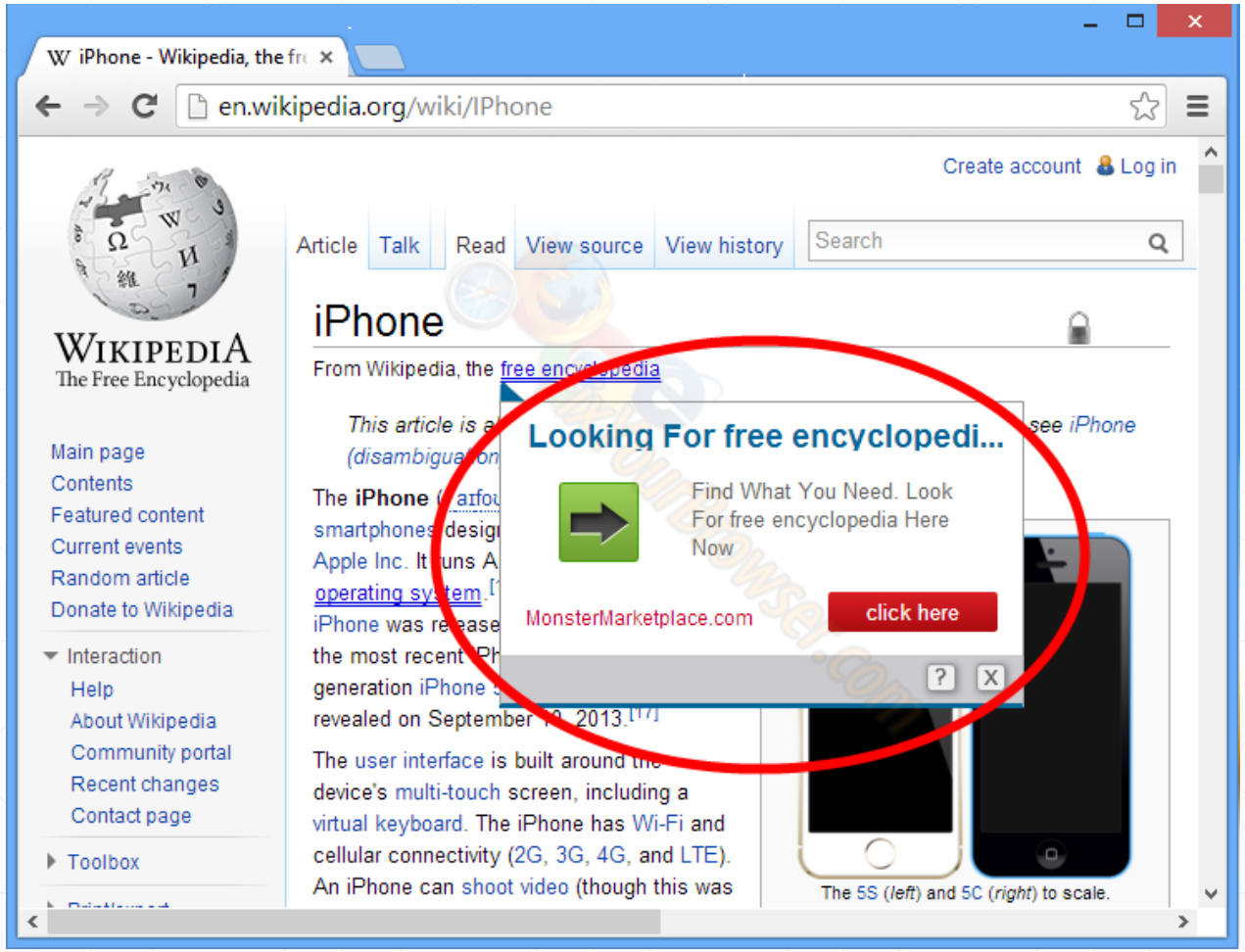
Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services

