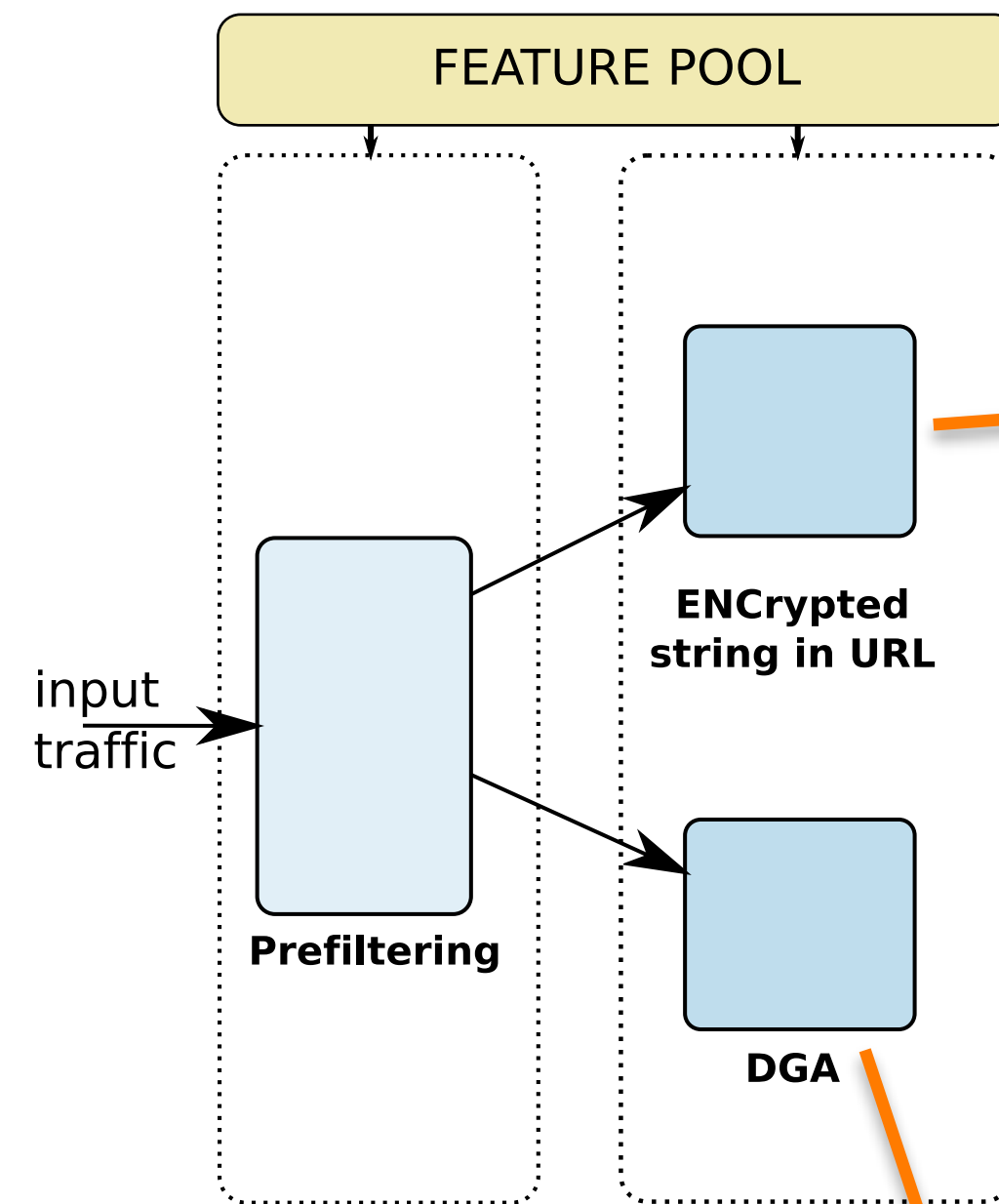


* T. Pevny, P. Somol: Discriminative models for multi-instance problems with tree structure, 2016 9th ACM Workshop on AISec with the 23rd ACM Conference on Computer and Communications (CCS)



*hxxp://cohostro[.]com/keyJjIjogMjM4MiwgImYiOiAwLCAibSI6IDI2M..
hxxp://cocloudex[.]com/peyJjIjogMjUyOCwgImYiOiAwLCAibSI6IDI3..
hxxp://adminxhost.com/8a766814986811e486083c4a92db07ce
hxxp://findreek[.]com/cen?ag=de6b7ffbf8a767e8bdecbb805143bca6-2..
hxxp://199.182.165[.]105/c.php?i=DFuwjKoDUiUNzF8Qnn%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
hxxp://lkckclckl1i1i[.]com/zKG2ZB1X6M5xt5c1Y2xrPTEuNyZiaWQ9..
hxxp://109.235.54[.]162/m/IbQEZVVjipFdkB0KHeNkNuGBabgSr2z3..
hxxp://78.140.164[.]160/jjlqXpP/~GIja7A3q/KqRSx+1s8kNC=/%2BsL..
hxxp://masterproweb[.]net/images2/BD3006FB490CADF111E40696D3..
http://www.thespec.com/DependencyHandler.axd/L0Rlc2t0b3BNb2R1b..
http://www.degruyter.com/assets/virtual/H4sIAAAAAAAAAAKWSwUo..
http://www.1001pneus.fr/ls/YToxNzp7czo0OiJwYWdlIjtzOjY6InNIYX..*

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



Malicious

*hxxp://cohostro[.]com/keyJjIjogMjM4MiwgImYiOiAwLCAibSI6IDI2M..
hxxp://cocloudex[.]com/peyJjIjogMjUyOCwgImYiOiAwLCAibSI6IDI3..
hxxp://adminxhost.com/8a766814986811e486083c4a92db07ce
hxxp://findreek[.]com/cen?ag=de6b7ffbf8a767e8bdecbb805143bca6-2..
hxxp://199.182.165[.]105/c.php?i=DFuwjKoDUiUNzF8Qnn%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
hxxp://lkckclckl1i1i[.]com/zKG2ZB1X6M5xt5c1Y2xrPTEuNyZiaWQ9..
hxxp://109.235.54[.]162/m/lbQEZVVjipFdkB0KHeNkNuGBabgSr2z3..
hxxp://78.140.164[.]160/jjlqXpP/~GIja7A3q/KqRSx+1s8kNC=/%2BsI..
hxxp://masterproweb[.]net/images2/BD3006FB490CADF111E40696D3..*

Legitimate

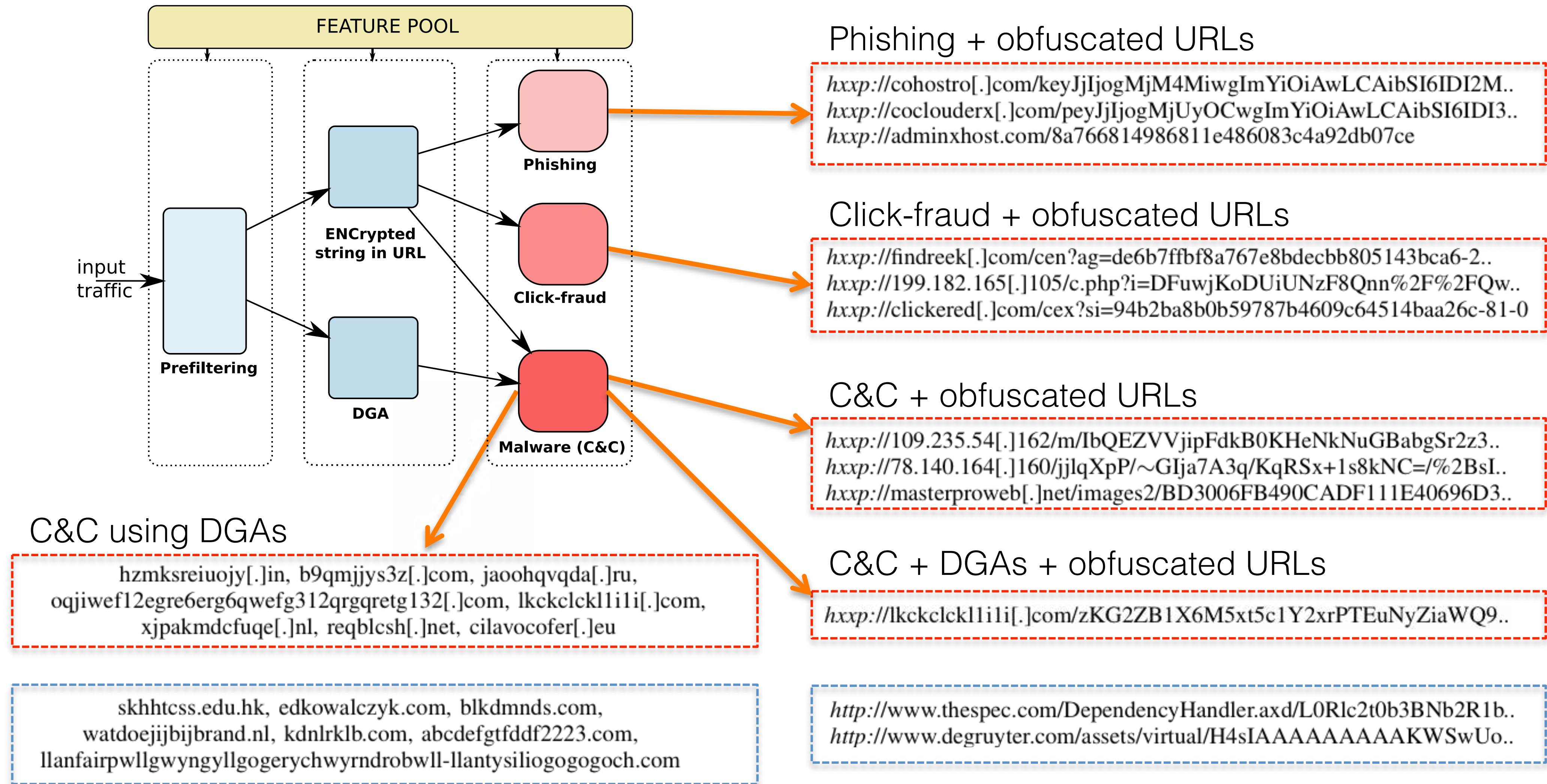
*http://www.thespec.com/DependencyHandler.axd/L0Rlc2t0b3BNb2R1b..
http://www.degruyter.com/assets/virtual/H4sIAAAAAAAAAAKWSwUo..
http://www.1001pneus.fr/ls/YToxNzp7czo0OiJwYWdlIjtzOjY6InNIYX..*

