Is traditional AV dead?

Real-time machine-learning detection of modern malware downloads

Cyberdéfense et détection du hacking

1er décembre 2016, Ecole Polytechnique à Palaiseau

Who am I?

- Dr. Marco Balduzzi (@embyte)
- M.Sc. In Computer Engineering, Ph.D. in System Security
- On top of things since 2002
- Sr. Research Scientist
  - Web, Malware, Privacy, Cybercrime, IoT, Threats
  - *http://www.madlab.it*

Traditional AV is Dead?

- Signature-based VS Statistical-based
- Signature-based malware detection is inefficient
  - Polymorphism, code obfuscation, packing
  - Analysis is time consuming (static , dynamic)
  - URL blacklists lag behind (DGA botnets)

Traditional AV is Dead?

- Local awareness VS Global awareness
- Local: Looks at one potential malicious file/URL at the time
- Global: Leverages a global situation awareness, e.g. relationships among files and machines

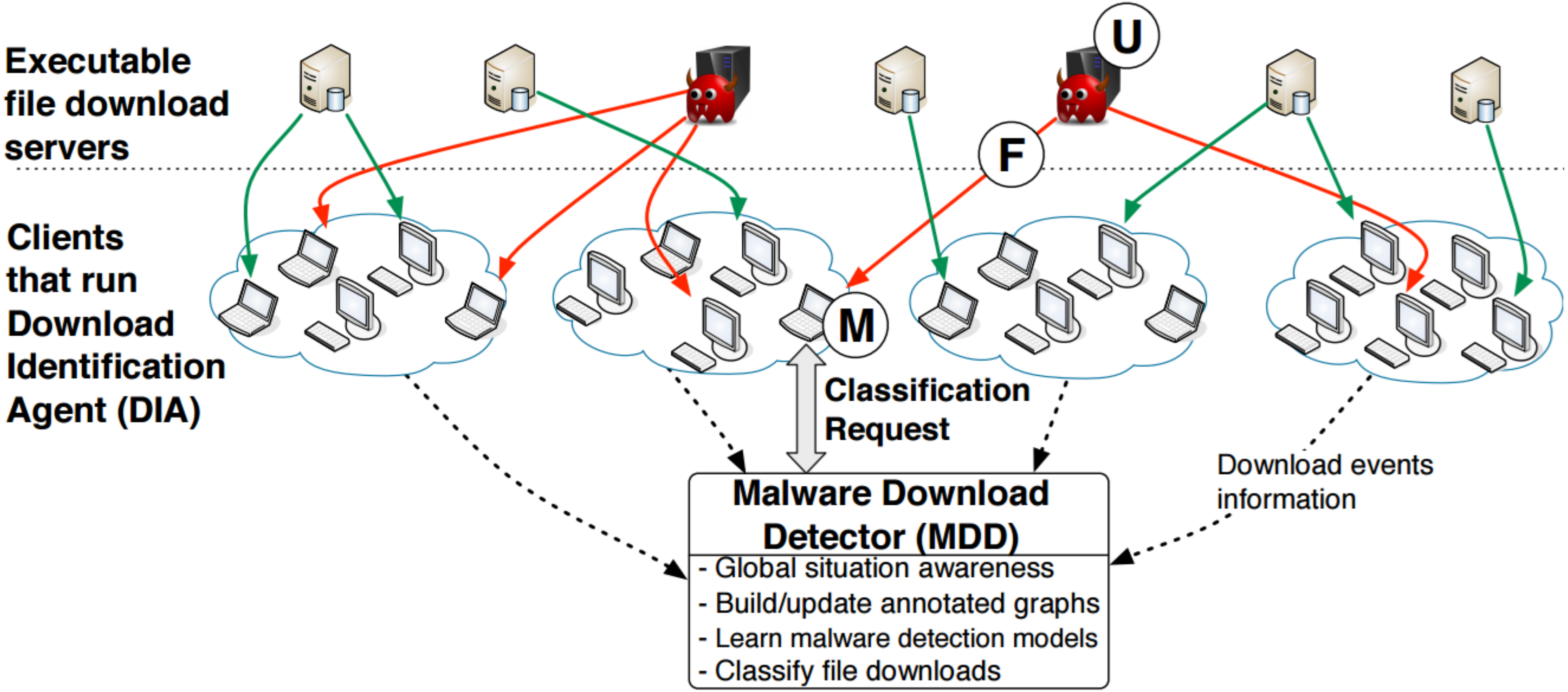
Our X-Gen Approach

- Content agnostic: Files' or webpages' content analysis is **not** needed
- Use of relationship patterns
  - 3W: "Who-What-Where" = who downloads what from where
  - Combination of system- and network-level informations
- Statistical-based detection
- Global situation awareness

Benefits

- Concurrent detection of malicious download events, i.e. files and URLs
- Complementary approach to existing solutions, e.g. static and dynamic detection
- Efficiency, real-time detection against *unknown* and modern threats

System Overview

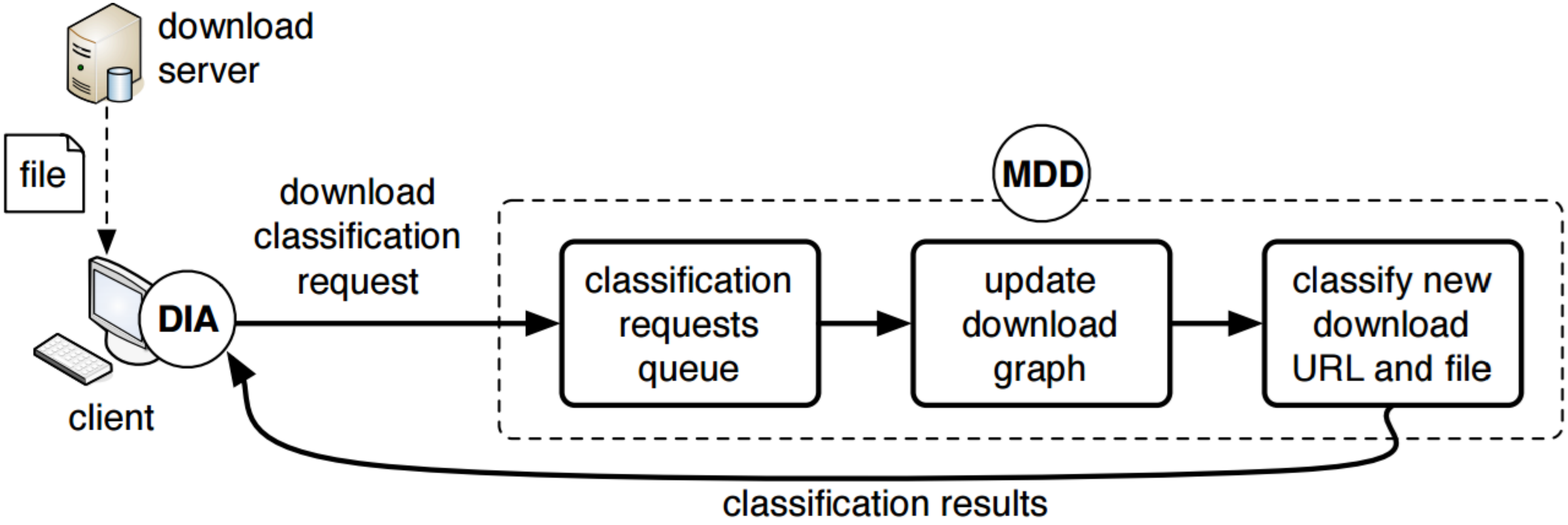


Executable file download servers
U
F
Clients that run Download Identification Agent (DIA)
M
Classification Request
Download events information