Platon Kotzias, Leyla Bilge, Juan Caballero

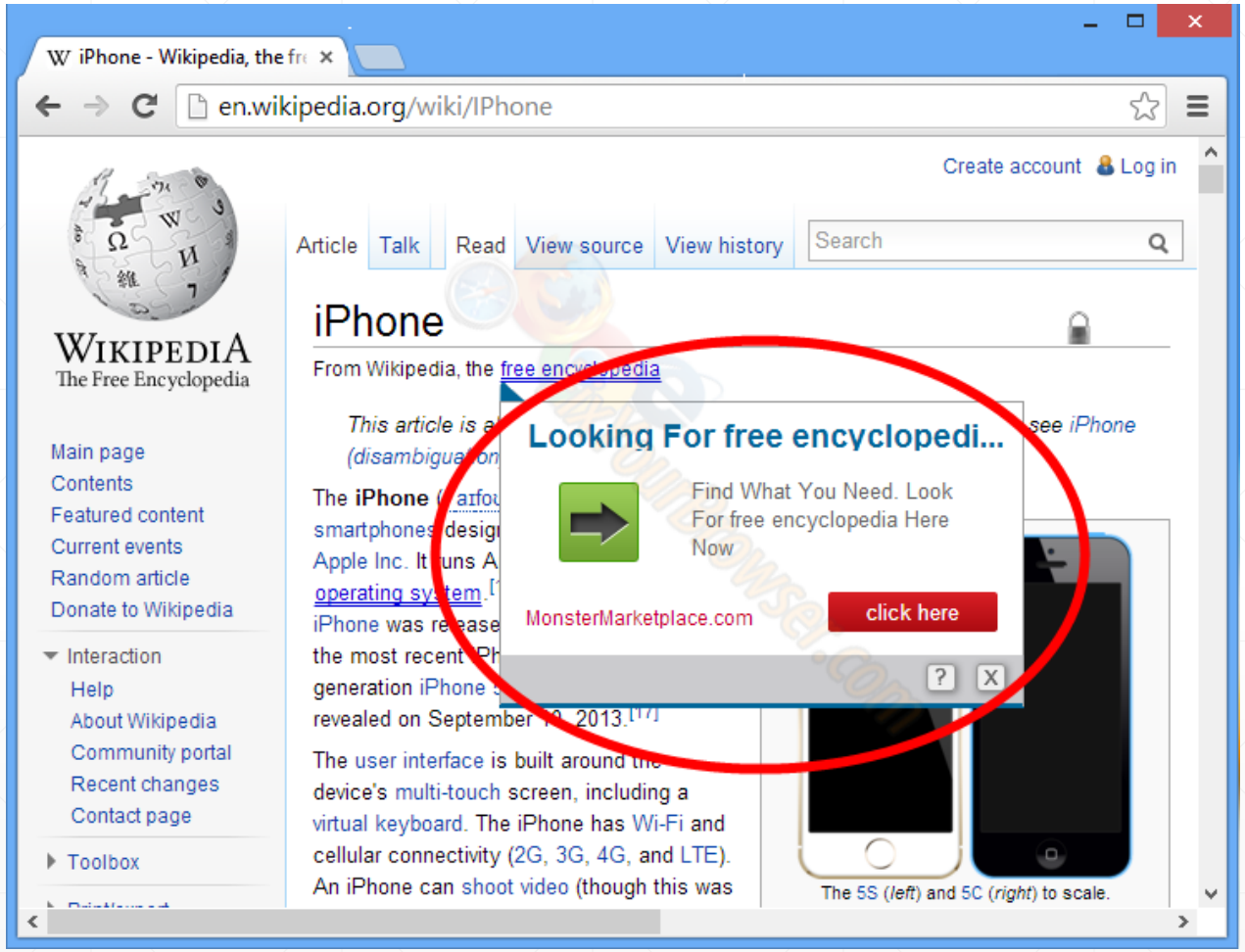




Potential Unwanted Programs (PUP)