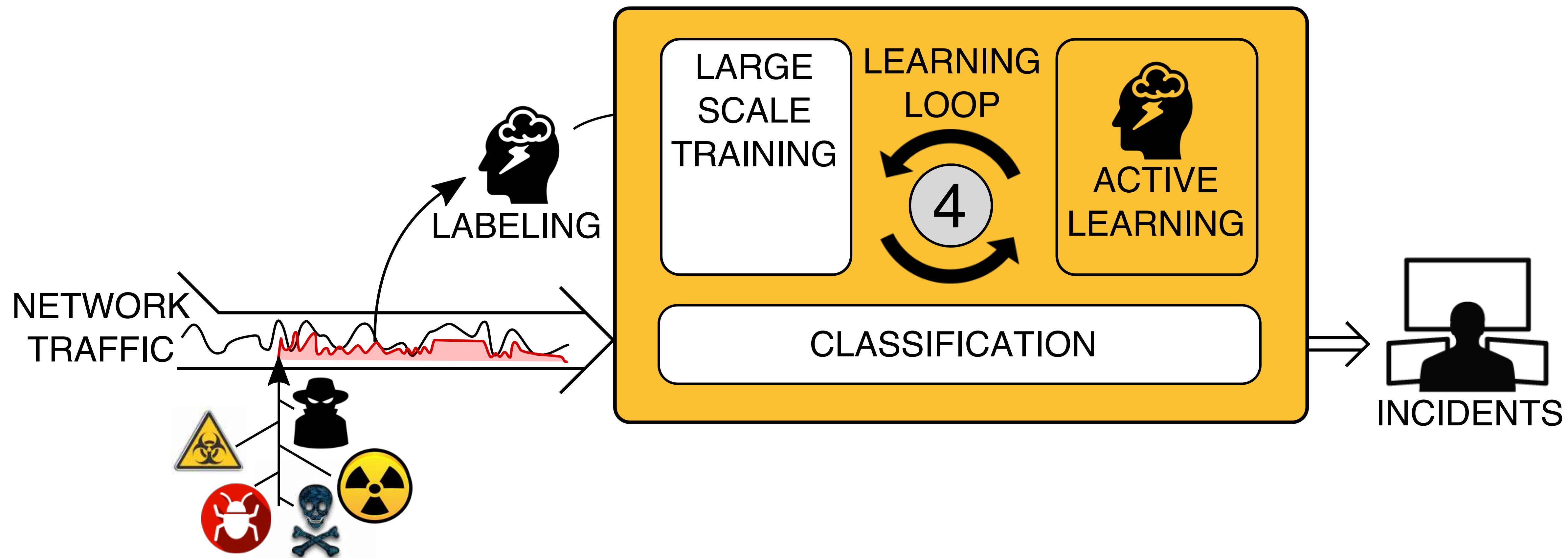
Malicious

*hzmksreiujy[.]in, b9qmjjys3z[.]com, jaoohqvqda[.]ru,
oqjiwefl2egre6erg6qwefg312qrgqretg132[.]com, lkckclckl1i1i[.]com,
xjpakmdcfuqe[.]nl, reqblcsh[.]net, cilavocofer[.]eu*

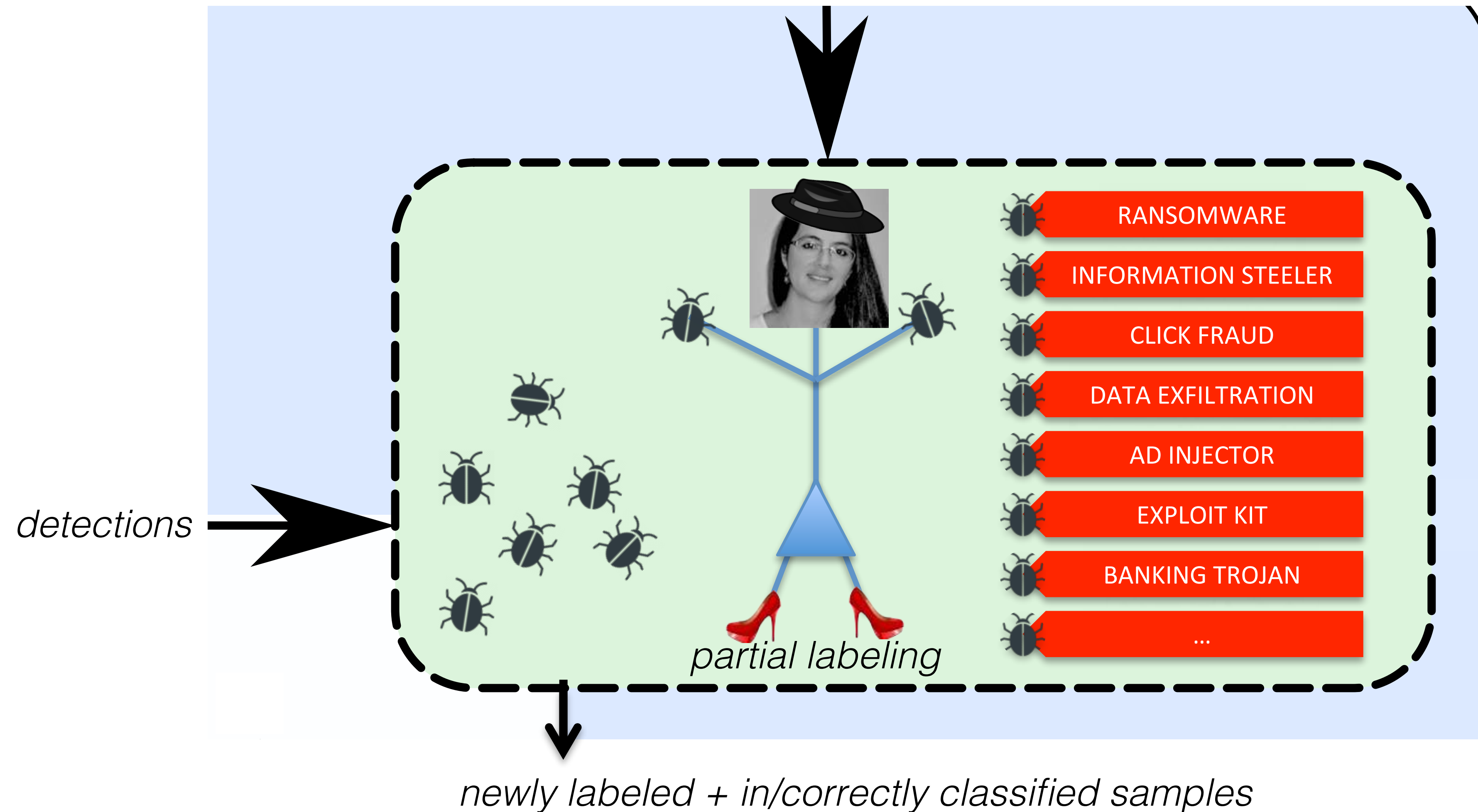
Legitimate

*skhhtcss.edu.hk, edkowalczyk.com, blkdmnds.com,
watdoejijbijbrand.nl, kdnlrklb.com, abcdefgtfddf2223.com,
llanfairpwllgwyngyllgogerychwyrndrobwll-llantysiliogogoch.com*

