Behavioral Clustering of HTTP-based Malware and Signature Generation using Malicious Network Traces

Roberto Perdisci[1,2], Wenke Lee[1,2], Nick Feamster[1]

[1] Georgia Tech College of Computing

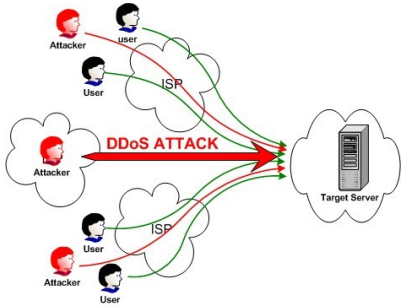
[2] DAMBALLA
Take Back Command-and-Control

USENIX NSDI 2010

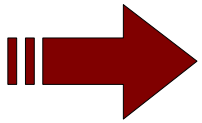
Malware = Malicious Software

- Most modern cyber crimes are carried out using malicious software

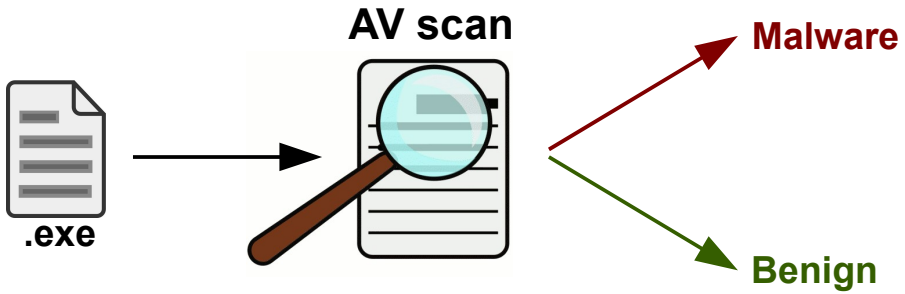
Spam, Identity Theft, DDoS…

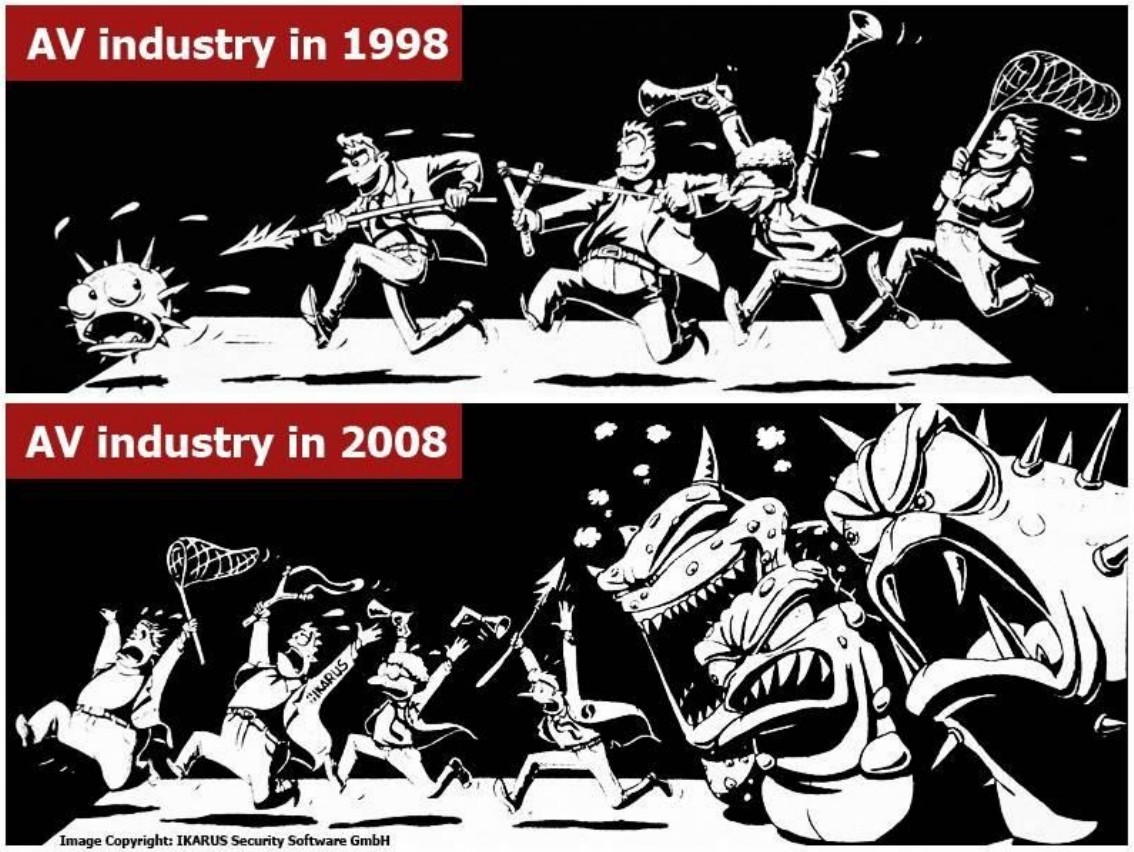


- Many different types of malware
  - ***Trojans***
  - ***Bots***
  - ***Spyware***
  - ***Adware***
  - ***Scareware ...***



Traditional AVs are not enough!





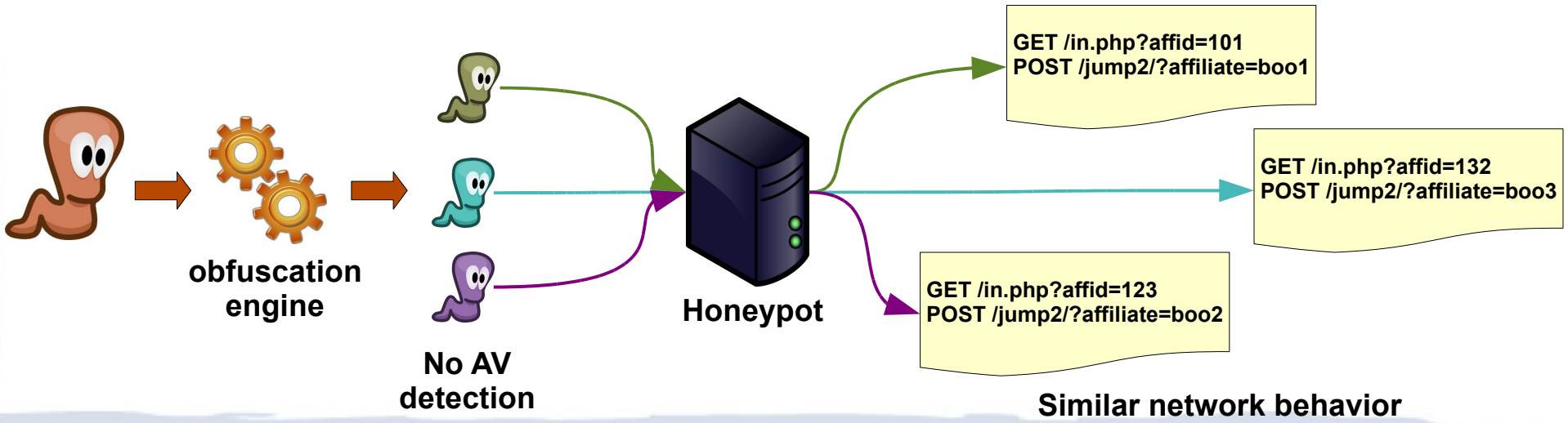
Original Malware

Executable *Packing*
(obfuscation)