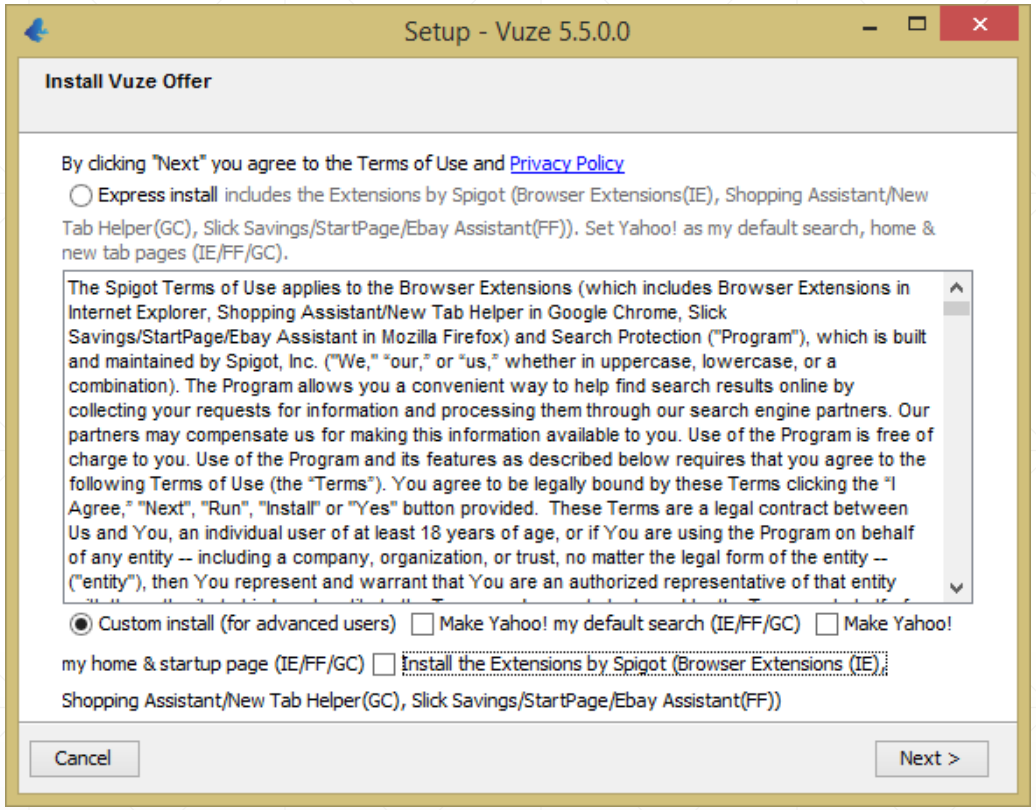


Potential Unwanted Programs (PUP)