Malware Download Detector (MDD)

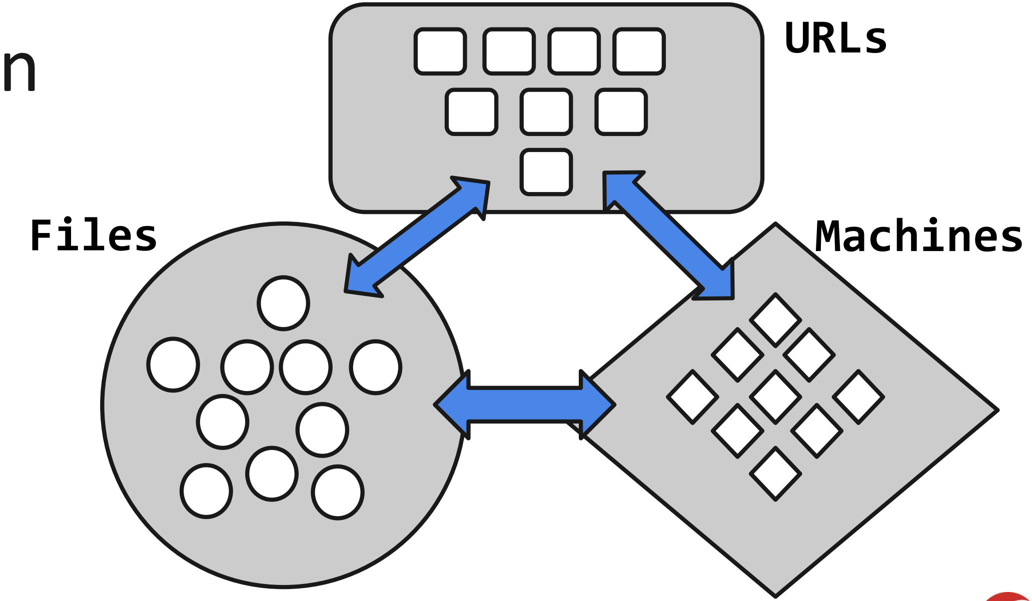
- Global situation awareness
- Build/update annotated graphs
- Learn malware detection models
- Classify file downloads

System Overview

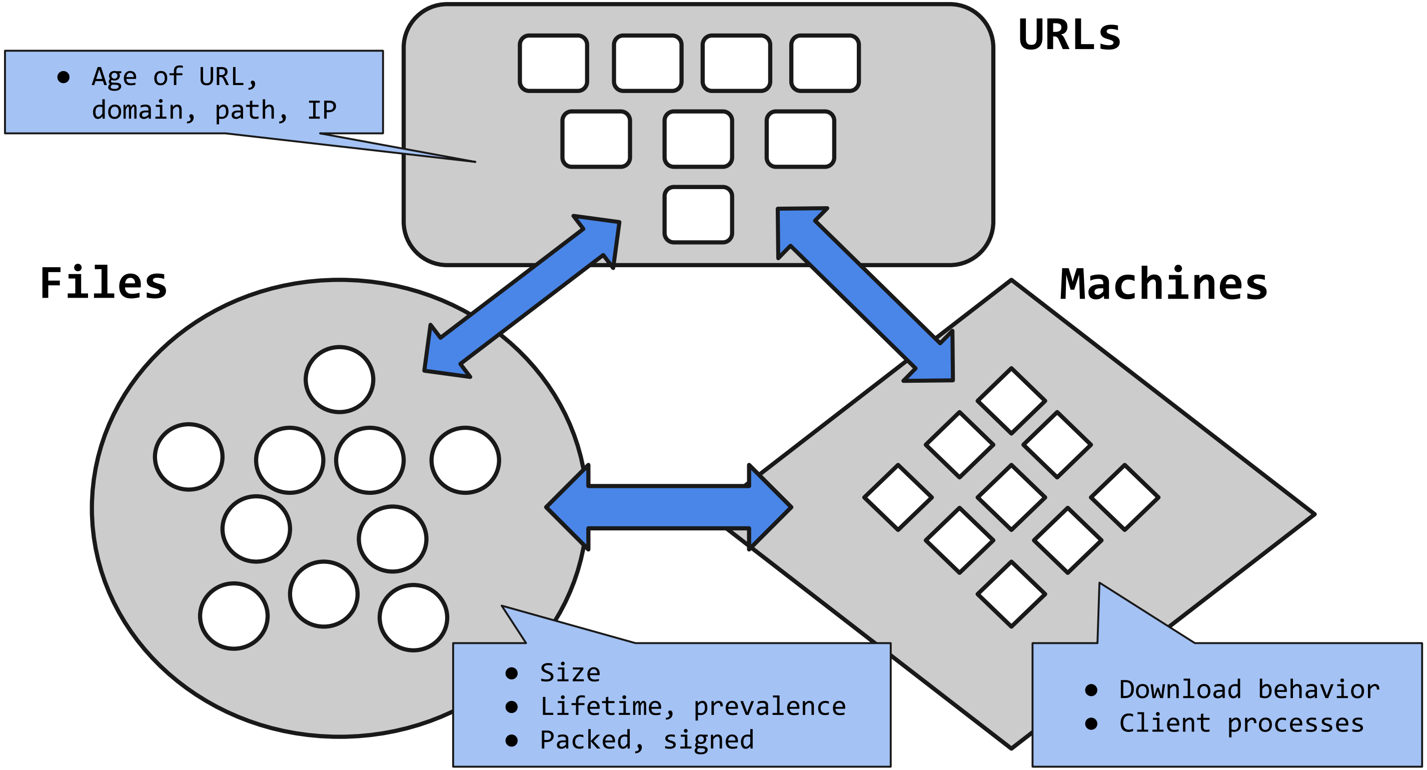

download server
file
download classification request
MDD
client
DIA
classification requests queue
update download graph
classify new download URL and file
classification results