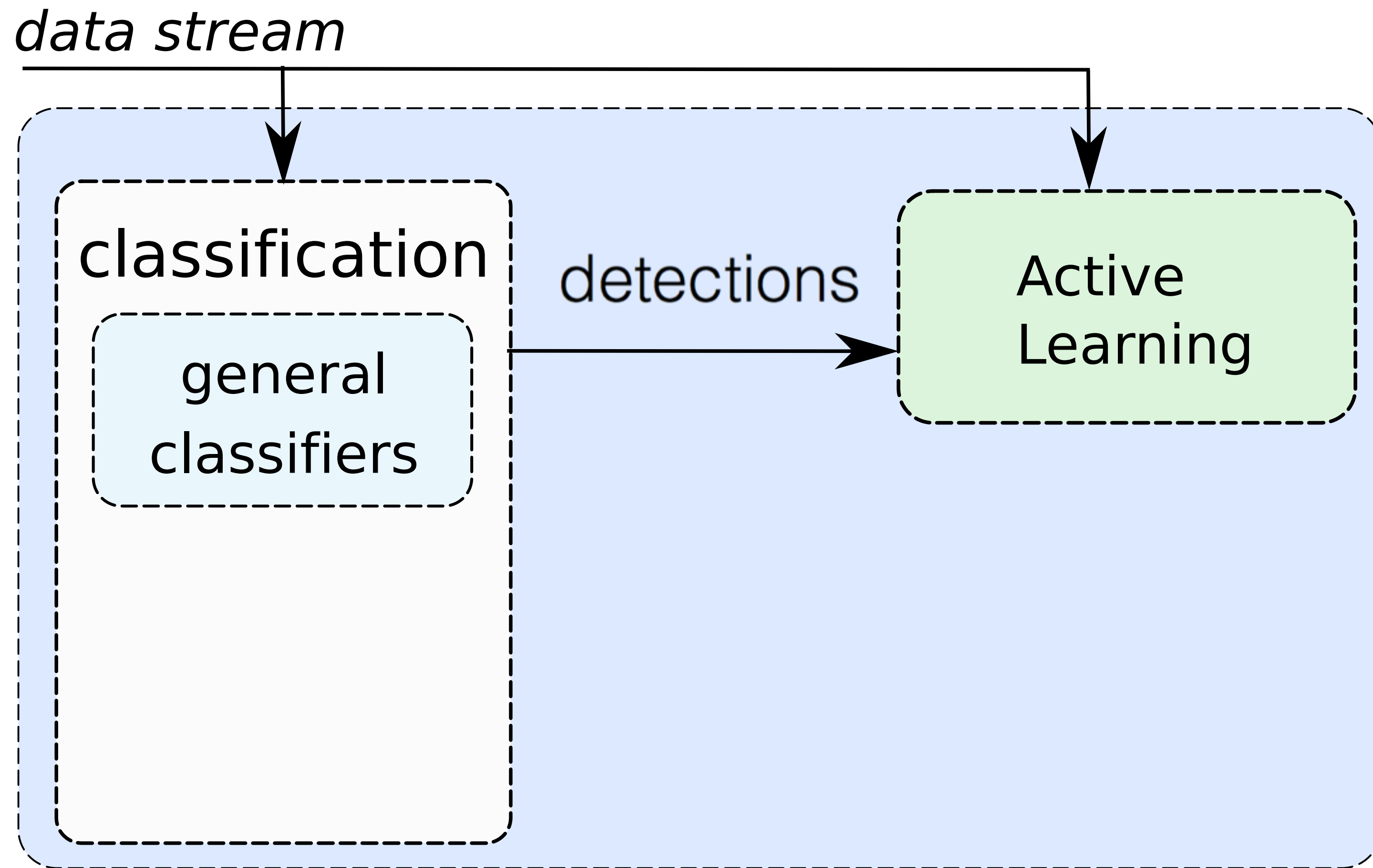




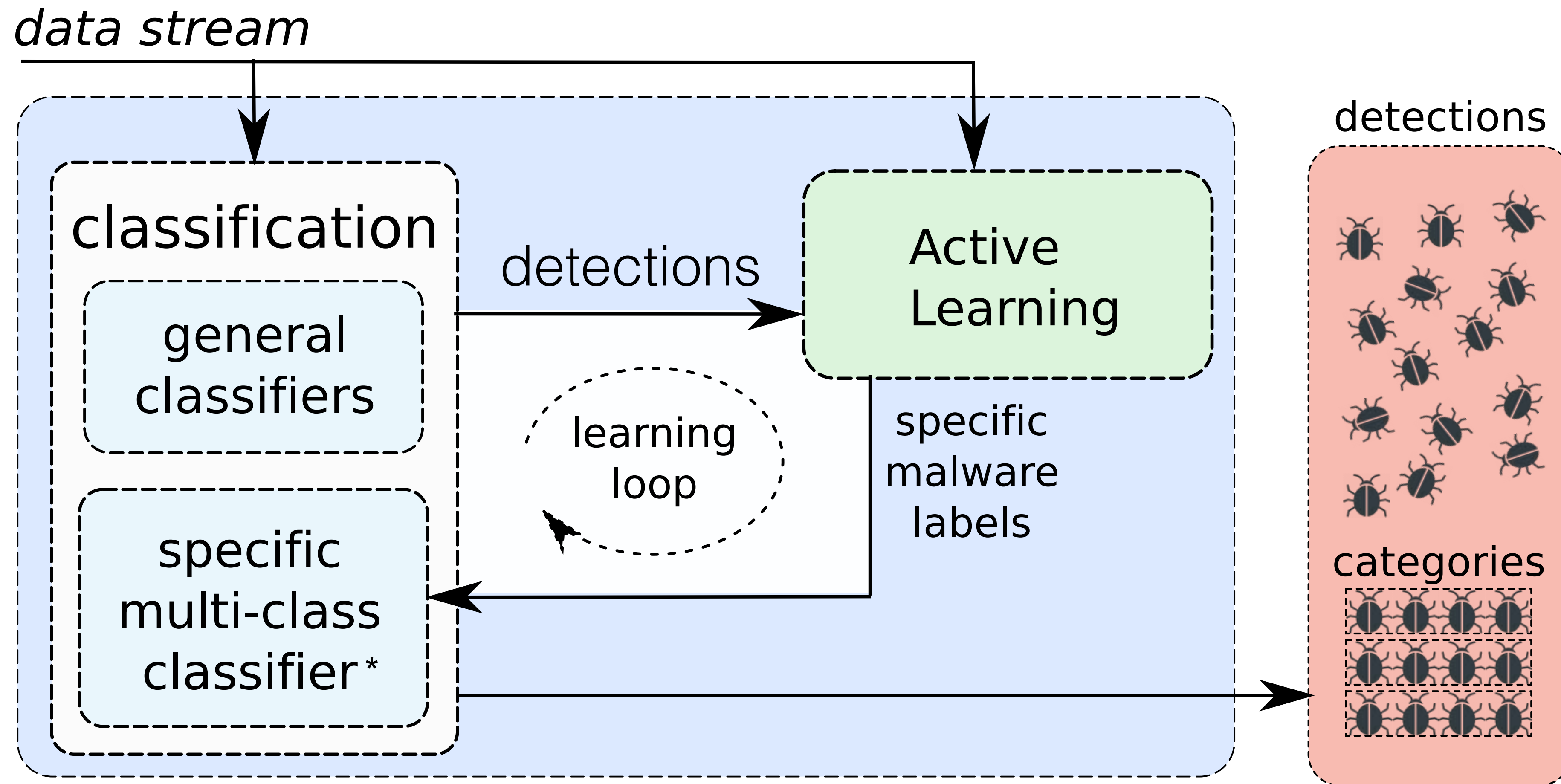
Active Learning – exploration vs. exploitation