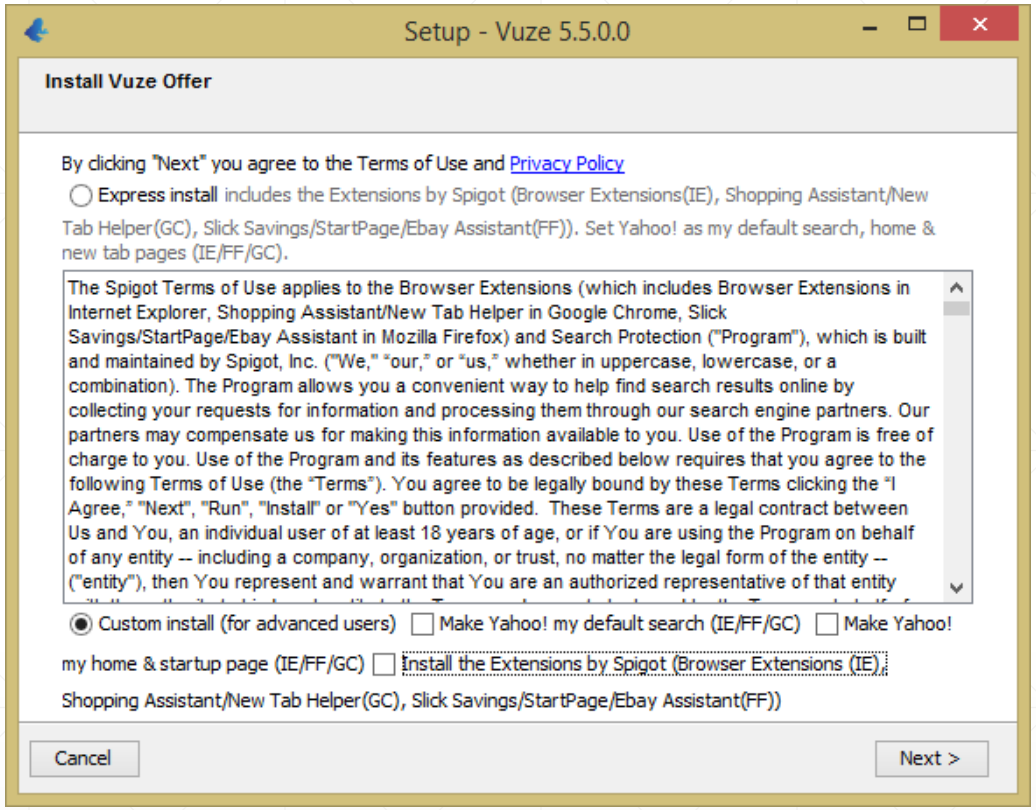


PUP vs Malware





PUP vs Malware



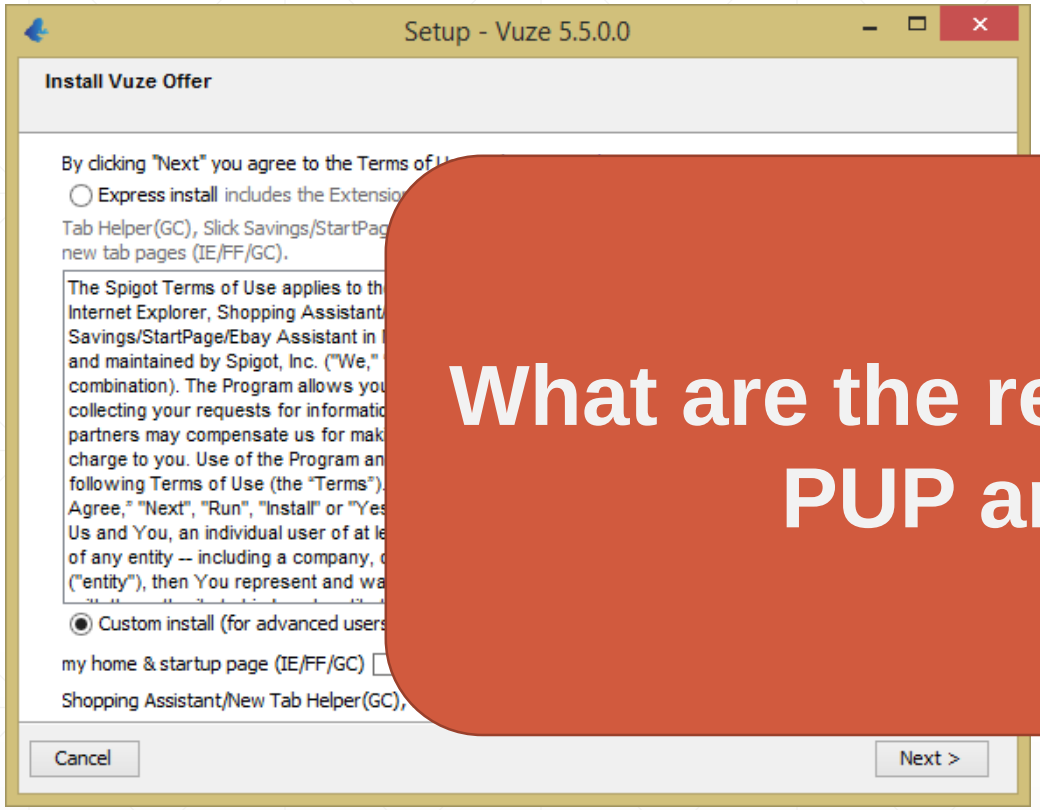


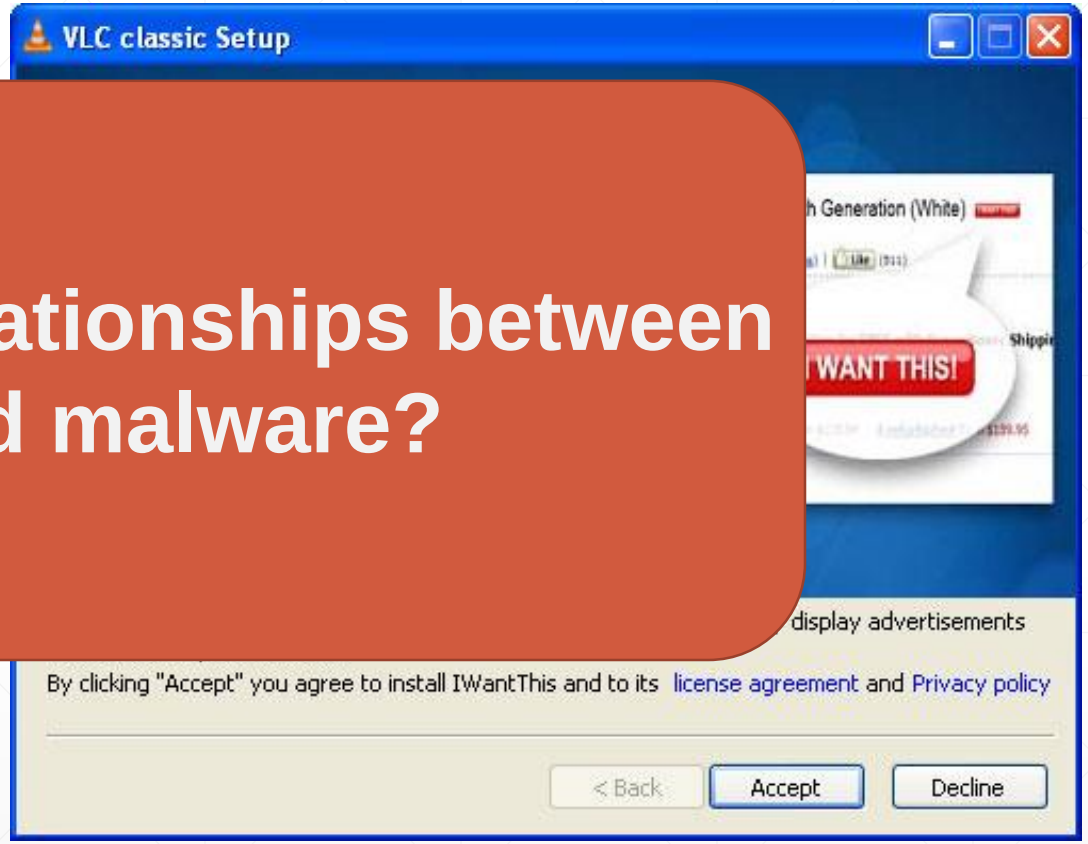
Home » Bad Sites » When Adware Goes Bad: The Installbrain and Sefnit Connection