Download Graph

- A representation of a collection of download events
- Global situation



Intrinsic Features

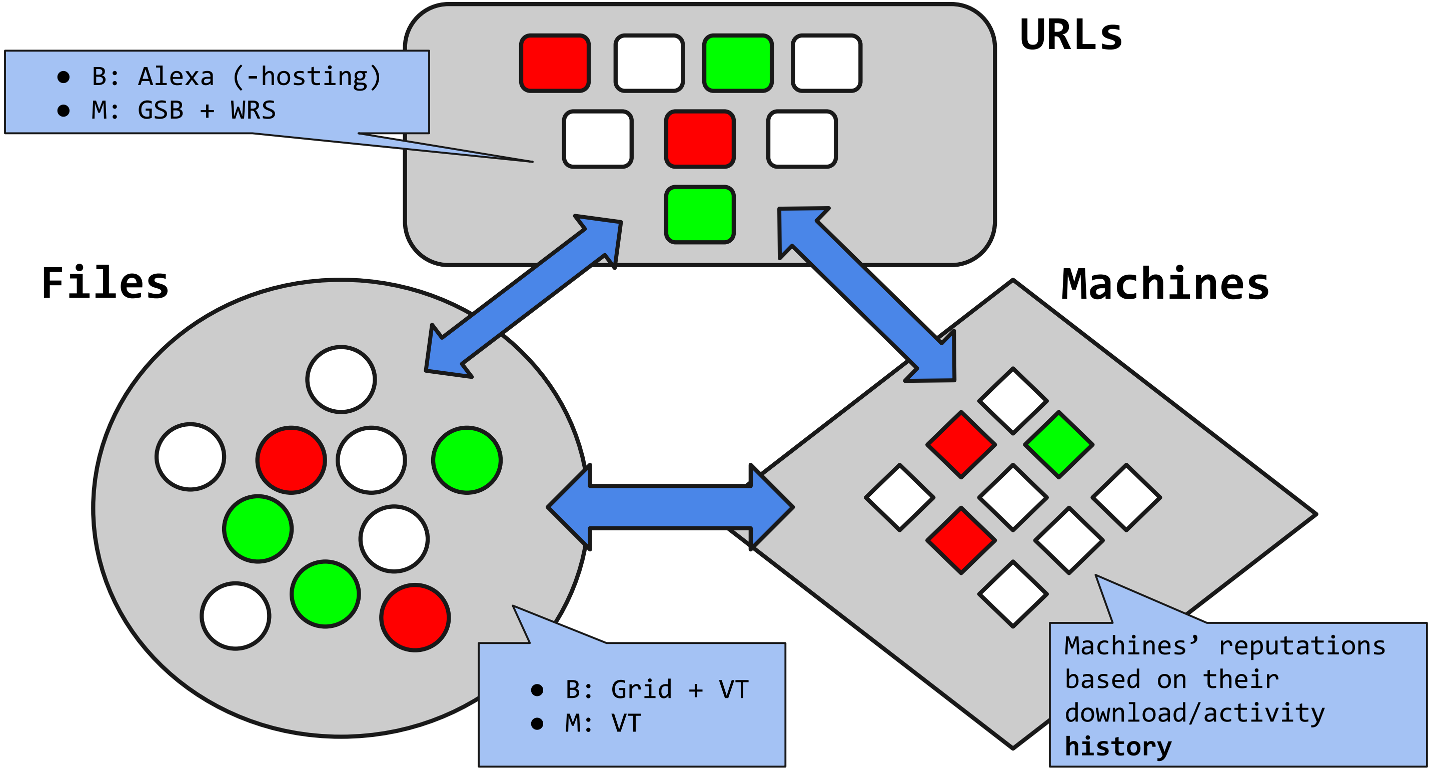


- Age of URL, domain, path, IP

- Size
- Lifetime, prevalence
- Packed, signed

- Download behavior
- Client processes

Labels

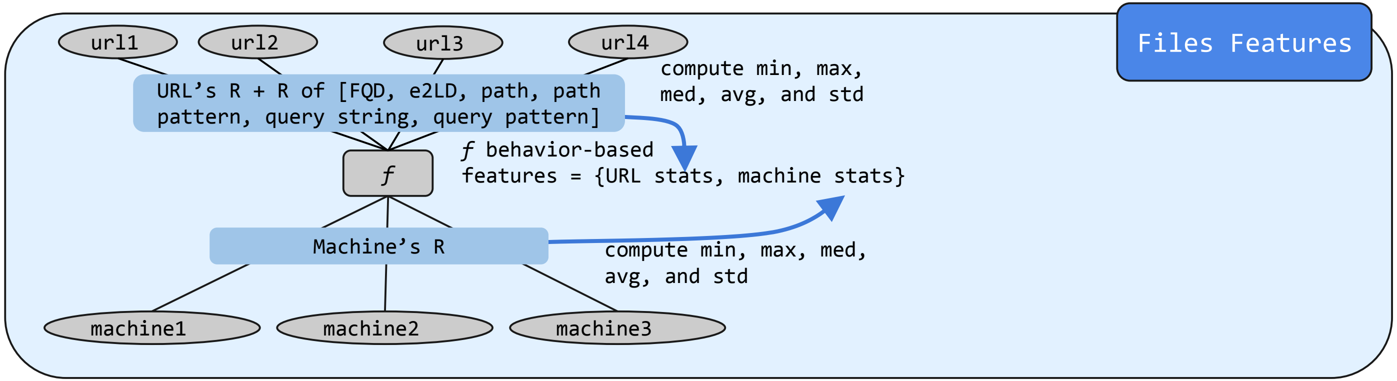


- B: Alexa (-hosting)
- M: GSB + WRS

- B: Grid + VT
- M: VT

Machines' reputations based on their download/activity **history**

Features Engineering



Files Features

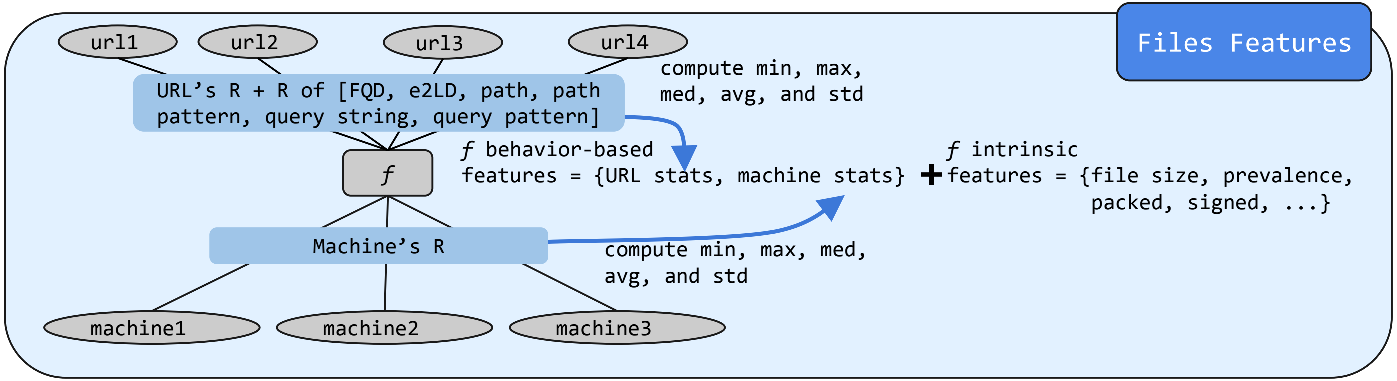
url1
url2
url3
url4
URL’s R + R of [FQD, e2LD, path, path pattern, query string, query pattern]
ƒ
Machine’s R
machine1
machine2
machine3

compute min, max, med, avg, and std

ƒ behavior-based features = {URL stats, machine stats}

compute min, max, med, avg, and std

Features Engineering



Files Features

url1

url2

url3

url4

URL's R + R of [FQD, e2LD, path, path pattern, query string, query pattern]

compute min, max, med, avg, and std

ƒ

ƒ behavior-based features = {URL stats, machine stats} + *ƒ* intrinsic features = {file size, prevalence, packed, signed, ...}