CTA Classification and Learning Loop

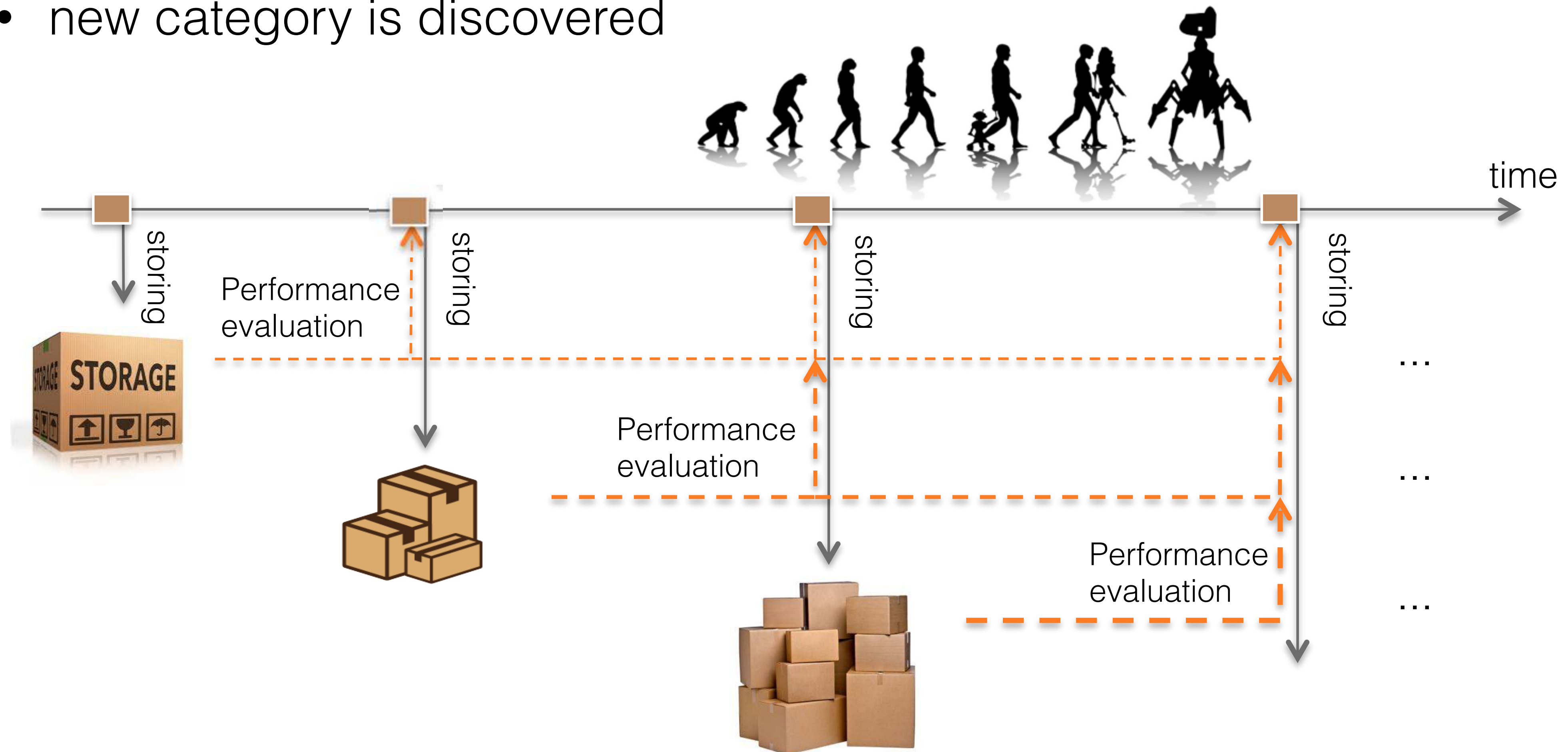


CTA Classification and Learning Loop



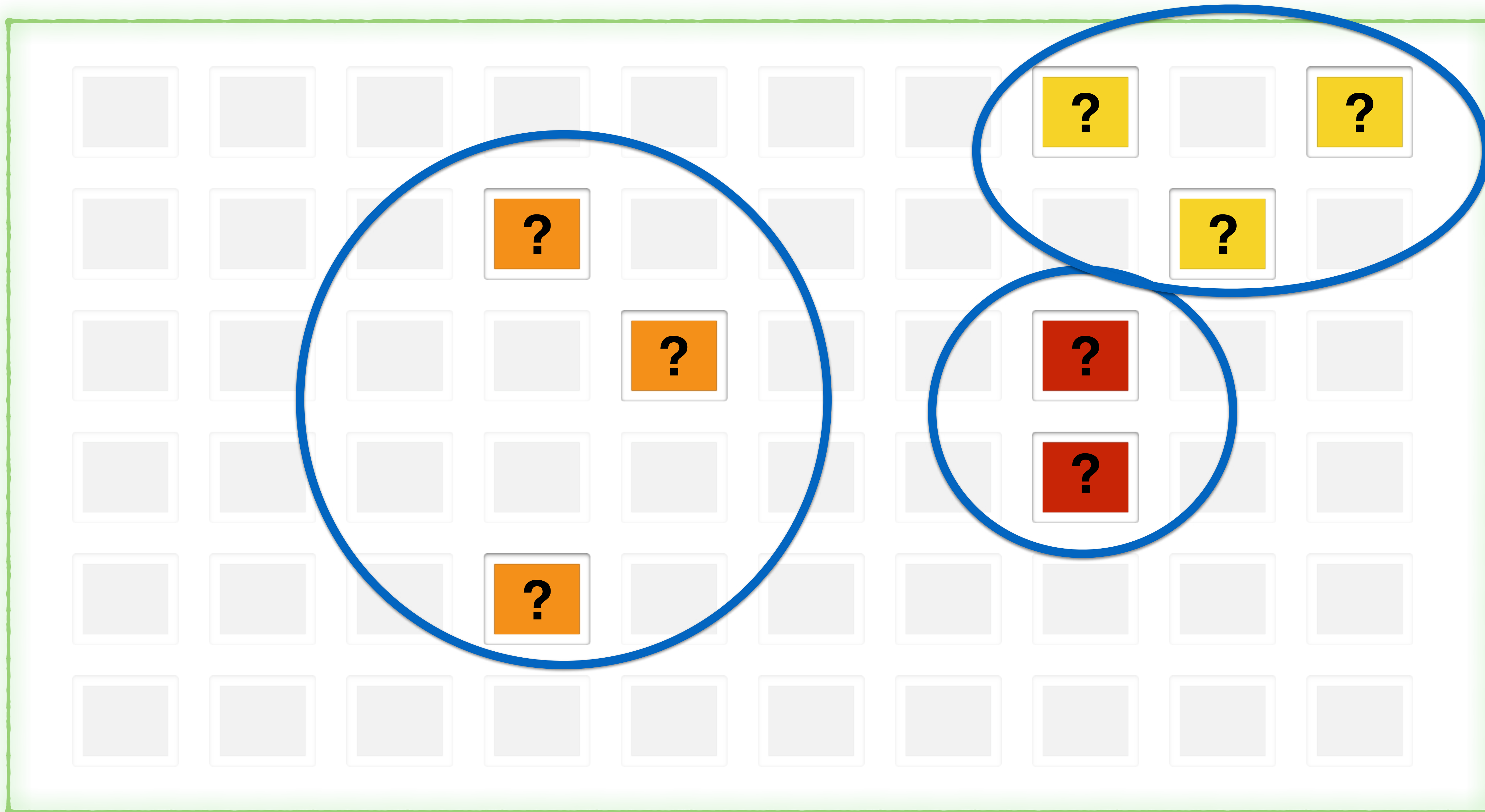
* We use SPARK to train the model (with 200 CPUs it takes approx. 1-2 days)

- **Automatic retraining of the classifier**
 - based on **new samples** in already observed categories
 - new category is discovered