***Hidden* Malware**

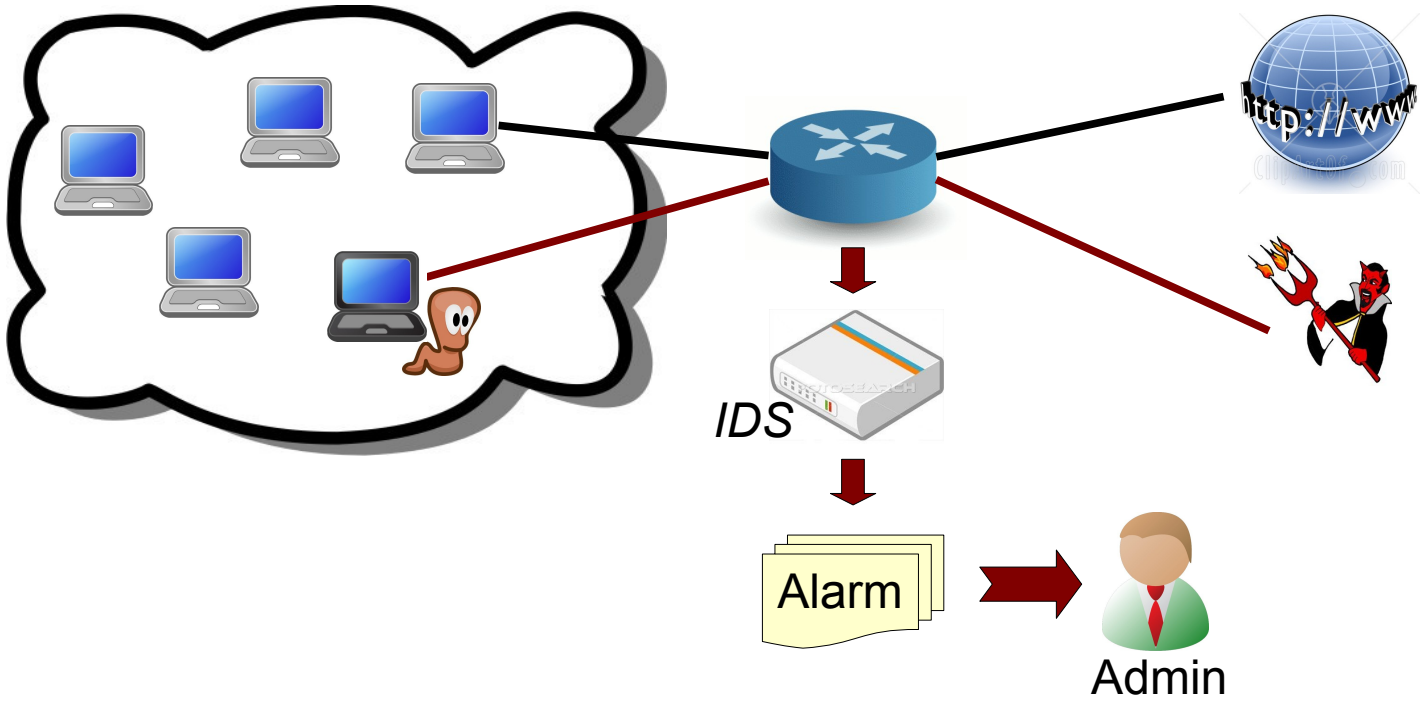
What can we do to detect malware?

- Most malware need a network connection to perpetrate malicious activities
  - *Bots* need to contact C&C server, send spam, etc...
  - *Spyware* need to exfiltrate private info
  - *Trojan droppers* need to download further malicious software ...
- Variants of the same malware can evade AVs
  - When executed they generate **similar malicious behavior**



Our Approach

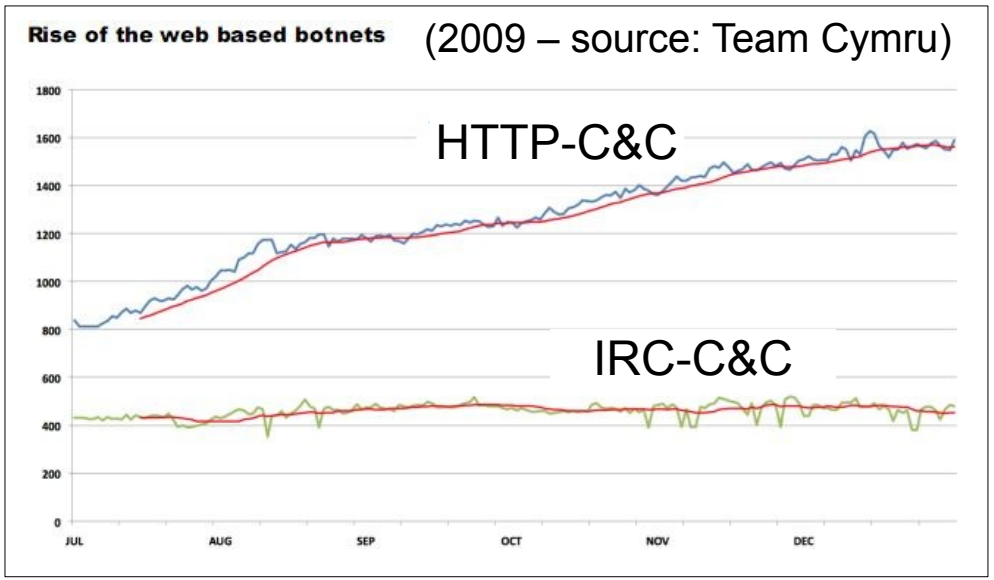
- Detect the Network Behavior of Malware

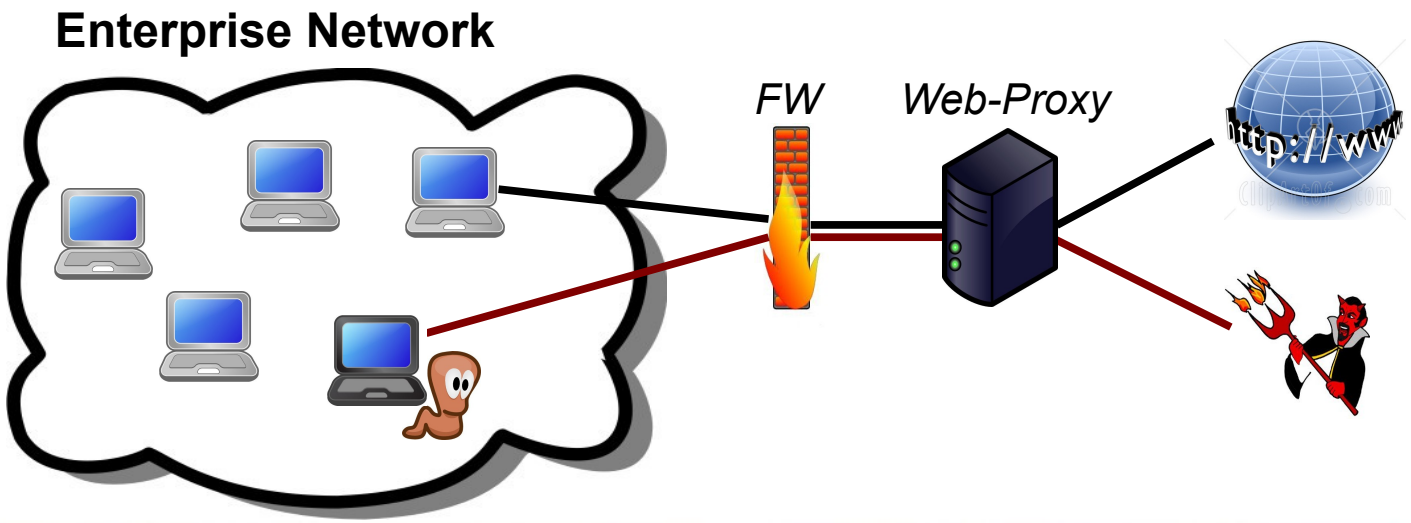


  - Complement existing host-based detection systems
  - Improve “coverage”

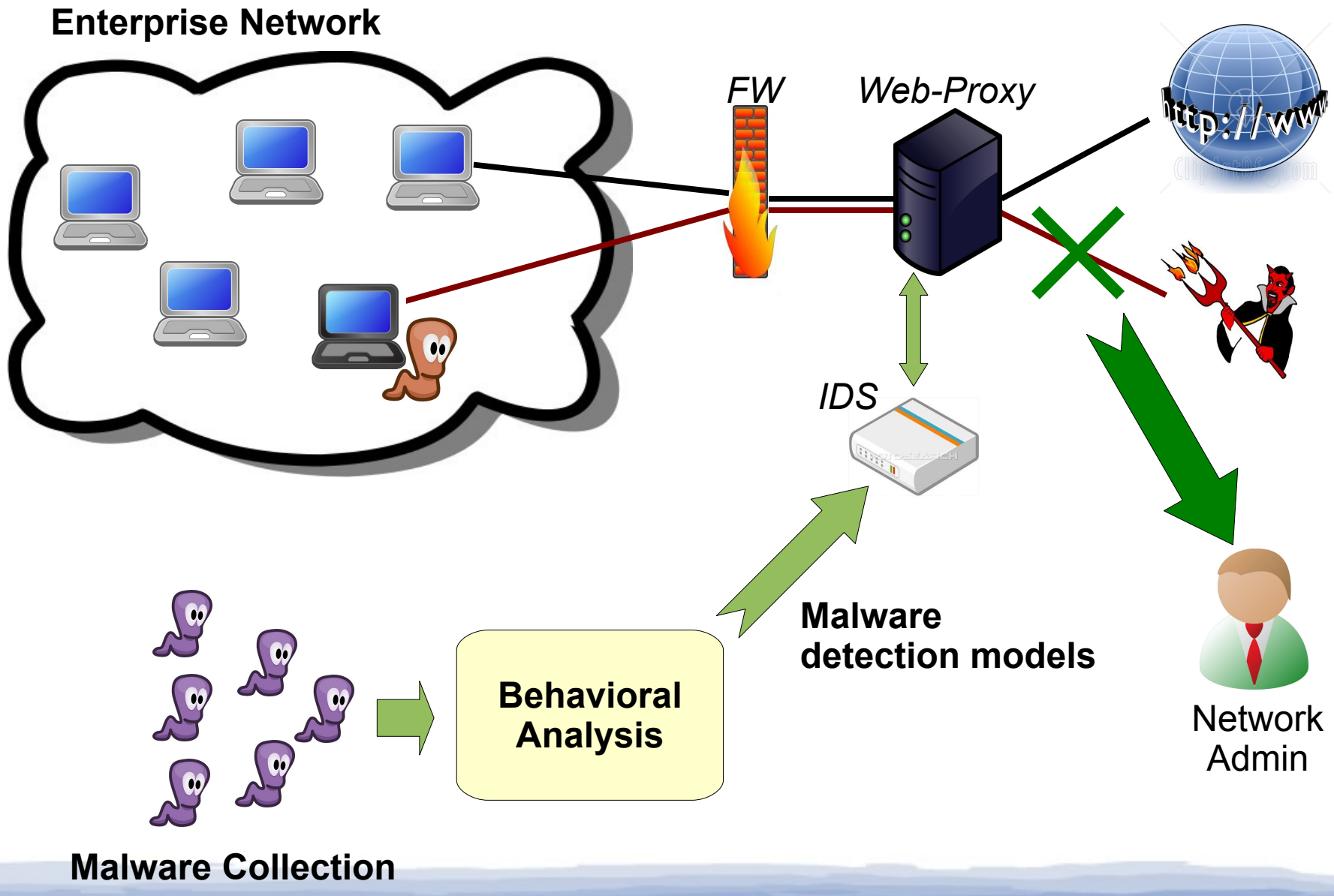
Web-based Malware

- Use HTTP protocol
- Bypass existing network defenses
  - Firewalls
- Web kits for malware control available