Machine's R

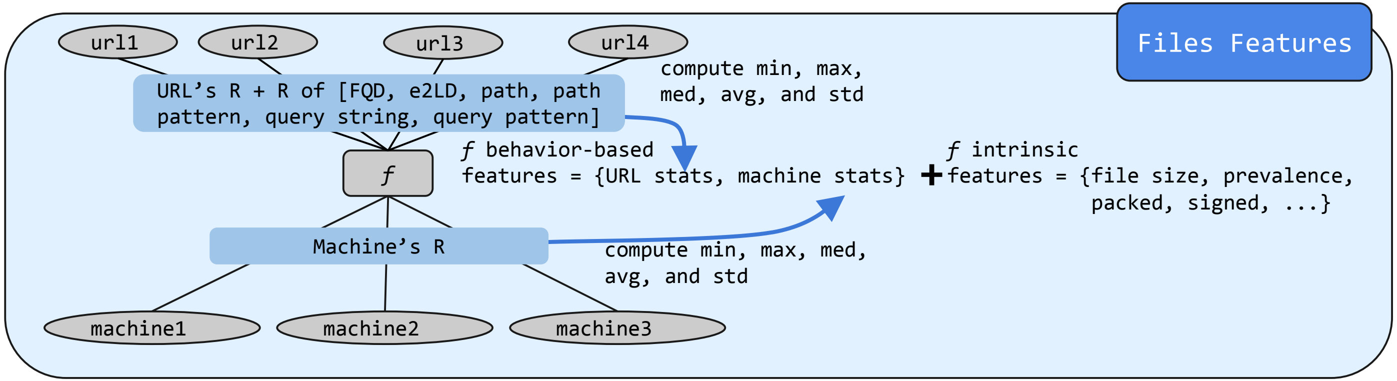
compute min, max, med, avg, and std

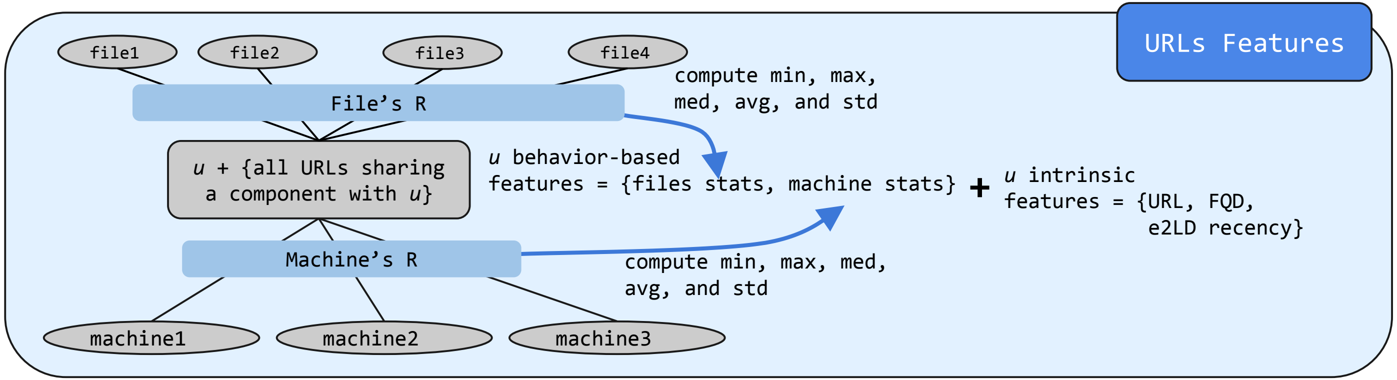
machine1

machine2

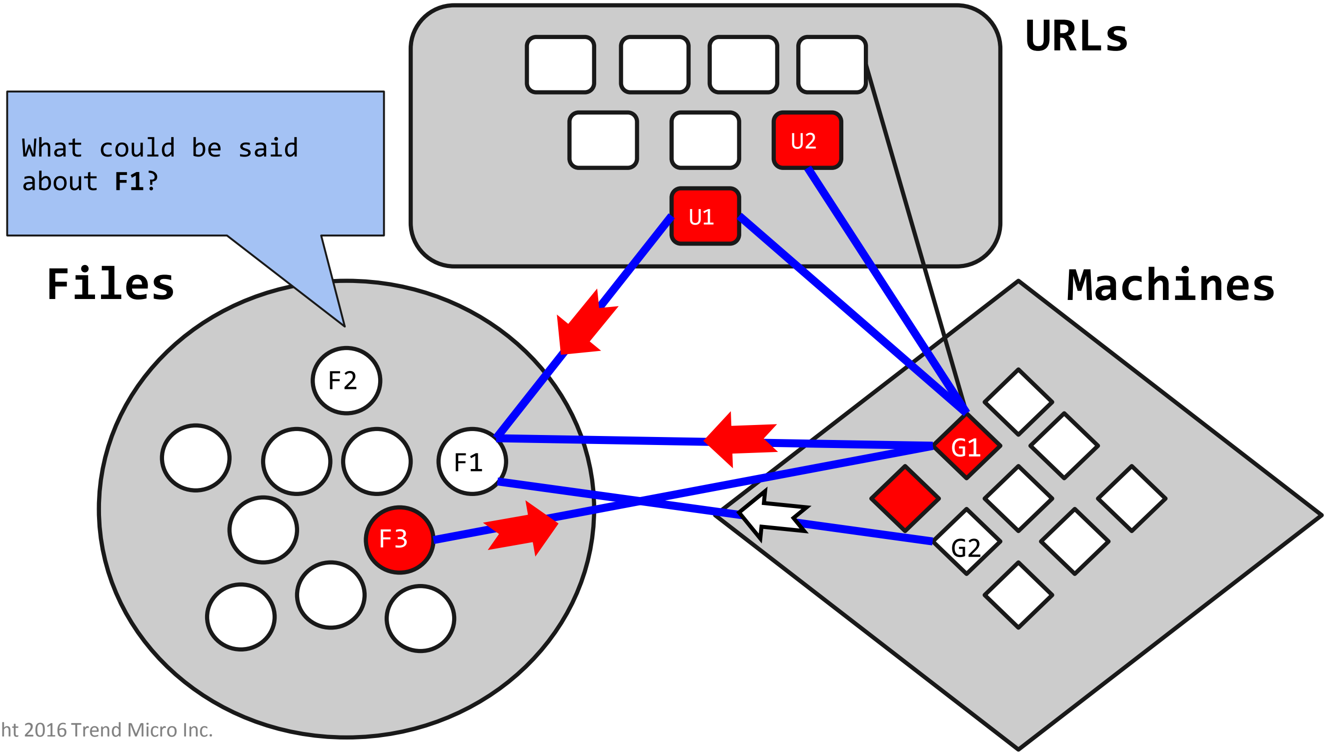
machine3

Features Engineering


Files Features
url1
url2
url3
url4
URL’s R + R of [FQD, e2LD, path, path pattern, query string, query pattern]
compute min, max, med, avg, and std
f
f behavior-based features = {URL stats, machine stats}
+
f intrinsic features = {file size, prevalence, packed, signed, ...}
Machine’s R
compute min, max, med, avg, and std
machine1
machine2
machine3