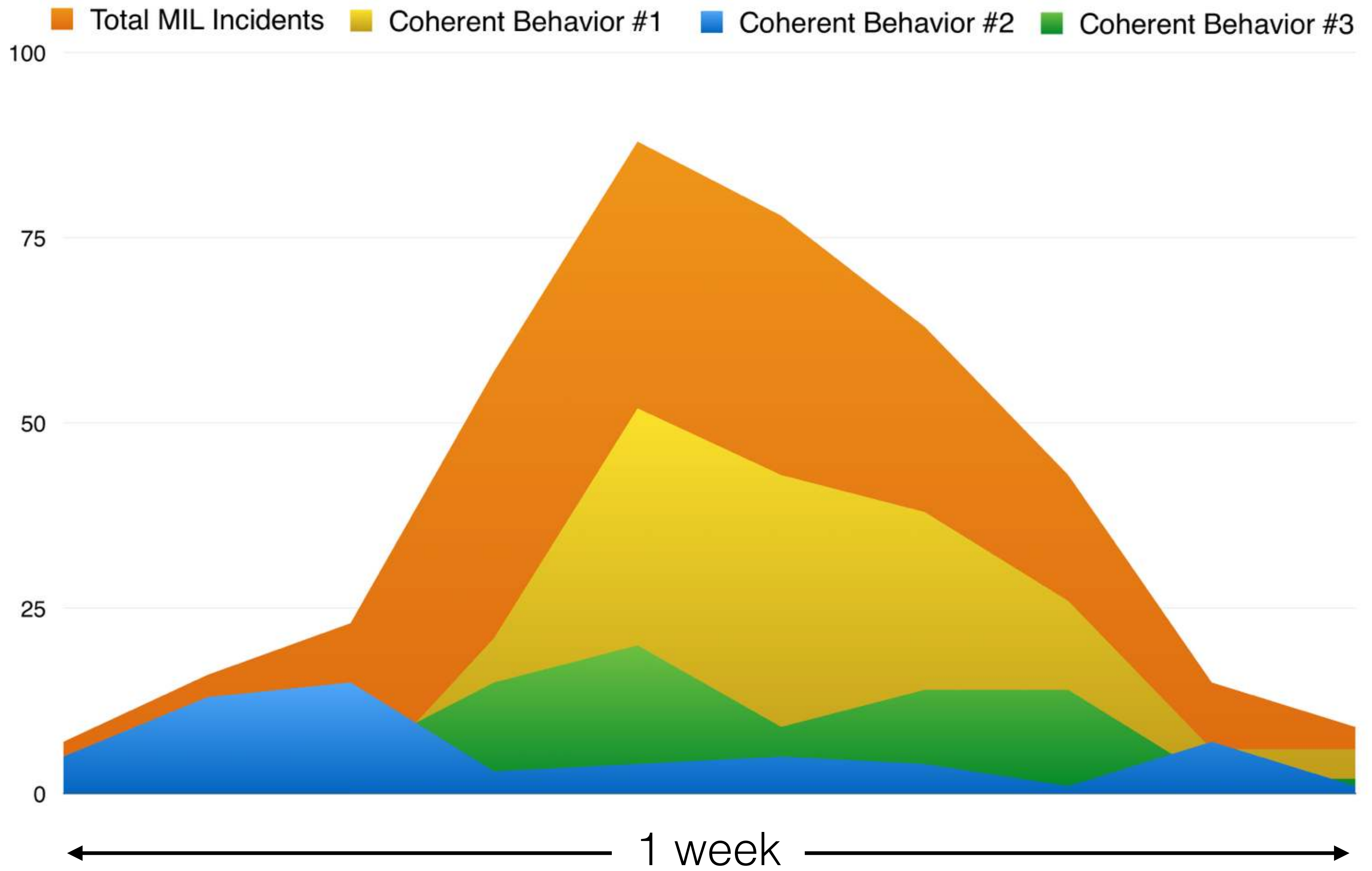


Real Life Example





DNSChanger



http://tablezip.info/u/?a=0orhl9LvTtd2301AbA3AbBoS08fcV0UsugrwSrOwFXaS87gzBW-4lPF2BrMs5hXuJAvufgwl20NI-wRdETcfSvq1Npu5F-lxktWkjf2KWchub6T1qVjklJlppKgH1wfaXVJBkkrR1VebQHWyFxfMq6QCL9gm3x9WdMOnQj2Slk6bN3XJytSG9l
koopzVCDRPeoMXJLeicxjNrFfjGPPYsYaqZ6tcgAc5tUTtWleKtF0VMtJt20p28bpfH5p6X_hOQgyVAFysG_mqSqlSuFVN9c1wQFAqfaw2n3ydikujUYWcZ87RipjhjUJ_vLY6_nS04ecmAEAnME1evmtuL4KXVybQLYEnRZhob-z7NXvmW9kPVWfq6hdwLch_XSYcY1;
Wi38lbnlRIKipZjXtwAfuMn5VMDyUwy6gEyBo0XA8Nc2RnbaFNoj37buEXhZleS-qWrJvxT5VKk3hcFu4OCFYWat-sCacDRQktkOFo6KShV0GulPgP4LSJDDlaF_jgTQ09J8WfJhGHFB_-vqkBK5yKMaR9zTrLW13EeiEwE7UpnUVGrcjqZQJRX6x30_MUIRHJChALUb
NaLl4Kkwl_hq51E98m3lloM75MCKxll_xYbMs1CViKlL_NWtE8R3WzE80PIA_I5QZ8c- IflIbfup2V90MP5mEvQWpcMwYCGww0cDqlp3_wbP32pxxt5wzBw8Tqt6lie53qlnpX7GYE14r59L_eBGCsRyEFTonyz45rstnrfKp6PRFAo77i0SzBcBTHiE6NylV/f72m_M0r6OwhD

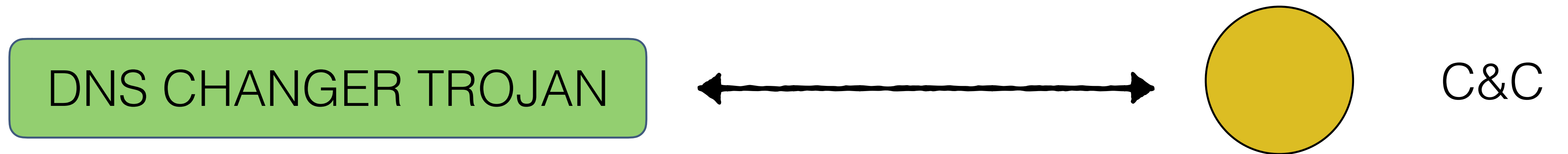
http://easypop.info/u/?

a=SKA3fIn2V9Pygoh80AFd4tR809WrWauz08ejnJeiA7HcmBgz7iR0LSXVupTV4Zq0Kj fGtN6zkF0qTQwrxZsSbHfo3z5pNfjxkLtX_c0NY0LRF5JFen_fzGs
0YU6cCgz6oMqogR80LR02NBhsu6H9mLAi0PIXX8XsKkbbpWcrqU2z4-
oPnBei0Fuj9rnSGgUIx2sUMj6KzDP6PEgdsWxt_VQodAyHo9DjmB9w5xGLD3pl7sIsPEvhZg5RDVzbLf03rpgsL1x-
QwGA9lqV9WxraPkERXQ3Wh5Bq3Ftl7euZke-HzQx-
QpNE9tQtxIu_uFGcIPAAzhfaPTiimRN4cPfBL3YvXaXJr52Q6fnlMhl8DeV4AC0GzTZ13DPY6JKI62fA6J4f1xZxPFonYLRXis8sogTUtPLRgcLFHUfCiCboZ
ax59gr8m94F70YoTejlfttAHA7LOJzGGGV4of_7YcgU0Am55ClbiGFp0yLGL_YyMX3pUiHd126UL8dnMPW4QMYbVur4dZVMc3rAgC1sJWVT-V_6es6dm-
G2cuYufwXrzWaef6o8_fpvprG7i1n6FU1_l1lamotkD4-
uIFpUJTZWUny79PfgwwS1n_3xWV1sCxWw9uHHhgcknFef1i1DPqP5eIq__KPc2h_aZaMH2FdJBDrMybMMpvPYKYKsrT3oBNVyTgPg5ncMYCFDdjxxSN-
y8HhxWj5ajB3Mw-euEKeoZAtx_vv-
lotvXeWfdJ0_vI9ZfnIjuVHbITagARPntiV9cC733IZa3ChsApBK6y56p0csh3DCLUS4LLL683AwwjKpL5ehCcpj0t0pebT-
GErhT2kN_DbtigbG6rgqevrFCoViKv1IPUNW1mp-wTnnNuEpc9x_ykcydASp5srVsrZ