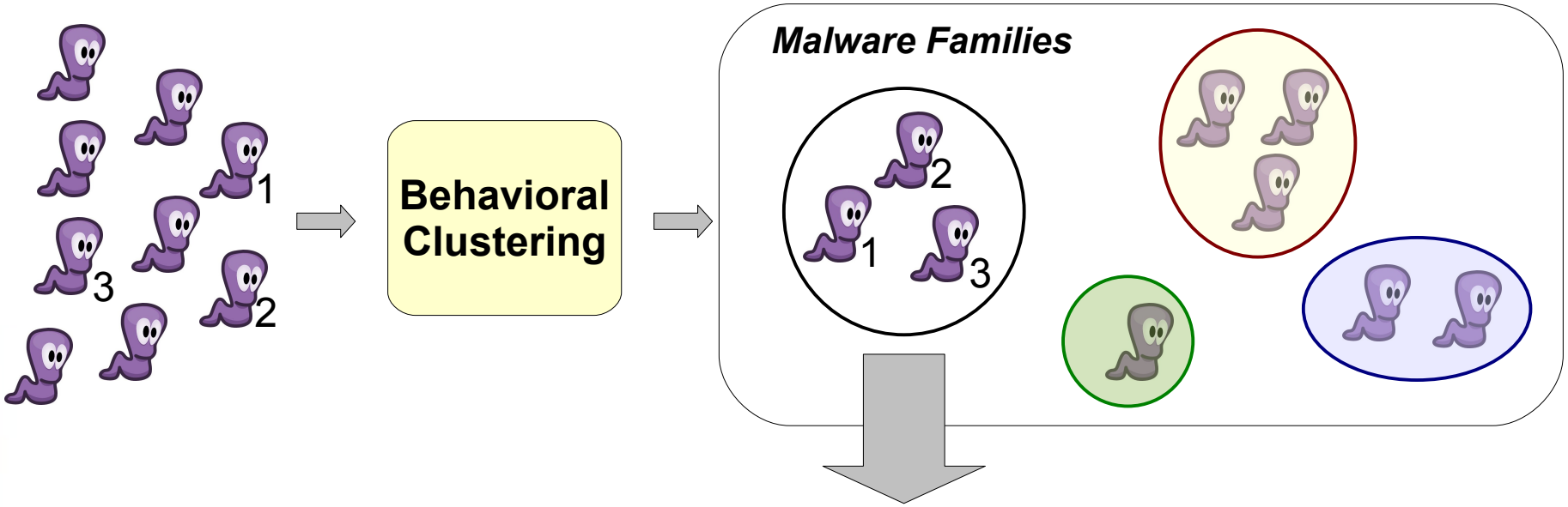




Detecting Web-based Malware



System Overview



Malware Traffic:

1 GET /in.php?affid=94901&url=5&win=Windows%20XP+2.0&sts=|US|1|6|4|1|284|0

2 GET /in.php?affid=43403&url=5&win=Windows%20XP+2.0&sts=

3 GET /in.php?affid=94924&url=5&win=Windows%20XP+2.0&sts=|US|1|6|8|1|184|0

Malware Detection Signature:

GET /in\.php\?affid=.*&url=5&win=Windows%20XP\+2\.0&sts=.*

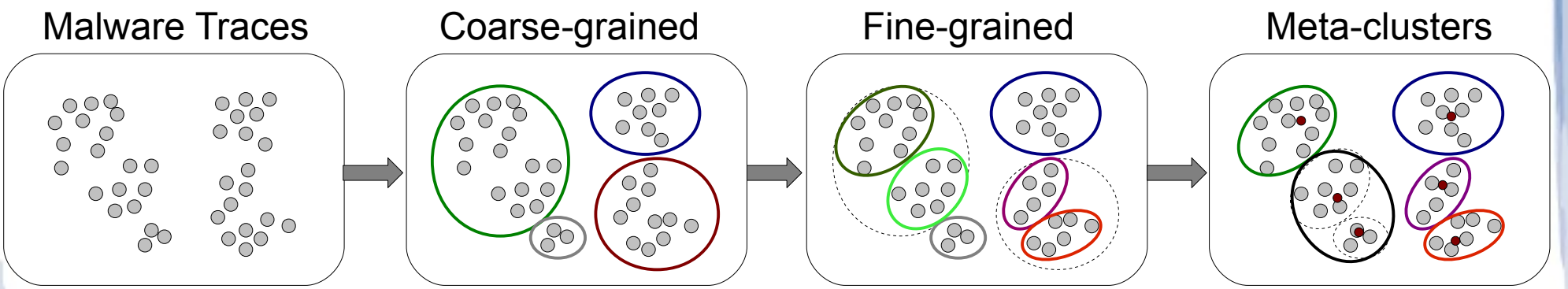
Behavioral Malware Clustering

- Related Work (host-level behavior)
  - Automated analysis of Internet malware [Bailey et al., RAID 2007]
  - Scalable malware clustering [Bayer et al., NDSS 2009]
  - Malware indexing using function-call graphs [Hu et al., CCS 2009]
- Our approach
  - Focus on network-level behavior

    ⇨ we want network signatures

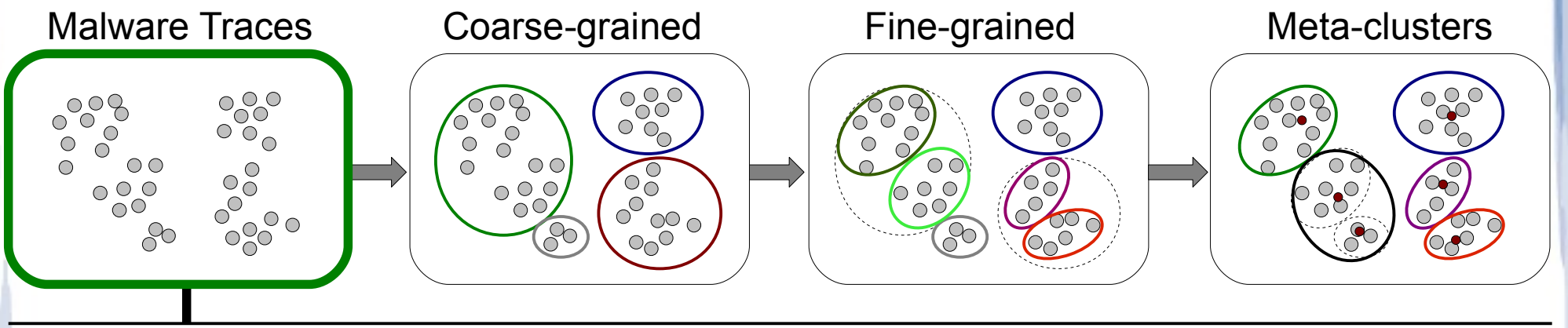
  - **Better malware detection signatures than using host-level behavior**

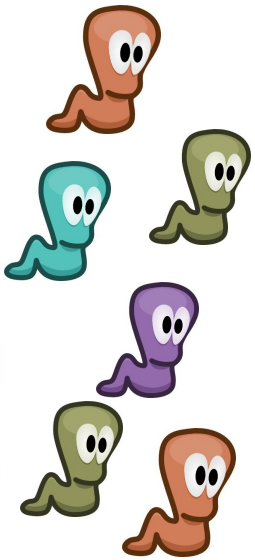
Network Behavioral Clustering

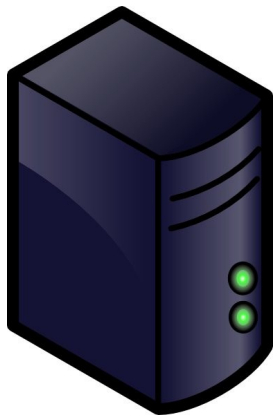


- ***Three-steps*** clustering refinement process
- Good trade-off between ***efficiency*** and ***accuracy***