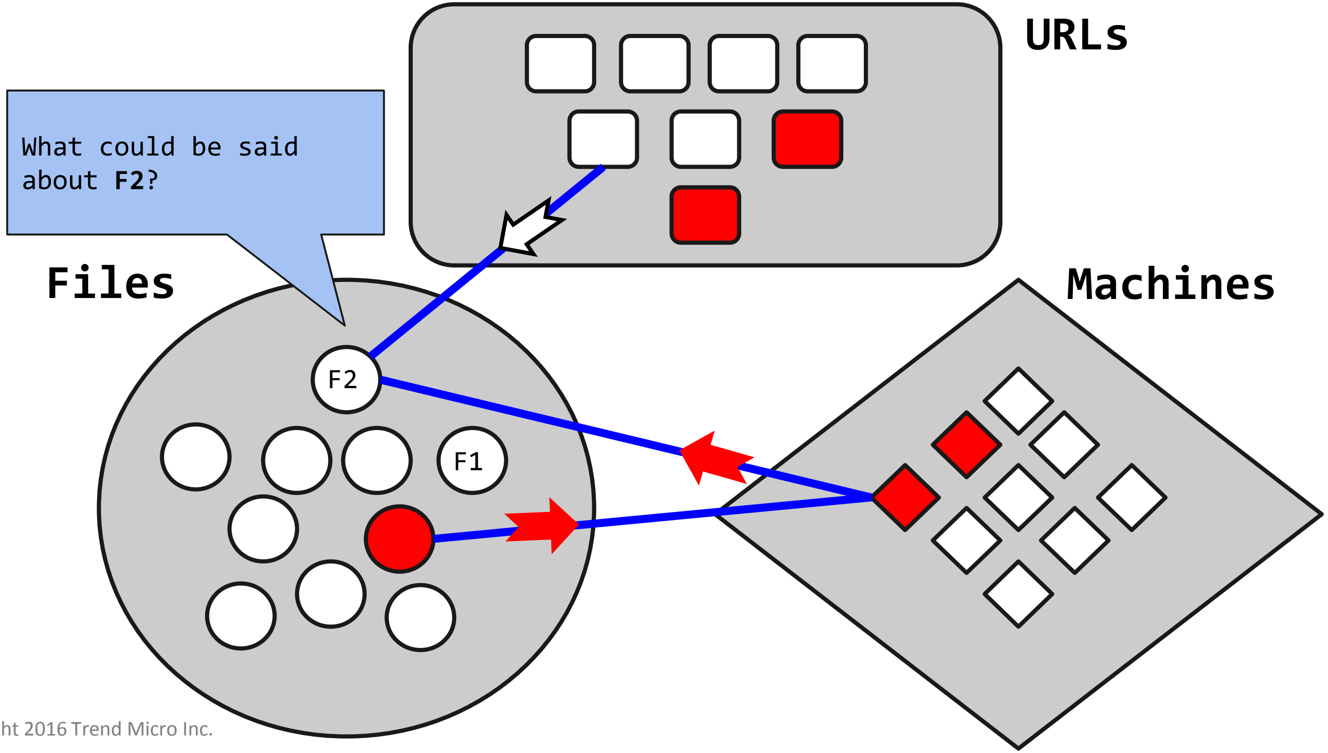

URLs Features
file1
file2
file3
file4
File’s R
compute min, max, med, avg, and std
u + {all URLs sharing a component with u}
u behavior-based features = {files stats, machine stats}
+
u intrinsic features = {URL, FQD, e2LD recency}
Machine’s R
compute min, max, med, avg, and std
machine1
machine2
machine3

Statistical Classifier, example



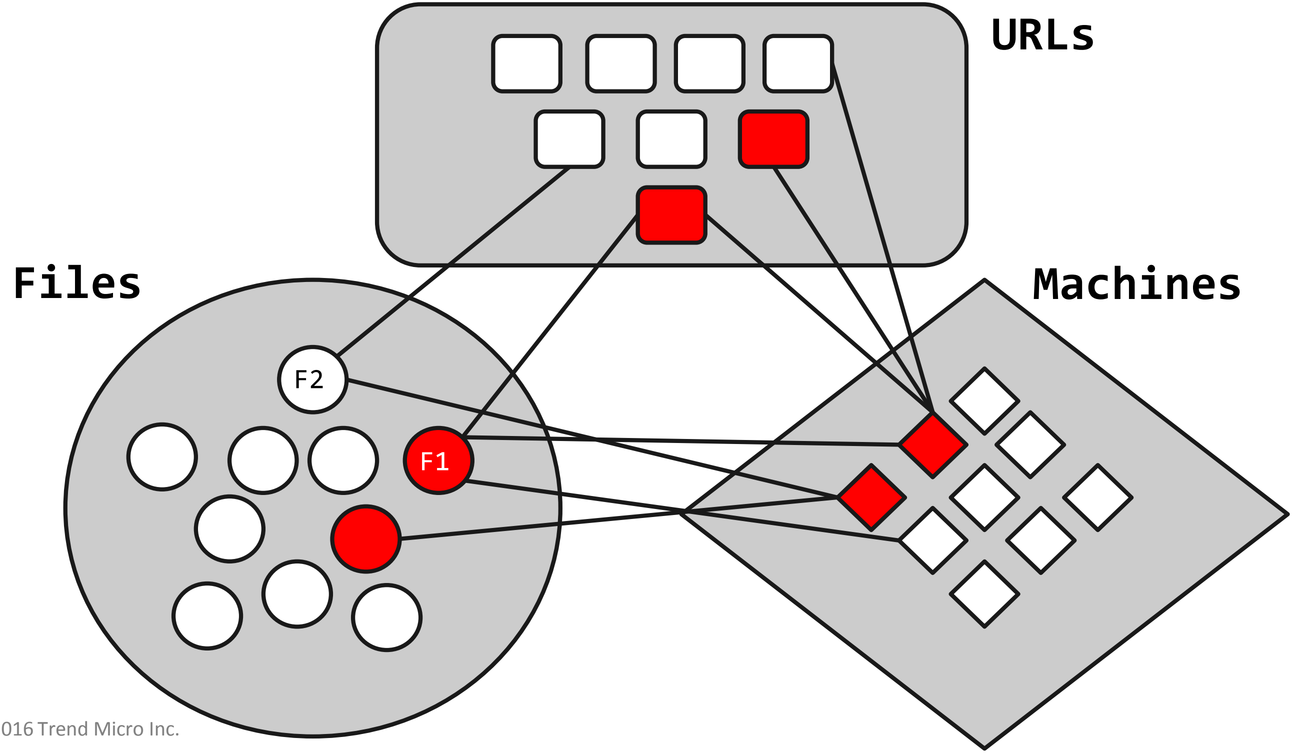
What could be said about **F1**?