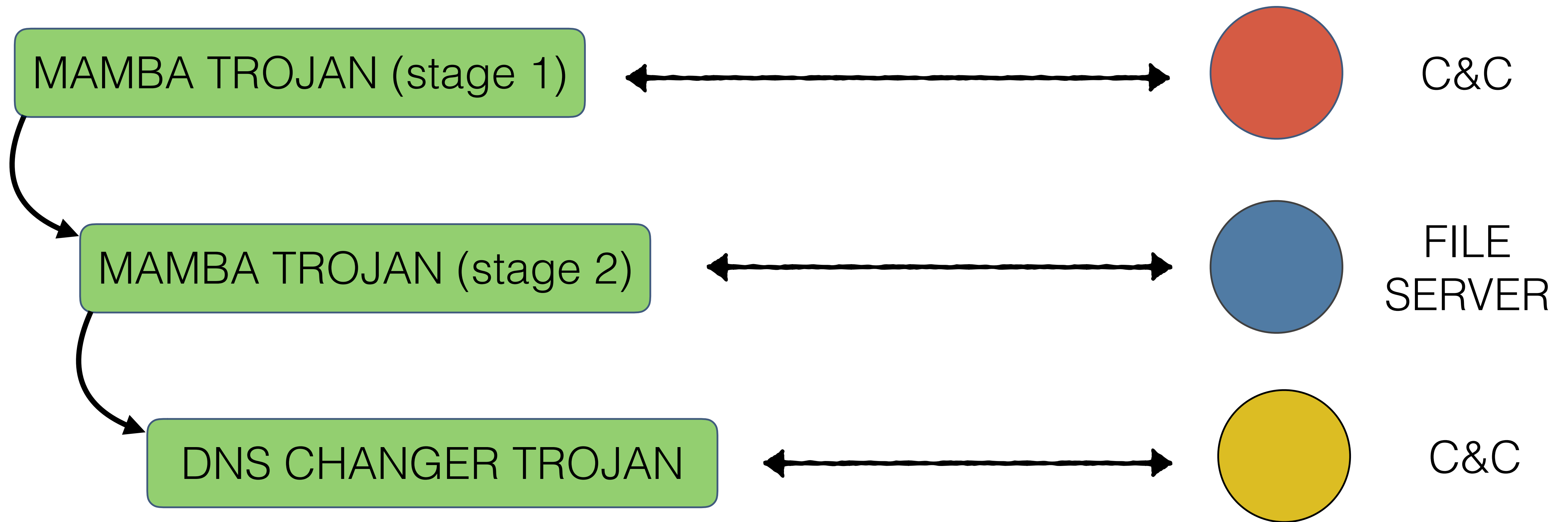
&c=zfVypc6VB7vBHYzfgPwLwY-DCAREZ82hzq3QMMlCT3NQxc7sLKeSstFxzCDHsCBz9VcuQ1-MDBM3ZsQ8DKmlyqEkgwIE-
JXVjsBsGjvE6Yd7v1Cm_C7gd0M2qvIp0MiQ8gpceM0XHii31Nfp9ME0f81HRwZayU8ur7fuRVSecIFvmm8gEUSmtM6YSYVWKqcMU0yL07xghihVCiAmbMTKIi
ld95UXLt0-6XeLFayjFPpb1JeiBrmfZk850Kp17Nzw3qhqcFPhduD5m01wqHa2qa0Mn3WIXhjWNFhdGRUsB911DyDFYDMPKSvc199YDPbzJ3X7rCIKibnYEM0
QJaWlPvYPrWfBU1zZe1kLx_c0DNckrw6Tze6mlPp4LCTRDmqgEW37gnoAgPf9xPpdWEtIddYWlb7SJSj4ugMZWYiVkkUMs54XG1gSVTTldYj8miLXKLtGyJRe
Jdxp0w9Mpwb9Ron98mcP-
BiT9sl4xV9gfsB8Lt0vcL6s5wHo5Uow2HlAWXndFbAdEjtijv01BVgyVzzvqV3hkIgn_TNZcckusf5qvPH6YHjl67I6Cyef6c6r0ycaz8eulPrdA0TxFN1Jpf
kRvaTnskV2XoZ5mAjcw3_bYFSSHAgPzWLiCu2uj3ftqrG9i1Sx_oeqSHRoNwe2YhYIJH9vZpSfSBWnCCvgC5pJK_1vpsIruX0rPlsBng3i5crHM7MrBtUXNe1
pmQurqDdgfhMdbheG5437gtBjUZP4iKVuX6aqAzhLi03FpogZl4Uj1HiLPXbVG5xaS3k10CYK0Hwv_vP5gB8X0JtC5QUi6_TGWdXY-0YJs4qU-2dWRHrjmyI
6cmt5LIEE7RPBKMEA8fR3wmxbAzm8g9Z2RqrhJKKEmxWQxGk000C5Qtsqrre4R_Q7ajwo2ibAQaP3td

&r=2667415679646581680

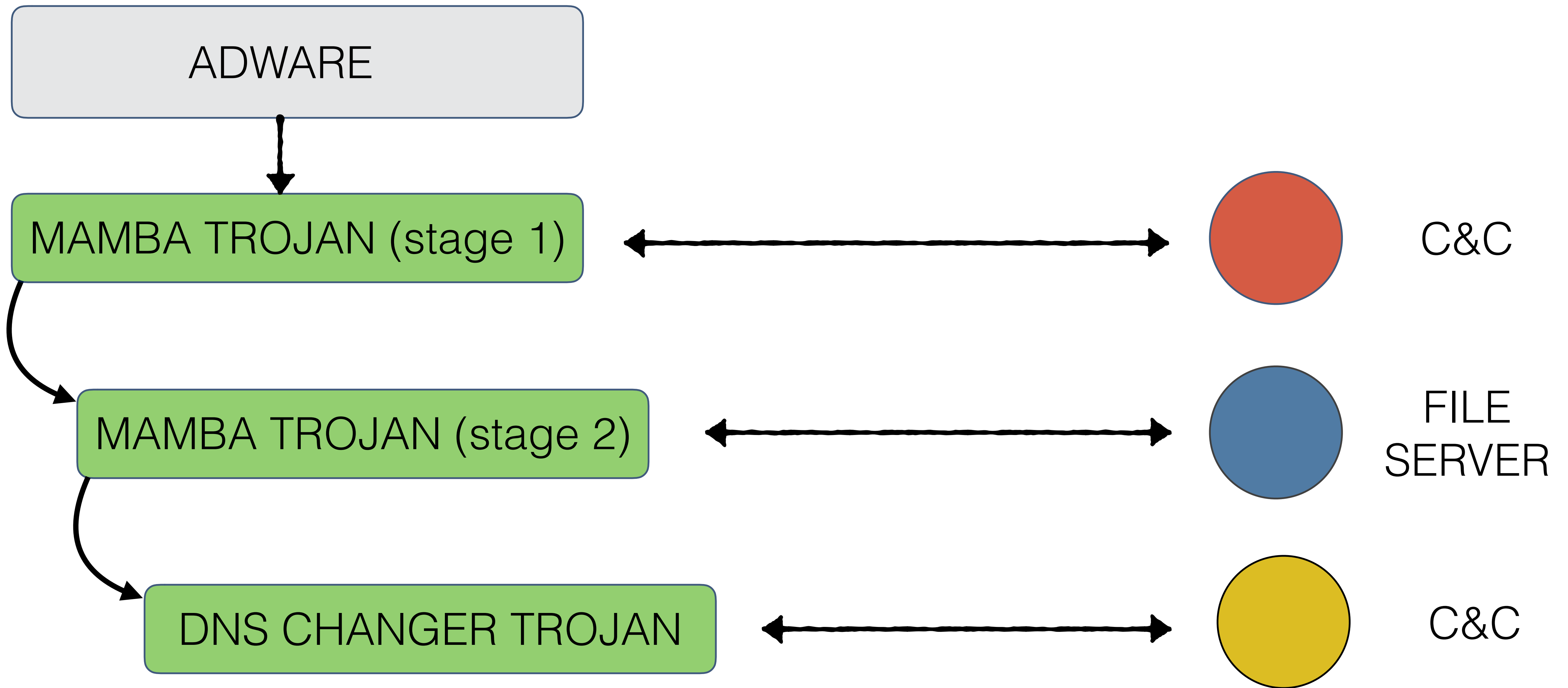
ROdUdMo662eGLxt9hrrkrleluWXdbB8m6VA24Fj8blUs8SHfb8Baeq1jKDNoelg8ZTlfDXUwjoOFFaie7XWpTfhkrTlFGFb5z3bn8v8mlWXxXYf6RslpyBkOvUCBDD2d31YeXZlwhW9Lt0NQjx4ZL3lCMzqxq0d-d096Ki_Yc54p6774OUR2JoeM6XnAJ50zuSfbB4ks3l7Cl
uLx1UiNqFVskWmePNfxArYulIT2bj7L8iyrpqTqYXi_JMVCEmKHAJaTPYst-tBeFOLyWD-VN4b0j1Y7Ndjq19J7s1ToXlfc67WQoNeU33cb62uQlOBIUX7TvBGGYQXbrf1sSCo0vKtbbBbawpr_pJNb7&c=IPqkCFMgPHJwvklb86tLGx5qRdhcB5SqeQLh3AL13Ug_6Xpli
89HE6tT1wQz97Mryjly7F_OnPAxlzelvXSACfVCX0Bdevv5-Vw5psnFASIZIDSaoFcJloyuhQ99pUYcEYg5TtNAFLt8RQ5Fc9kDLCCSE32WYSO7KRru_2d7LSAjPr5pXZnCmuj4l_qNuBNmQruytlcBnjB0DXjuPdkhPuckKTr1Zewd71iyj5qPvf1Zz837QBKPH5aSXsvJZf
QCK40HKfA7Eevht8fIXtwa2adNRkU4Q9MpovXxxVfrlVosleASBSByATAvVjSLCzgGJarD535CXghRMagv1GCO4yUua5n7iluYNWRFgDk9E-B2Vle1XCGmHG0MN91pnD5KT3W1G9rXYb2m2692p_jOfCqM-G6jfYlvrG9sxc8Yky-Fd0D_Xj4zldQExY6MwQMMNsE
38yg7QzxWJ7-3WVO-LOE_mUWmwm-G5dYRxQ6EG0dS2ZsDJtV19dU7rFhuuyXk6pgk4bMLkoCVD4FgANwC1BmSNVeECHvlK0ilshsC9vMnCWMXB43Px657Hy7uWBMkyGFUxOUQYYqjc8BRqpPAyL4mGV2HgXhHilLTGe4jzLIP-4HYh4utsY2Vf&r=71640759;



Thanks to Ross Gibb (Cisco AMP Threat Grid)!



Thanks to Ross Gibb (Cisco AMP Threat Grid)!



Thanks to Ross Gibb (Cisco AMP Threat Grid)!

[**http://finhoome.info/u/?a=kLz-Yckq\(..\)&c=fPOnv\(..\)&r=987\(..\)**](http://finhoome.info/u/?a=kLz-Yckq(..)&c=fPOnv(..)&r=987(..))

[**http://domenjob.com/u/?a=D-2n5k7\(..\)&c=vTB5\(..\)&r=589\(..\)**](http://domenjob.com/u/?a=D-2n5k7(..)&c=vTB5(..)&r=589(..))