Network Behavioral Clustering





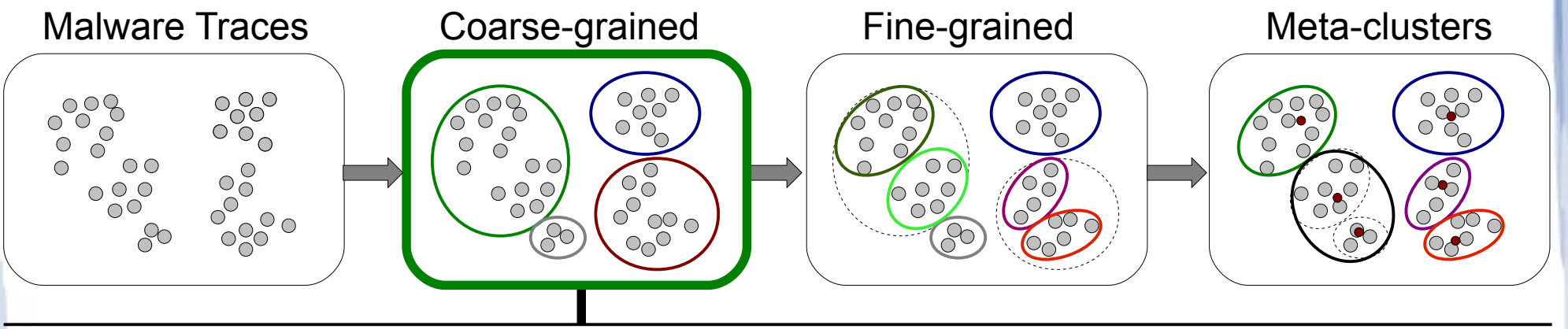


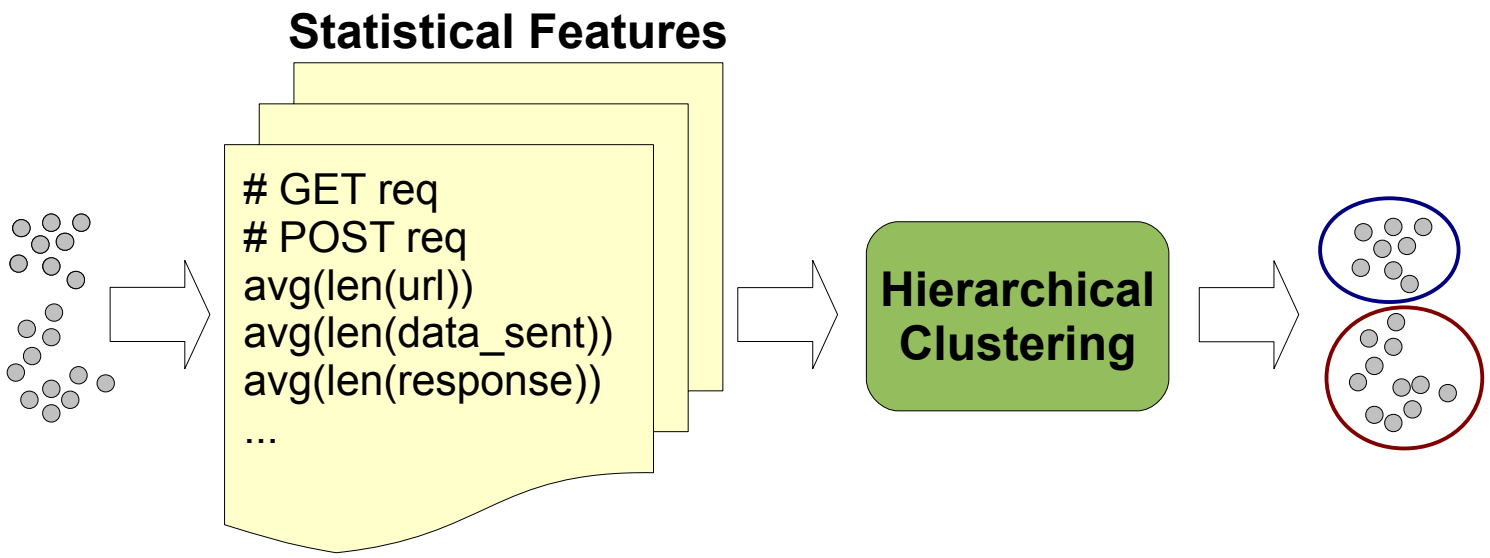
Honeypot

GET /bins/int/9kgen_up.int?fxp=6d HTTP/1.1
User-Agent: Download
Host: X1569.nb.host192-168-1-2.com
Cache-Control: no-cache

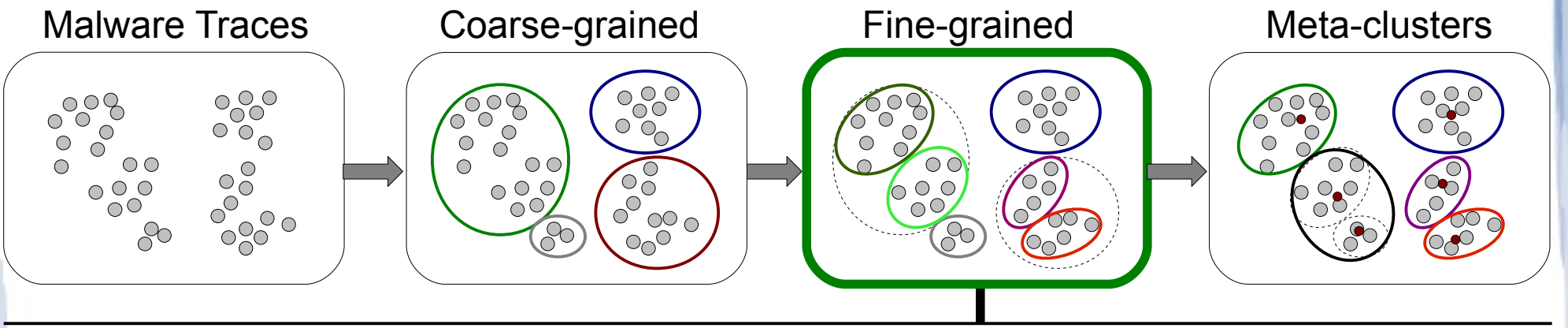
HTTP/1.1 200 OK
Connection: close
Server: Yaws/1.68 Yet Another Web Server
Date: Mon, 15 Mar 2010 11:47:11 GMT
Content-Length: 573444
Content-Type: application/octet-stream

Network-level Clustering

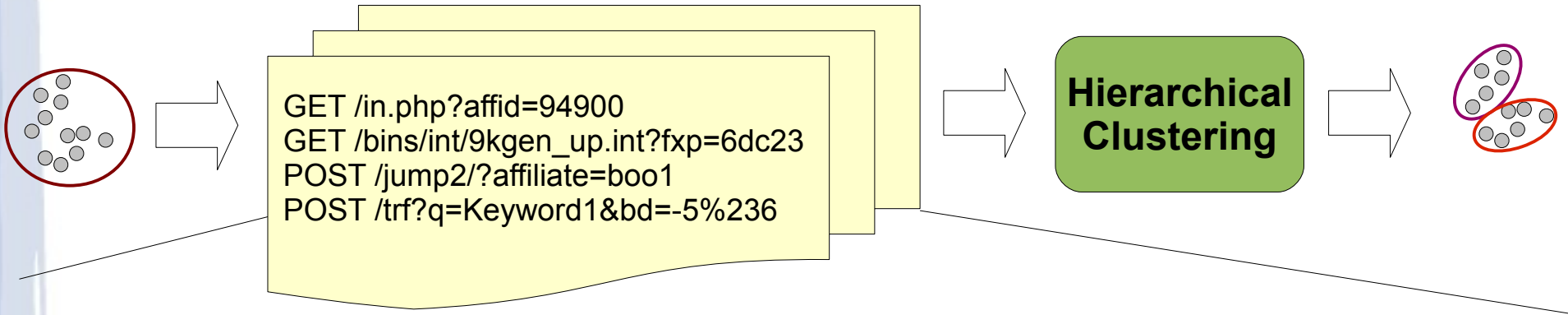




Network-level Clustering



Structural Features



Malware Trace m_1

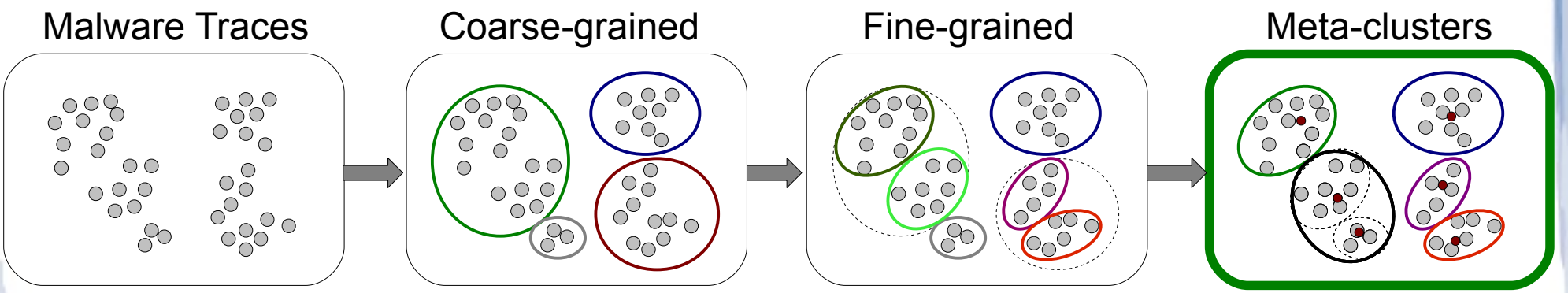
```
GET /in.php?affid=94900
GET /bins/int/9kgen_up.int?fxp=6dc23
POST /jump2/?affiliate=boo1
POST /trf?q=Keyword1&bd=-5%236
```