When Adware Goes Bad: The Installbrain and Sefnit Connection

Posted on: July 7, 2014 at 8:30 am **Posted in:** Bad Sites, Malware **Author:** Trend Micro

PUP vs Malware





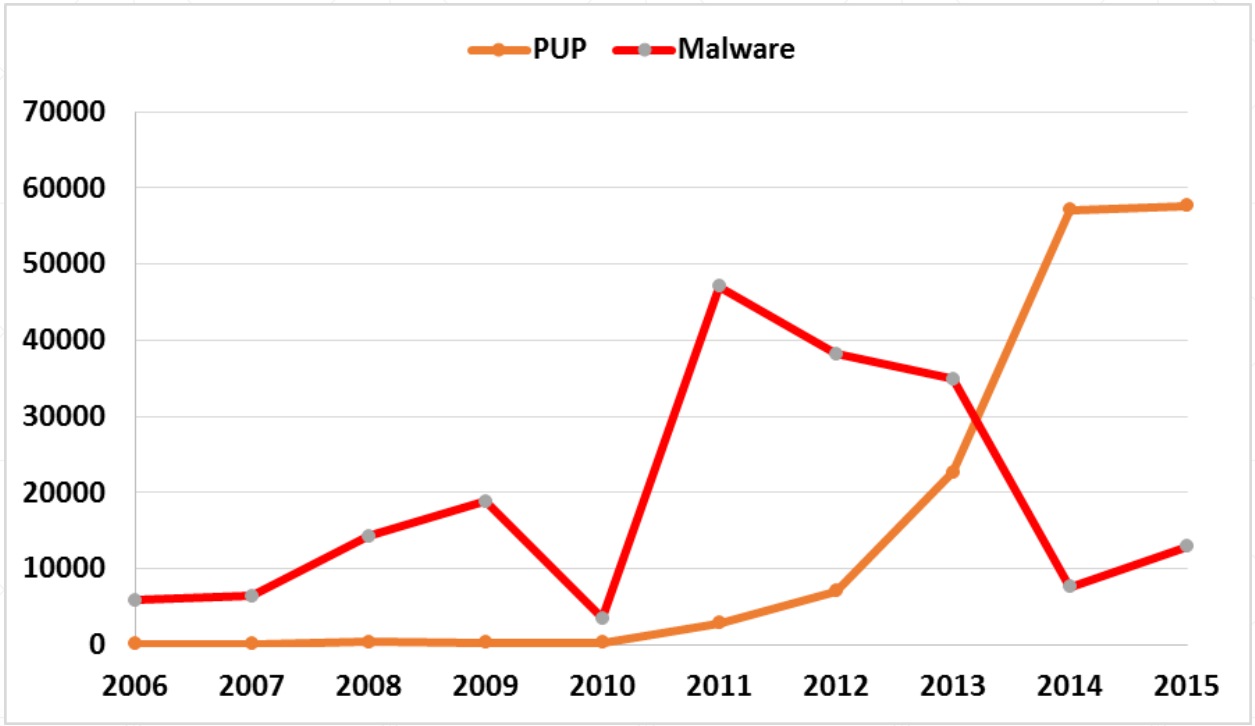
What are the relationships between PUP and malware?