[**http://domenjob.net/u/?a=qk7BKV9\(..\)&c=m6V\(..\)&r=327\(..\)**](http://domenjob.net/u/?a=qk7BKV9(..)&c=m6V(..)&r=327(..))

[**http://listcool.net/u/?q=jW6H5obe2\(..\)&c=be2G\(..\)&r=684\(..\)**](http://listcool.net/u/?q=jW6H5obe2(..)&c=be2G(..)&r=684(..))

[**http://listcool.info/u/?q=J5DM4nrA\(..\)&c=rASU\(..\)&r=911\(..\)**](http://listcool.info/u/?q=J5DM4nrA(..)&c=rASU(..)&r=911(..))

[**http://usafun.info/u/?q=S42YFQPC\(..\)&c=YFQP\(..\)&r=769\(..\)**](http://usafun.info/u/?q=S42YFQPC(..)&c=YFQP(..)&r=769(..))

[**http://realget.info/u/?a=fDrS_9vLG\(..\)&c=GM0-\(..\)&r=528\(..\)**](http://realget.info/u/?a=fDrS_9vLG(..)&c=GM0-(..)&r=528(..))

[**http://alwaysweb.info/u/?a=G3ZGb\(..\)&c=wNR4\(..\)&r=781\(..\)**](http://alwaysweb.info/u/?a=G3ZGb(..)&c=wNR4(..)&r=781(..))

Ads Gone Rogue

[http://ddprxzxnhzbq.com/cVERg.htm?
l=1475373009865&p=3&r=313449&v=0.0013&h=0&k=&z=https%3A%2F
%2Fwww.google.com%2F&f=1920,1080,1,1920,1080](http://ddprxzxnhzbq.com/cVERg.htm?l=1475373009865&p=3&r=313449&v=0.0013&h=0&k=&z=https%3A%2F%2Fwww.google.com%2F&f=1920,1080,1,1920,1080)

[http://avrdpbiwvwy.com/asdds.php?
_750352&v=direct&siteId=1299913&minBid=0.0&popundersPerIP=10&default=
http%3A%2F%2Fonclickads.net%2Fafu.php%3Fzoneid%3D699158&doref=&s=](http://avrdpbiwvwy.com/asdds.php?_750352&v=direct&siteId=1299913&minBid=0.0&popundersPerIP=10&default=http%3A%2F%2Fonclickads.net%2Fafu.php%3Fzoneid%3D699158&doref=&s=)

[http://eeqabqioietkquydwxfgtvpzkuilfcpzkplhcckoghwgacb.com/
kKifq.htm?k=1474870164116&n=3&a=24892&c=0&x=0&m=&t=http%3A%2F
%2Fvidup.me%2Fsw6jvd1g05ye&y=1440,900,1,1440,900](http://eeqabqioietkquydwxfgtvpzkuilfcpzkplhcckoghwgacb.com/kKifq.htm?k=1474870164116&n=3&a=24892&c=0&x=0&m=&t=http%3A%2F%2Fvidup.me%2Fsw6jvd1g05ye&y=1440,900,1,1440,900)

[http://cdrjblrhsuxljwesjholugzxwukkerpobmonocjygnautvzjjm.com/TV.asp?
q=1474398263431&e=3&s=1153313&f=0&l=0&k=&o=http%3A%2F
%2Fonbokep.com%2Ftag%2Fvideo-bokep-indo%2F26177%2Fpage
%2F3&w=720,1280,1,720,1280](http://cdrjblrhsuxljwesjholugzxwukkerpobmonocjygnautvzjjm.com/TV.asp?q=1474398263431&e=3&s=1153313&f=0&l=0&k=&o=http%3A%2F%2Fonbokep.com%2Ftag%2Fvideo-bokep-indo%2F26177%2Fpage%2F3&w=720,1280,1,720,1280)

[http://www.xxyafiswqcqz.com/ZITV**k**.swf](http://www.xxyafiswqcqz.com/ZITVk.swf)

[http://www.xxyafiswqcqz.com/JQ**k**.swf](http://www.xxyafiswqcqz.com/JQk.swf)

[http://www.xxyafiswqcqz.com/**a**.swf](http://www.xxyafiswqcqz.com/a.swf)

[http://www.higygtvnzxad.com/Y**smcib**.swf](http://www.higygtvnzxad.com/Ysmcib.swf)

[http://www.higygtvnzxad.com/UCT**p**v**P**.swf](http://www.higygtvnzxad.com/UCTpvP.swf)

[http://www.lbypppwfvagq.com/q**P**D**ps**.swf](http://www.lbypppwfvagq.com/qPDps.swf)

[http://www.lbypppwfvagq.com/ci**G**k**KZ**.swf](http://www.lbypppwfvagq.com/ciGkKZ.swf)

> popads.net

Flash file (4.2 KB)

Zlib compressed

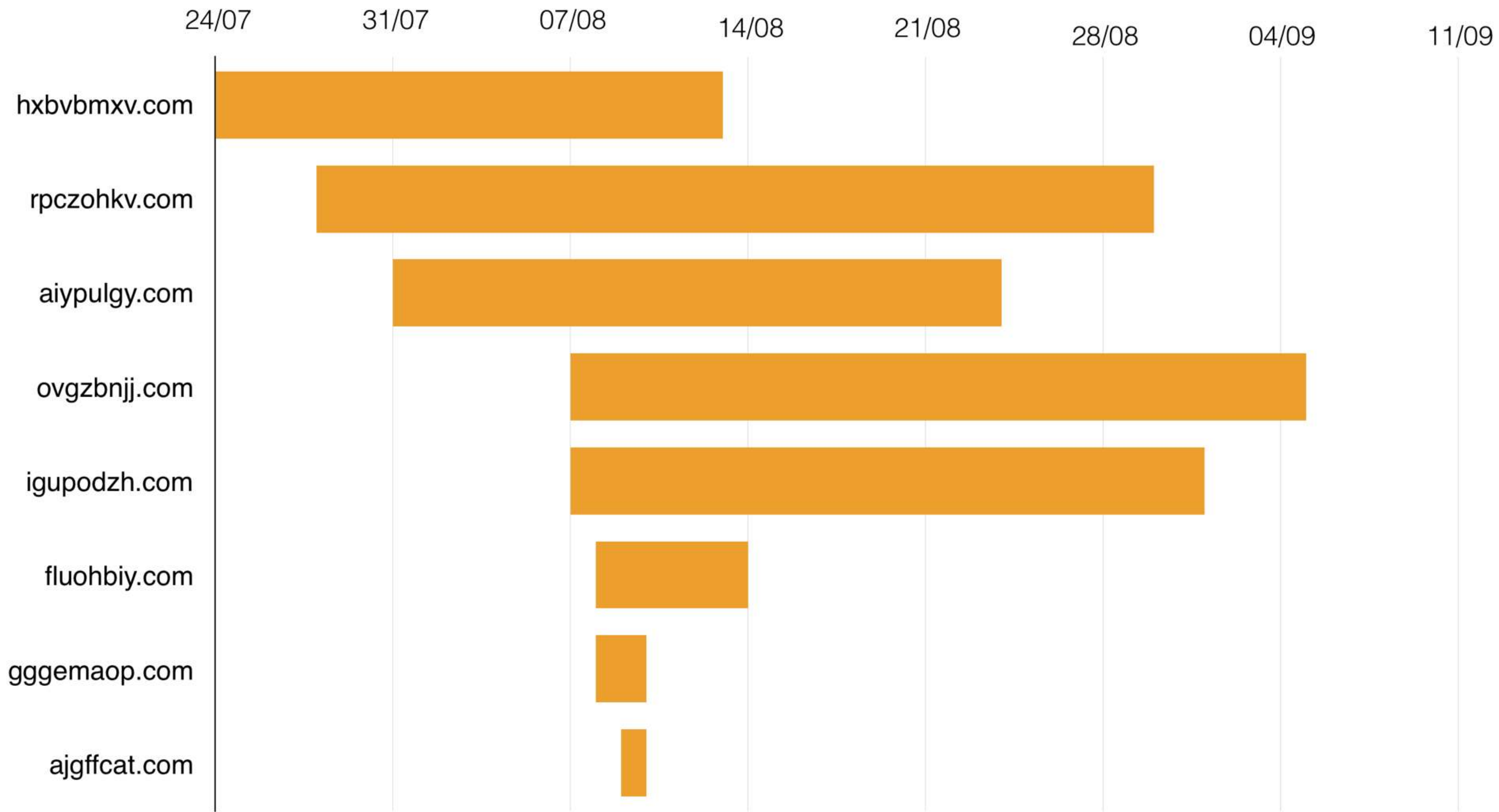
RIG Exploit Kit

bbd6e73b1eb7415c563c5ab3
4b4992b5

Detection ratio: **16 / 54**

Analysis date: 2016-11-02 11:20:47 UTC

Thanks to Ross Gibb (Cisco AMP Threat Grid)! & Avast Team!