Statistical Classifier, example

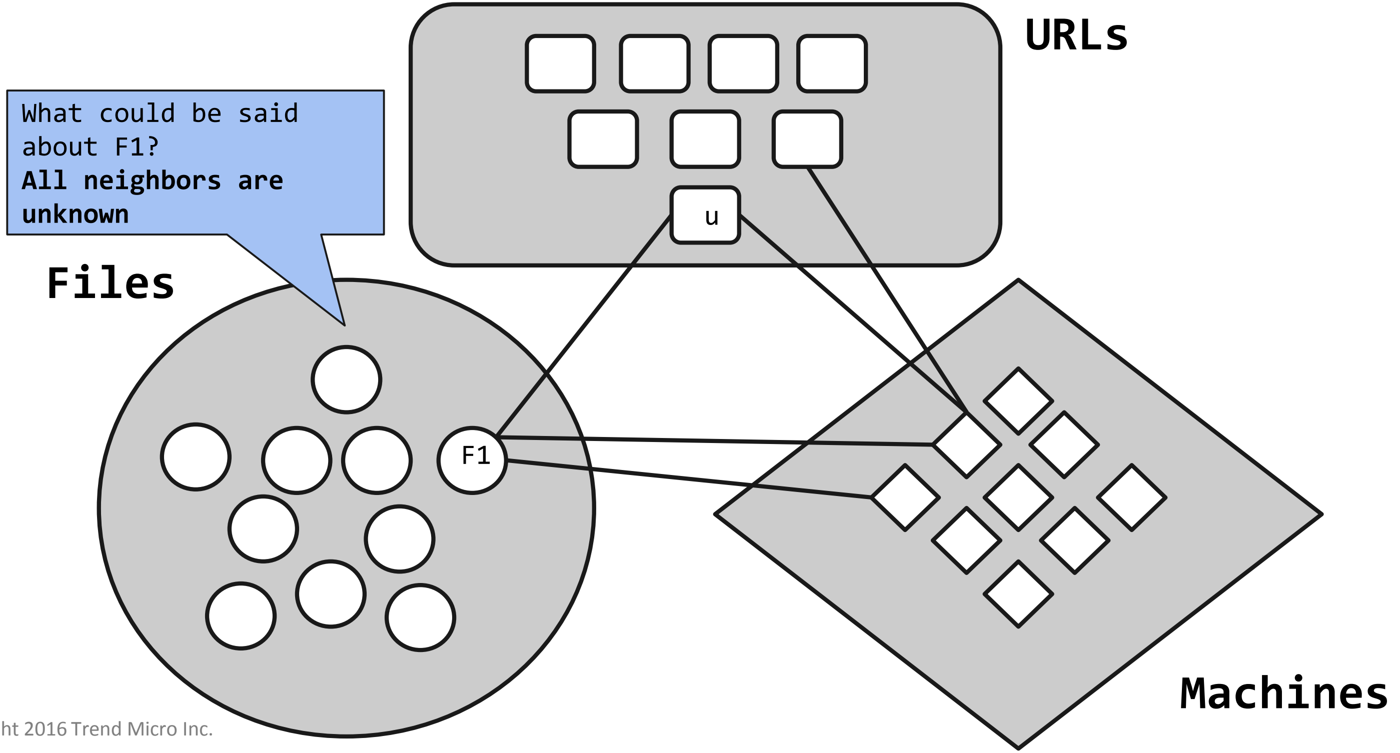


What could be said about **F2**?