$d(m_1, m_2)$

Malware Trace m_2

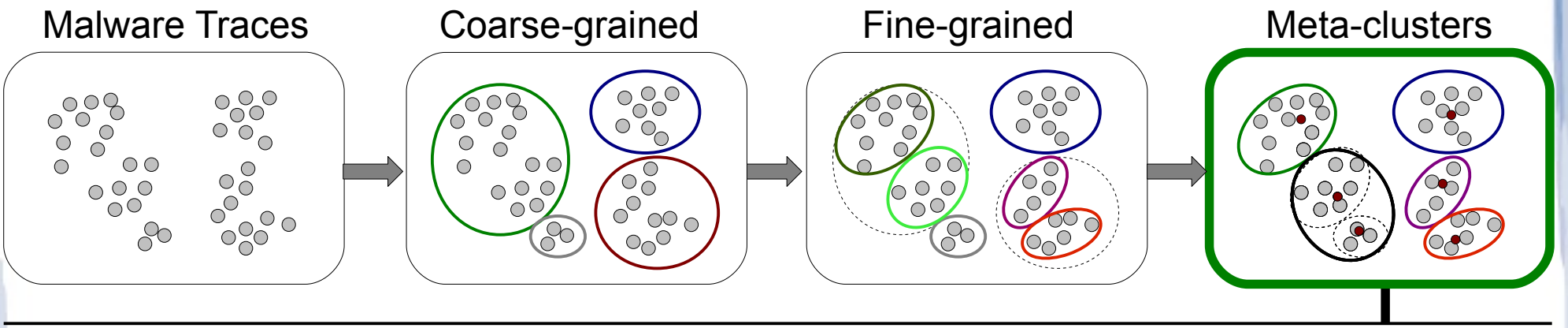
```
GET /index.php?v=1.3&os=WinXP
GET /kgen/config.txt
POST /bots/command.php?a=6.6.6.6
POST /attack.php?ip=10.0.1.2&c=dos
```

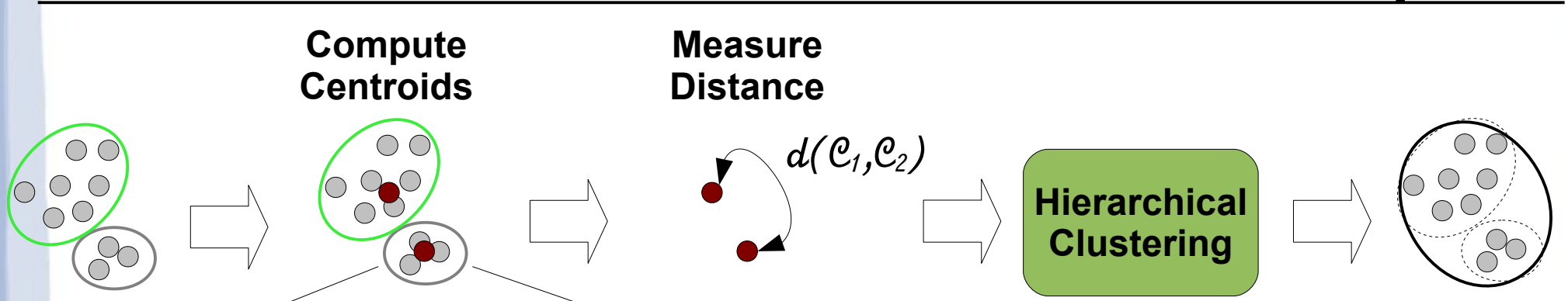
Network-level Clustering

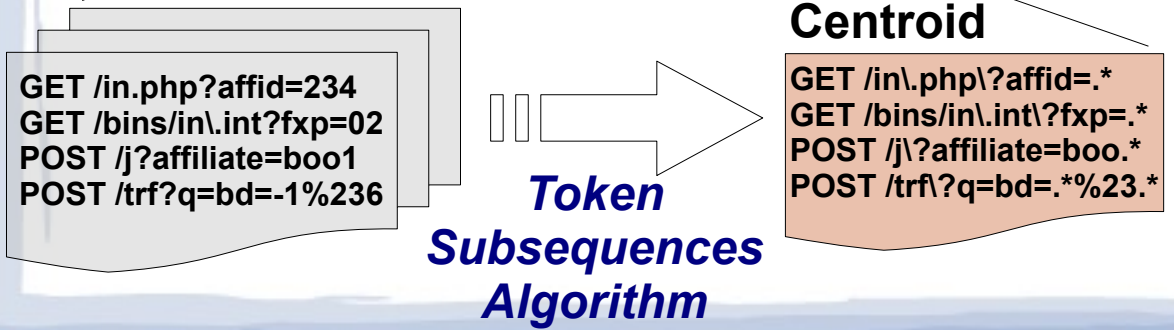


- ***Meta-clustering*** recovers from possible mistakes made in previous steps
- Improves overall **quality** of malware clusters and malware detection models

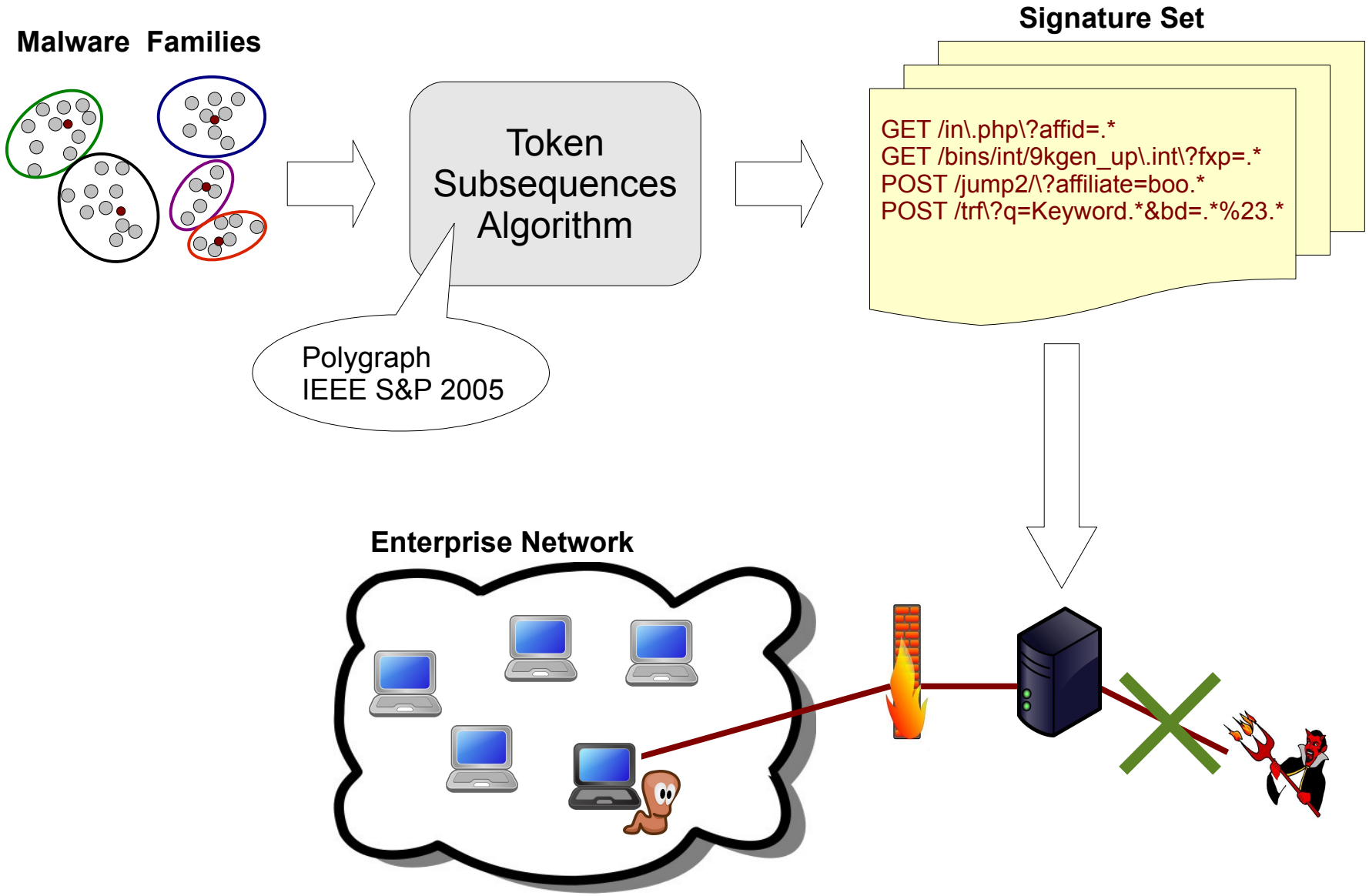
Network-level Clustering







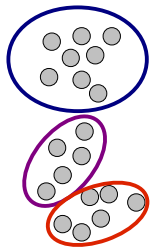
Signature Generation

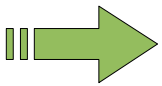


Experimental Results

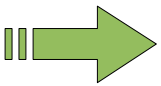
- Malware Dataset
  - 6 months of malware collection (Feb-Jul 2009)
  - **~25k** distinct *real-world* malware samples
- Clustering Results