24/07

07/08

21/08

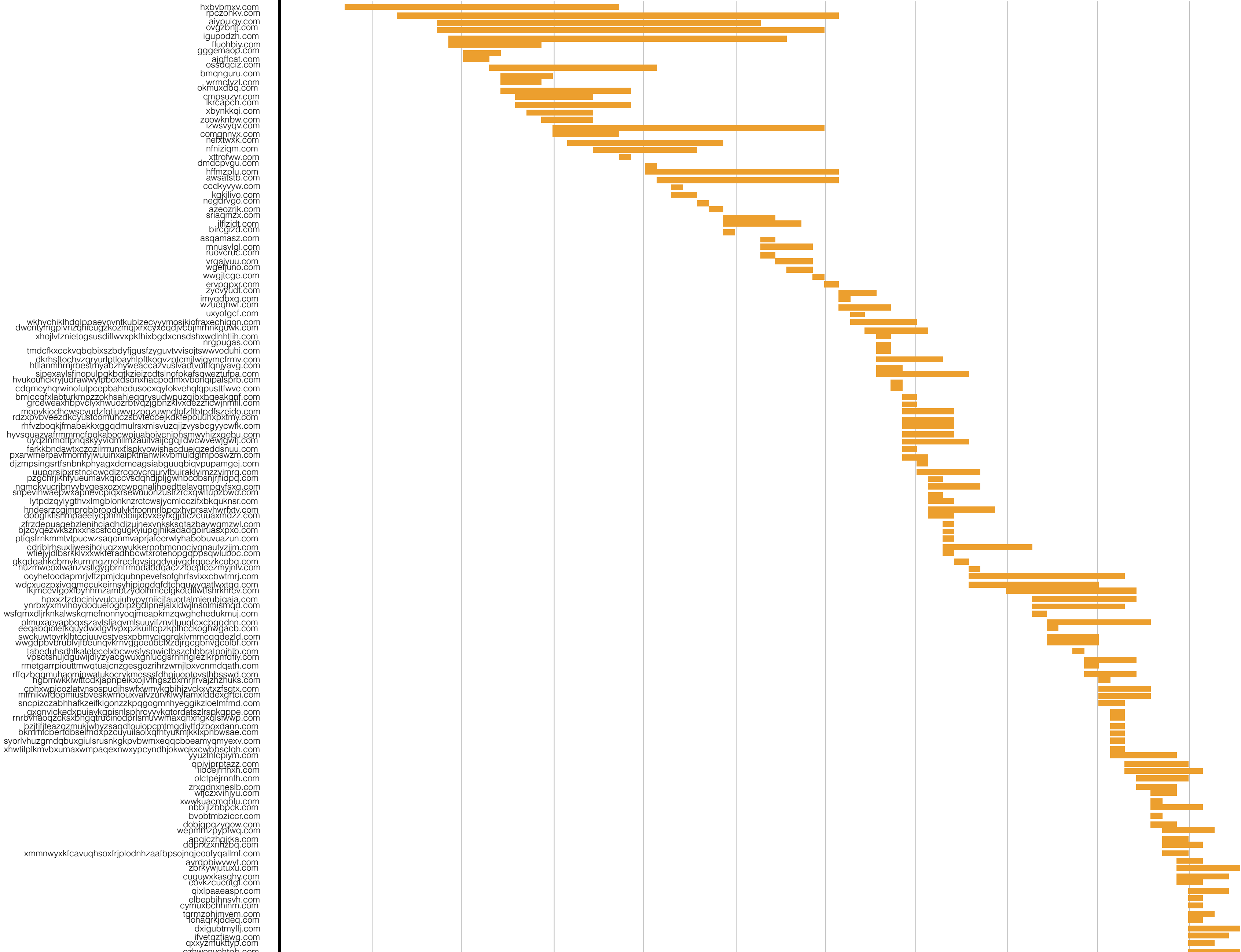
04/09

18/09

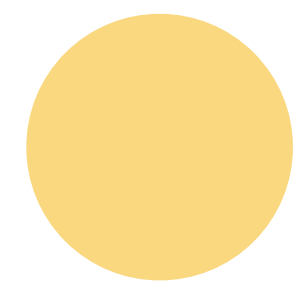
02/10

16/10

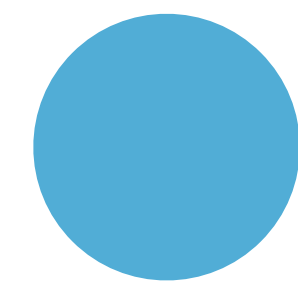
30/10



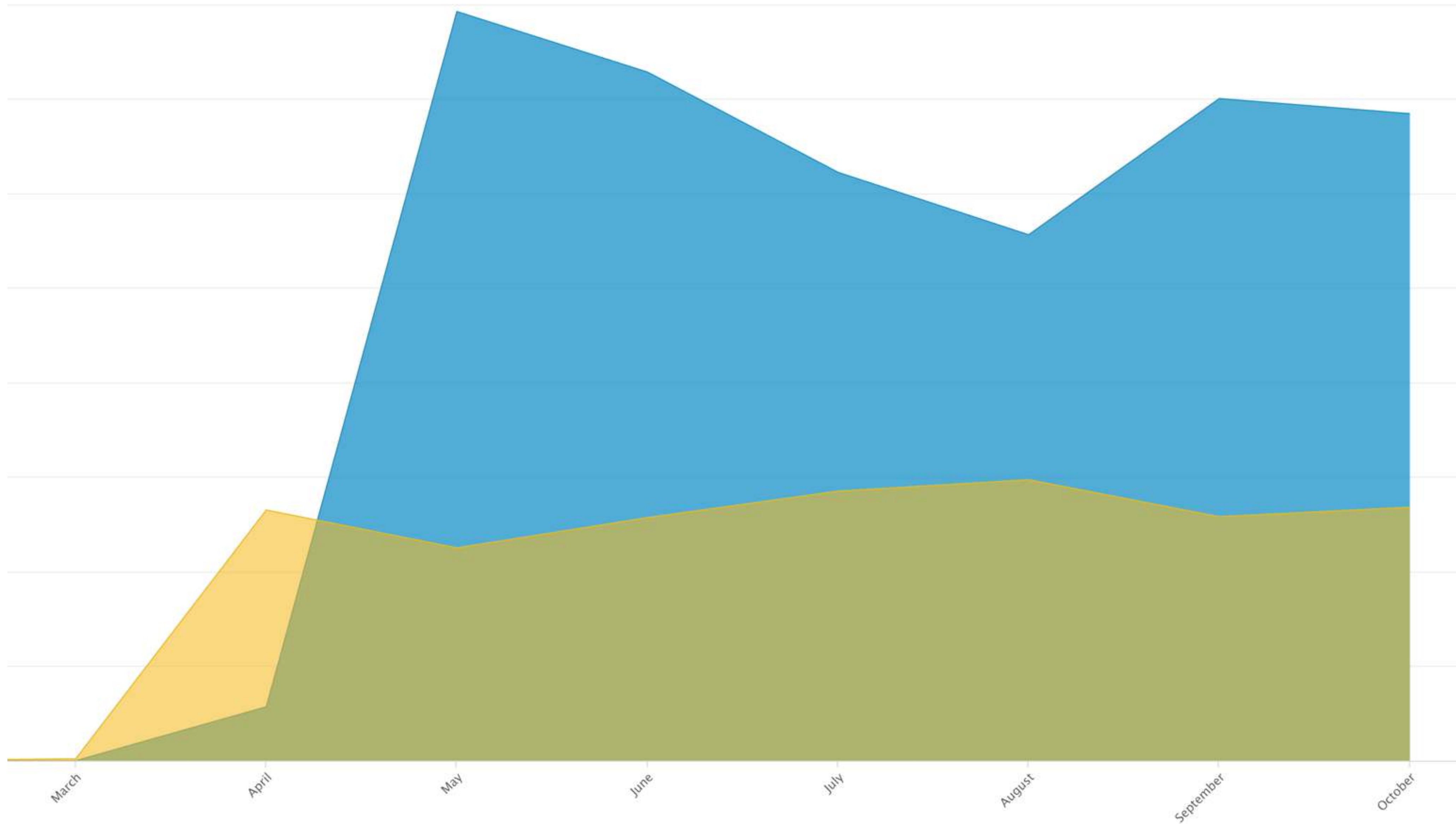
Automated Threat Hunting



Initial Malicious Traffic (training)



New Malicious Traffic



3x more detections

Tracking hundreds of malicious
campaigns

So

Designed representation
invariant to rapidly evolving
malware

Large scale learning
from weak labels

Active learning for automated malware tracking

Millions of users

Tens of thousands of infections

What got us here
won't take us there.



Thanks!

Veronica Valeros
vvaleros@cisco.com

Karel Bartoš
kbartos@cisco.com

Lukáš Machlica
lumachli@cisco.com

The end.