Statistical Classifier, example

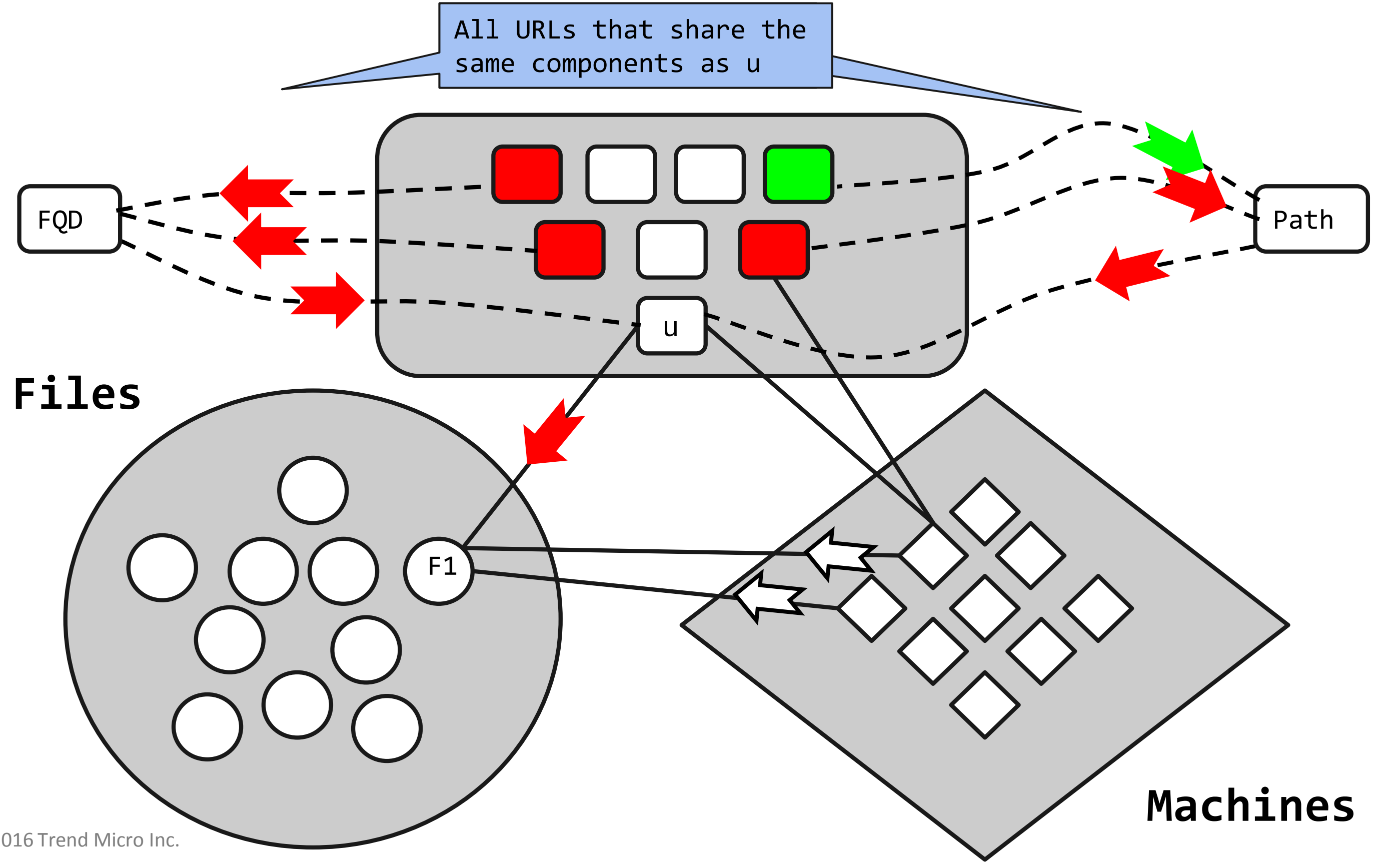


Statistical Classifier, example

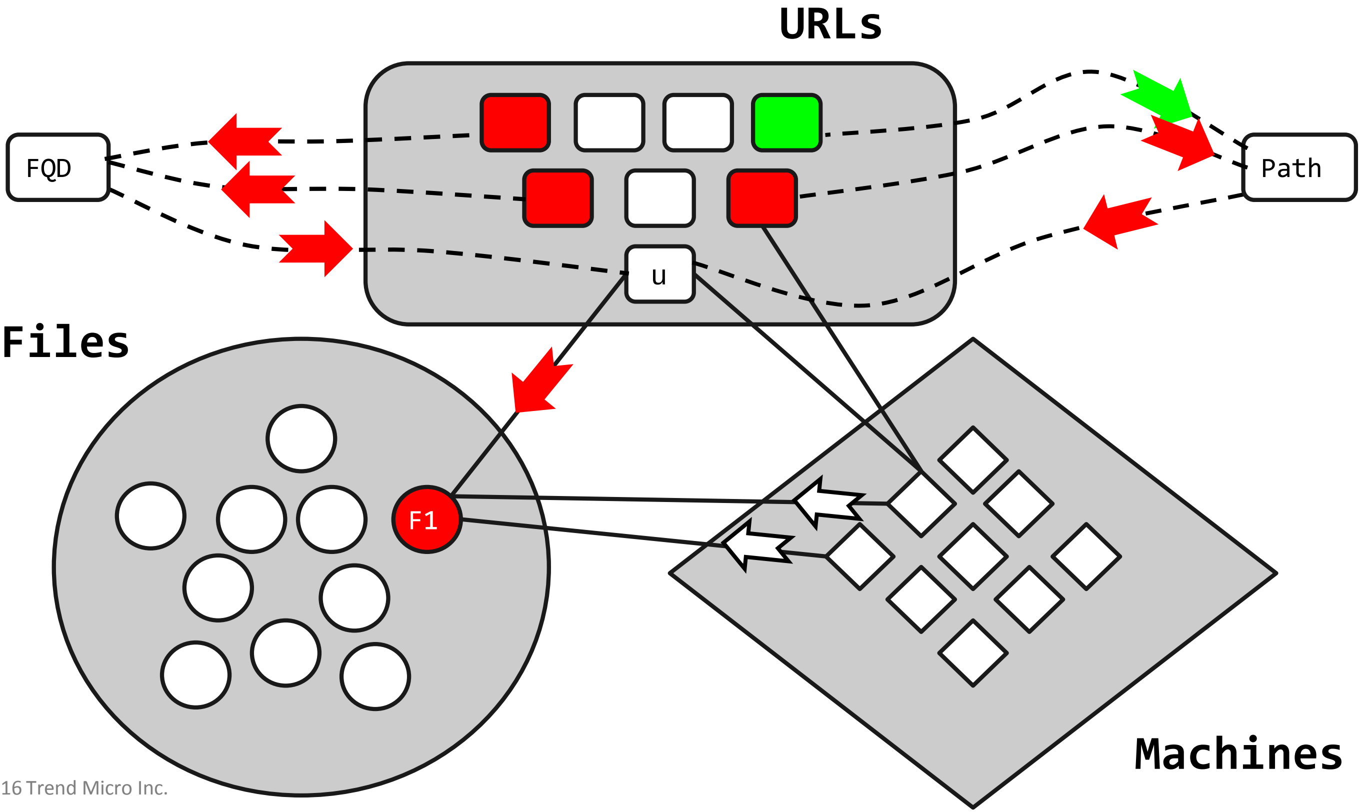


What could be said about F1?
All neighbors are unknown

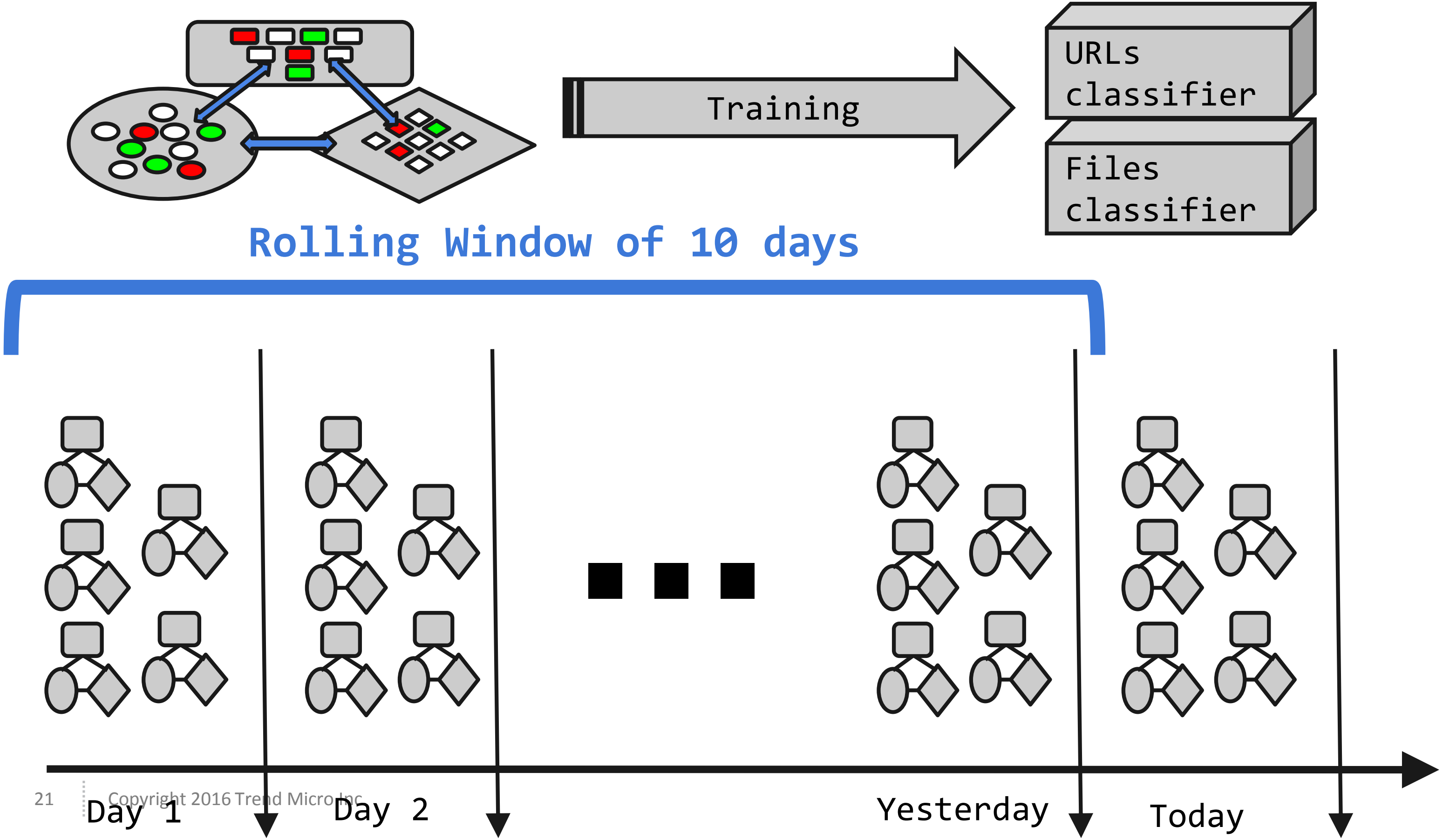
Statistical Classifier, example



Statistical Classifier, example



Deployment



Training

URLs classifier

Files classifier

Rolling Window of 10 days

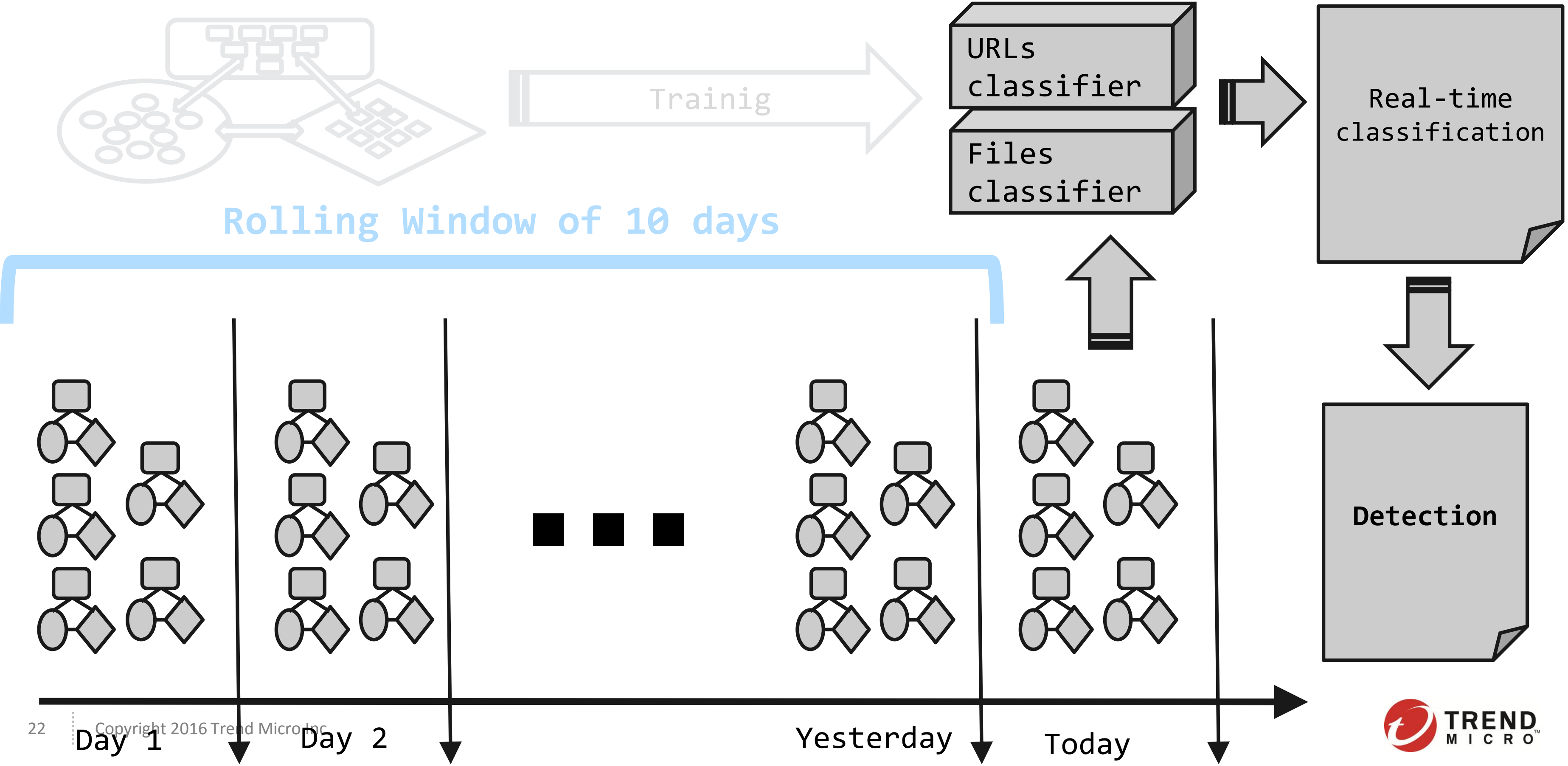
Day 1

Day 2

Yesterday

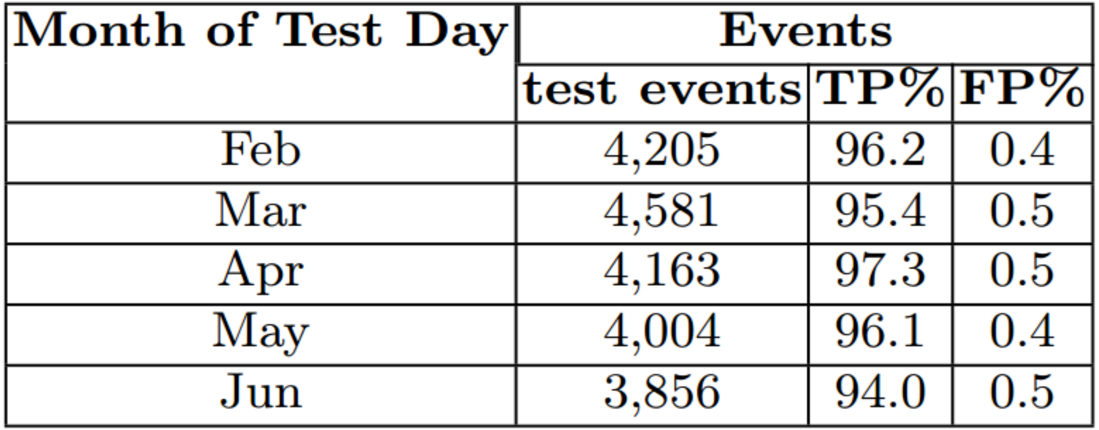
Today

Deployment


Trainig
URLs classifier
Files classifier
Real-time classification
Rolling Window of 10 days
Detection
Day 1
Day 2
Yesterday
Today

Testing Results

- Detection



Month of Test Day	Events		
	test events	TP%	FP%
Feb	4,205	96.2	0.4
Mar	4,581	95.4	0.5
Apr	4,163	97.3	0.5
May	4,004	96.1	0.4
Jun	3,856	94.0	0.5

- Efficiency: requests are served in ~0.16 sec

Early Detection Experiment

- We did classification at t=0.
- We queried Virus Total 6 months after.

- We identified 84% future malware in advance.

Early Detection Experiment

- Droppers and downloaders, e.g. `Win32/InstallCore.MI, TrojanDropper:Win32/Rovnix, Downloader .ATW and MalSign.InstallC.4DB`