Dataset	Samples	Malware Families	Modeled Samples	Signatures	Time
Feb-2009	4,758	234	3,494	446	~8h



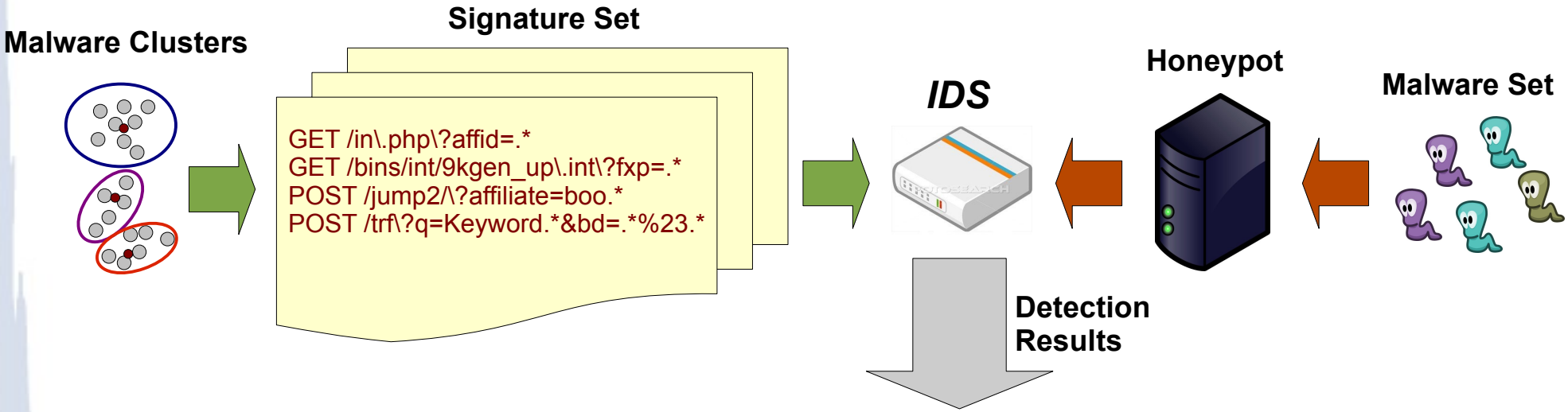


Cluster Validity Analysis



Compact and well Separated Clusters

Experimental Results



Detection Test on All Samples

	Feb09	Mar09	Apr09	May09	Jun09	Jul09
Sig. Feb09	85.9%	50.4%	47.8%	27.0%	21.7%	23.8%

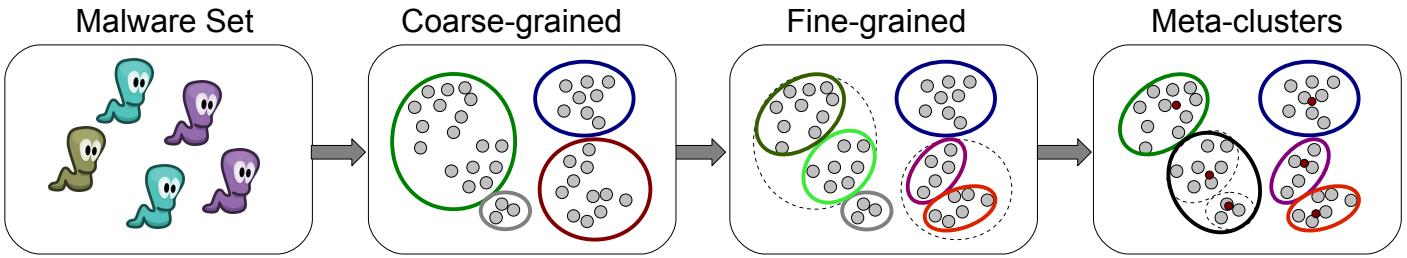
Detection Test on Malware undetected by commercial AVs

	Feb09	Mar09	Apr09	May09	Jun09	Jul09
Sig. Feb09	54.8%	52.8%	29.4%	6.1%	3.6%	4.0%

Sig. Feb09 **No False Alerts** → Tested on 12M legitimate HTTP queries

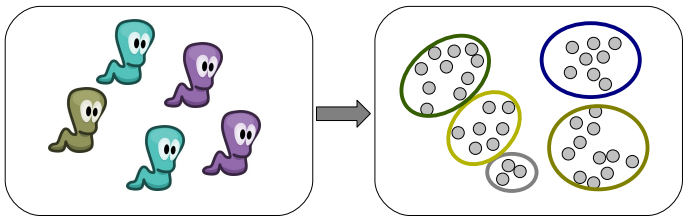
Comparison with other approaches

Signature extracted from reduced malware set of ~2k malware samples



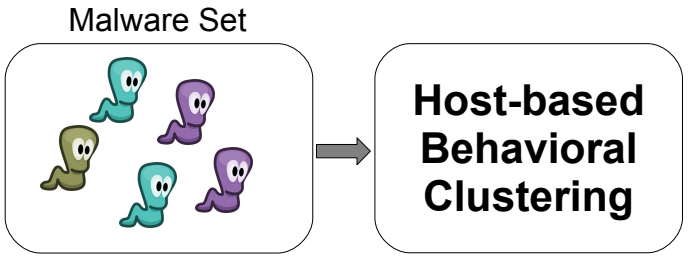
Feb09	Mar09
78.6%	48.9%

Using only fine-grained clustering



Feb09	Mar09
60.1%	35.1%

Using approach proposed in [Bayer et al. NDSS 2009]



Feb09	Mar09
56.9%	33.9%

Conclusion

- Novel behavioral malware clustering system
- Focus on network-level behavior
- Find malware families
- Trade-off between efficiency and accuracy
- Better detection models compared to using host-level behavioral clustering approaches
- Malware signatures complement existing host-level malware detection approaches

"If I haven't said this enough, this tool is so badass Roberto...
It does an awesome job correlating and clustering these samples"

Sean M. Bodmer, CISSP CEH
Senior Research Analyst
Damballa, Inc.

Thank You!

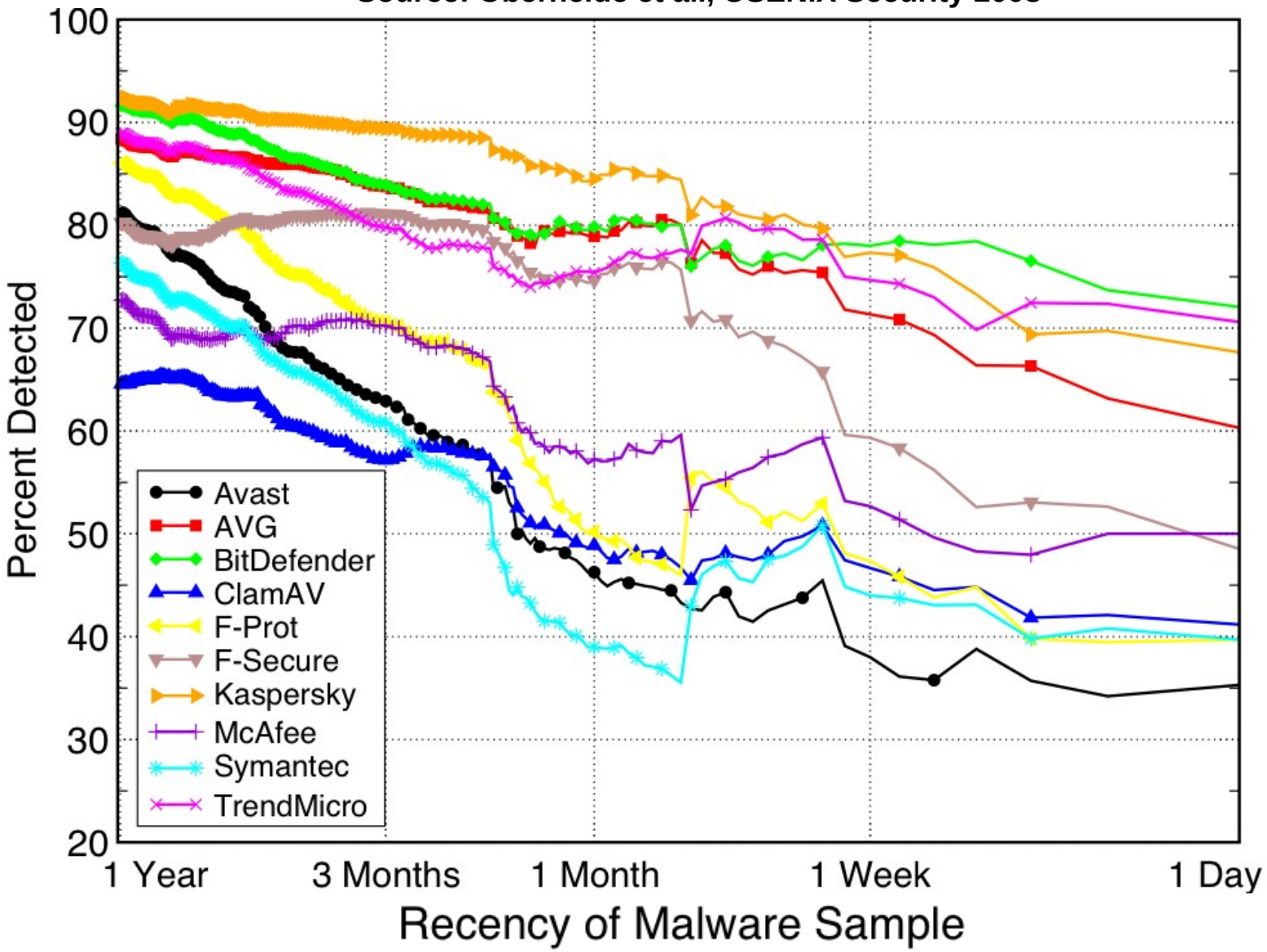
Q&A?