- Adware, bots, banking Trojans, key-loggers, e.g.: `Rogue:Win32/FakePAV, Win32:Crypt-QTG, PWS: Win32/Zbot, FakeAV_r.YE, Backdoor.Trojan, and Trojan .FakeAV`

Case Study 1, Wuachos Dropper

- Filename `file_saw.exe`
- Low prevalence
- Invalid signature
- URLs with **no** reputation, BUT path pattern with R of 0.72 (malicious)
  - `/f/1392240240/1255385580/2, /f/1392240120/4165299987/2 -> /H1/I10/I10/I1`
  - 1,445 URLs serving 182 polymorphic malware

Case Study 2, Somoto Adware

- Packed, short lifetime, low prevalence
- 1 graph-connected machines downloaded 1 labeled (known) sample

- Detected a campaign of 695 samples
  - Filename `FreeZipSetup-[\d].exe`
- 616 were unknown to VirusTotal
  - 61 unknown +6 months (10%)

Case Study 3, TTAWinCDM Spyware

- Machine and URL with **no** reputation ☹

- Low lifetime & prevalence & countries
- Mismatch on downloading process
  - Acrobat process + Unauthoritative domain
- Flash 0-day (+2 month)

Conclusions

- Traditional AV is not dead, but tends to become quickly obsolete and inefficient
- Complementary system
  - Content agnostic, statistical based
  - Global awareness
- 90% TP at 0.1% FP
- Detect unknown threats in real-time! ☺

Thanks!

- Questions?

Dr. Marco Balduzzi, @embyte

surname (at) trendmicro.com