perdisci@gtisc.gatech.edu

Appendix

AV malware detection stats

Source: Oberheide et al., USENIX Security 2008

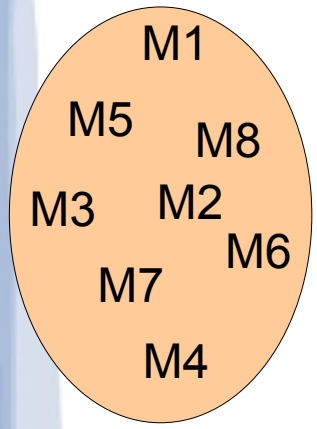


Real-World Deployment

- Deployed in large enterprise network
  - ~ 2k-3k active nodes
  - 4 days of testing
- Findings
  - **25** machines infected by ***spyware***
  - **19** machines infected by ***scareware*** (fake AVs)
  - **1** ***bot***-compromised machine
  - **1** machine compromised by ***banker trojan***

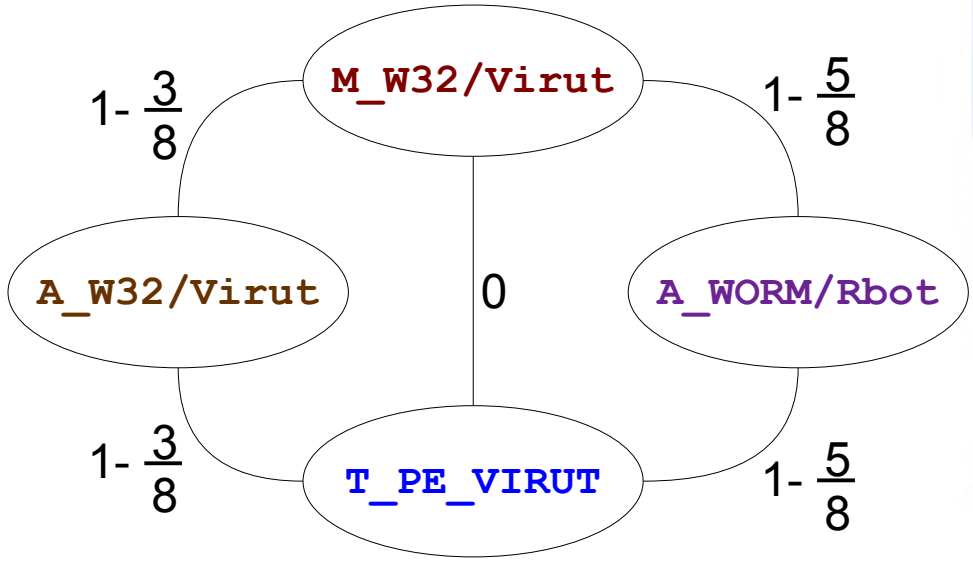
Cluster Validity Analysis

Malware Cluster



	McAfee	Avira	Trend Micro
M1 :	W32/Virut.gen	WORM/Rbot.50176.5	PE_VIRUT.D-1
M2 :	W32/Virut.gen	WORM/Rbot.50176.5	PE_VIRUT.D-2
M3 :	W32/Virut.gen	W32/Virut.Gen	PE_VIRUT.D-4
M4 :	W32/Virut.gen	W32/Virut.X	PE_VIRUT.XO-2
M5 :	W32/Virut.gen	WORM/Rbot.50176.5	PE_VIRUT.D-2
M6 :	W32/Virut.gen	W32/Virut.H	PE_VIRUT.NS-2
M7 :	W32/Virut.gen	WORM/Rbot.50176.5	PE_VIRUT.D-2
M8 :	W32/Virut.gen	WORM/Rbot.50176.5	PE_VIRUT.D-1

AV-Label Graph



Cohesion Index

$$c(\mathbf{C}_i) = 1 - \frac{1}{\gamma} \frac{2}{n \cdot v(n \cdot v - 1)} \sum_{l_1 < l_2} \delta_{l_1, l_2}$$

Separation Index

$$s(\mathbf{C}_i, \mathbf{C}_j) = \frac{1}{\gamma} \operatorname{avg}_{k,h} \{\Delta(V_k^{(i)}, V_h^{(j)})\}$$

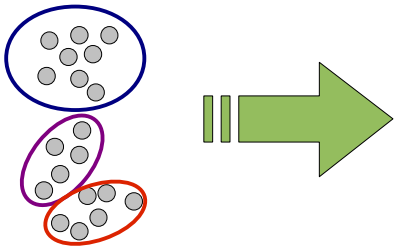
Experimental Results

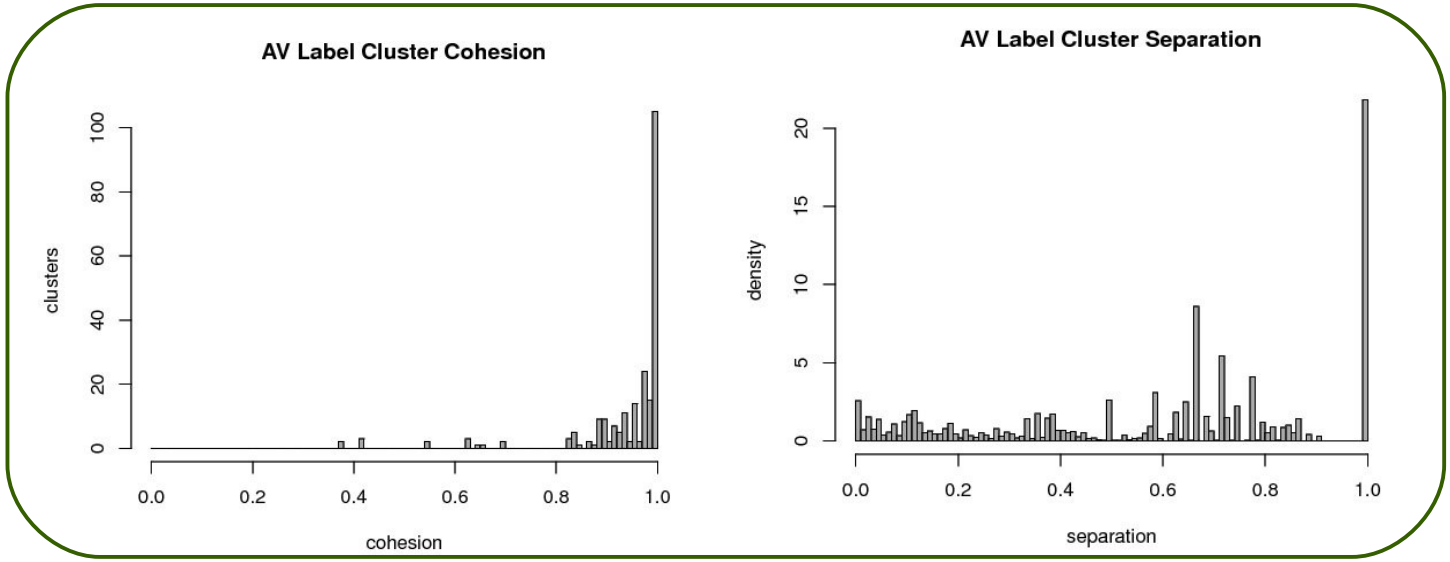
6 months malware collection → over 25k distinct samples

	Malware Samples			Number of Clusters			Processing Time		
dataset	**samples**	**undetected by all AVs**	**undetected by best AV**	**coarse**	**fine**	**meta**	**coarse**	**fine**	**meta+sig**
Feb09	4,758	208 (4.4%)	327 (6.9%)	2,538	2,660	1,499	34min	22min	6h55min
Mar09	3,563	252 (7.1%)	302 (8.6%)	2,160	2,196	1,779	19min	3min	1h3min
Apr09	2,274	142 (6.2%)	175 (7.7%)	1,325	1,330	1,167	8min	5min	28min
May09	4,861	997 (20.5%)	1,127 (23.2%)	3,339	3,423	2,593	56min	8min	2h52min
Jun09	4,677	1,038 (22.2%)	1,164 (24.9%)	3,304	3,344	2,537	57min	3min	37min
Jul09	5,587	1,569 (28.1%)	1,665 (29.8%)	3,358	3,390	2,724	1h5min	5min	2h22min

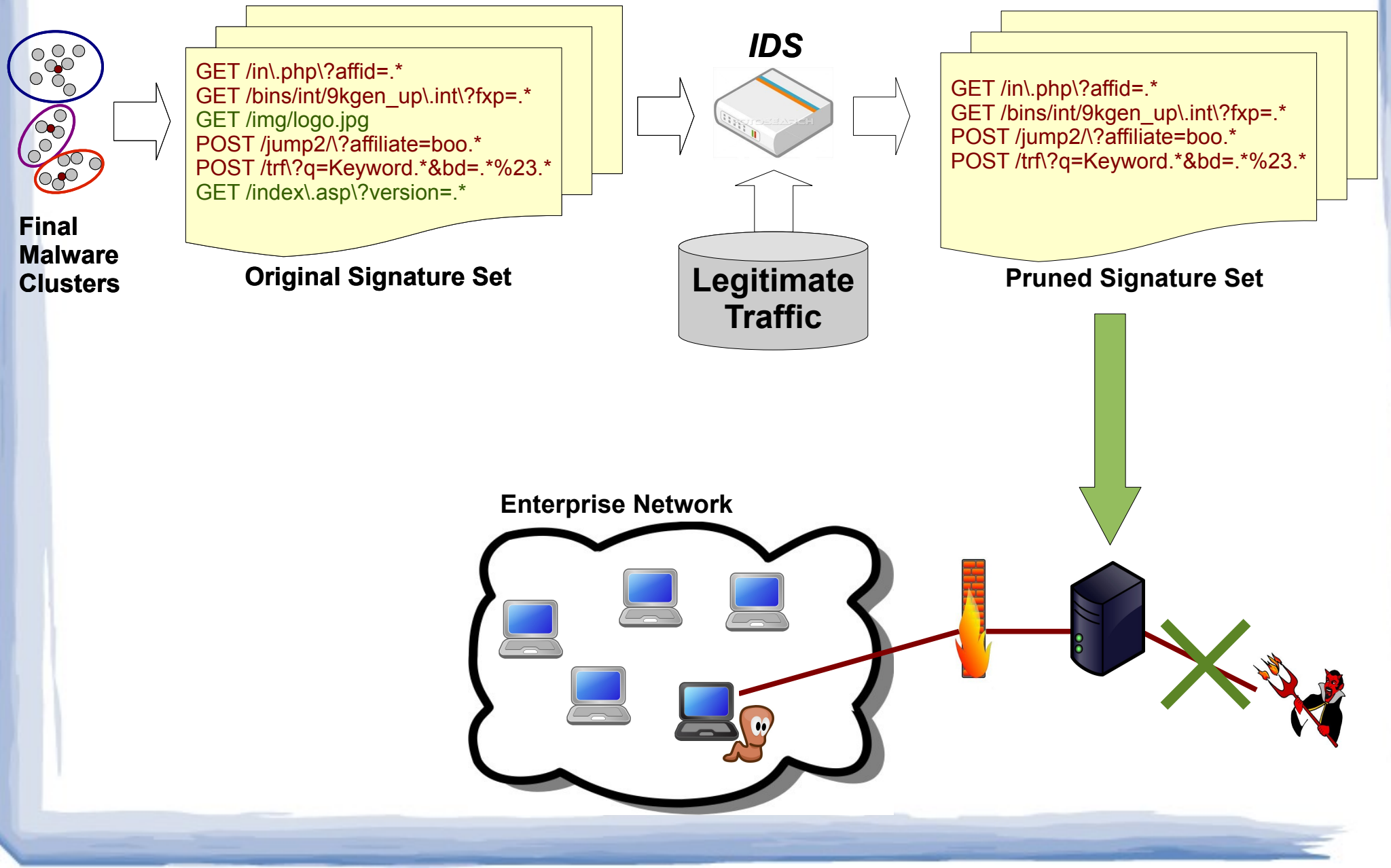
Compact and well Separated Clusters

Cluster Validity Analysis





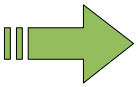
Signature Generation and Pruning



Experimental Results

Malware Detection rate (all samples)

	Feb09	*Mar09*	*Apr09*	*May09*	*Jun09*	*Jul09*
Sig_Feb09	85.9%	50.4%	47.8%	27.0%	21.7%	23.8%
Sig_Mar09	-	64.2%	38.1%	25.6%	23.3%	28.6%
Sig_Apr09	-	-	63.1%	26.4%	27.6%	21.6%
Sig_May09	-	-	-	59.5%	46.7%	42.5%
Sig_Jun09	-	-	-	-	58.9%	38.5%
Sig_Jul09	-	-	-	-	-	65.1%



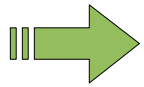
Detects significant fraction of current and *future* malware variants

False Positives as measured on 12M legitimate HTTP requests from 2,010 clients

	Sig_Feb09	*Sig_Mar09*	*Sig_Apr09*	*Sig_May09*	*Sig_Jun09*	*Sig_Jul09*
FP rate	0% (0)	$3 \cdot 10^{-4}$% (38)	$8 \cdot 10^{-6}$% (1)	$5 \cdot 10^{-5}$% (6)	$2 \cdot 10^{-4}$% (26)	10^{-4}% (18)
Distinct IPs	0% (0)	0.3% (6)	0.05% (1)	0.2% (4)	0.4% (9)	0.3% (7)
Processing Time	13 min	10 min	6 min	9 min	12 min	38 min

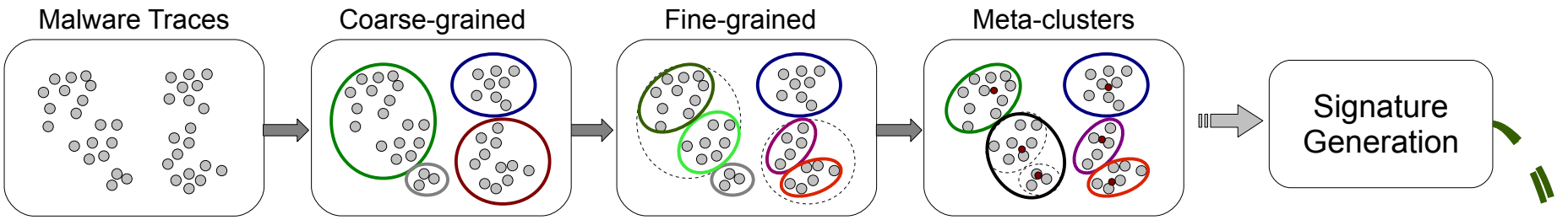
"Zero-Day" Malware Detection rate

	Feb09	*Mar09*	*Apr09*	*May09*	*Jun09*	*Jul09*
Sig_Feb09	54.8%	52.8%	29.4%	6.1%	3.6%	4.0%
Sig_Mar09	-	54.1%	20.6%	5.0%	3.1%	5.4%
Sig_Apr09	-	-	41.9%	5.8%	3.8%	5.2%
Sig_May09	-	-	-	66.7%	38.8%	16.1%
Sig_Jun09	-	-	-	-	48.9%	21.8%
Sig_Jul09	-	-	-	-	-	62.9%



Complements traditional AV detection systems

Comparison with other approaches



	Feb09	*Mar09*	*May09*	*Jun09*
Sig_Feb09 net-clusters	78.6%	48.9%	-	-
Sig_Feb09 net-fg-clusters	60.1%	35.1%	-	-
Sig_Feb09 sys-clusters	56.9%	33.9%	-	-
Sig_May09 net-clusters	-	-	56.0%	44.3%
Sig_May09 net-fg-clusters	-	-	50.8%	42.5%
Sig_May09 sys-clusters	-	-	32.7%	32.0%

Reduced dataset of ~4k malware samples

net-clusters **= our three-step clustering approach**
net-fg-clusters **= only fine-grained clustering**
sys-clusters **= using approach proposed in [Bayer et al. NDSS 2009]**

Challenges

- Detecting malware traffic is hard
  - Many different types of malware
  - Different communication protocols
  - Malware can use legitimate protocols to communicate (e.g., HTTP)
  - Identify malware traffic among **very large** volumes of legitimate traffic

Find a needle in haystack!