Home » Bad Sites » When Adware Goes Bad: The Installbrain and Sefnit Connection

When Adware Goes Bad: The Installbrain and Sefnit Connection

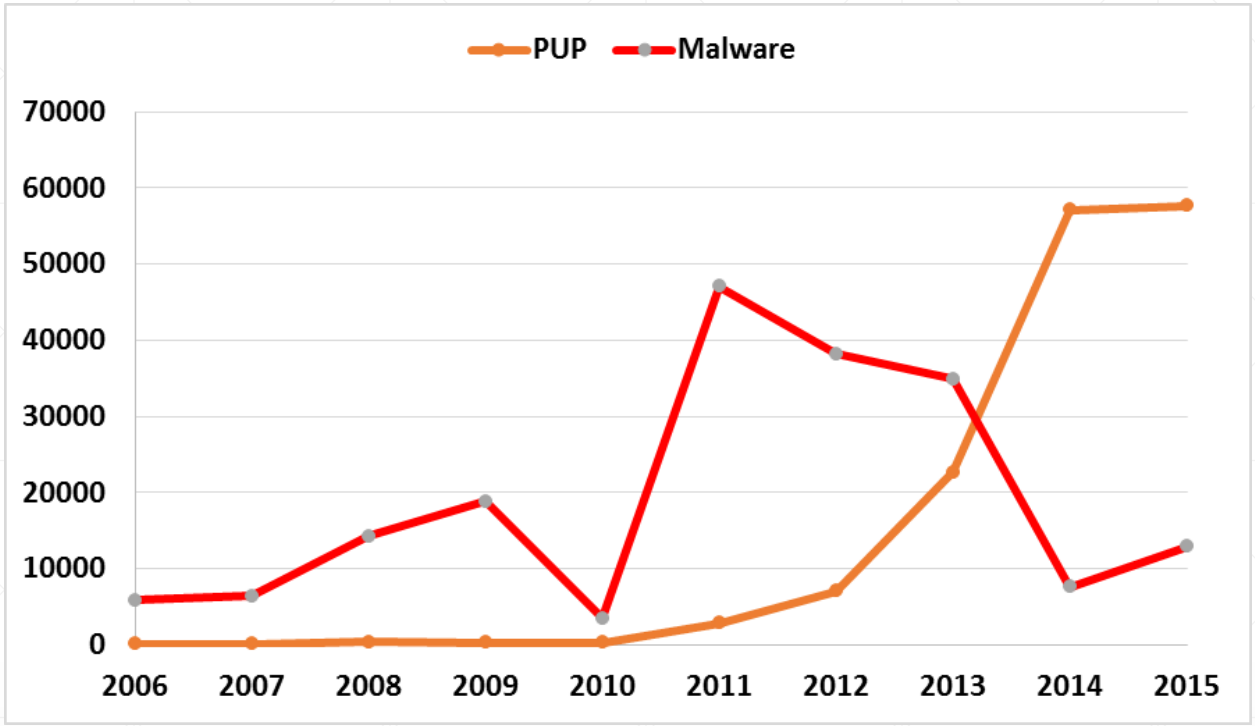
Posted on: July 7, 2014 at 8:30 am **Posted in:** Bad Sites, Malware **Author:** Trend Micro

Evidence of PUP Prevalence



Kotzias et al. Certified PUP: Abuse in Authenticode Code Signing. In Proceedings of the 22nd ACM Conference on Computer and Communication Security, 2015.

Evidence of PUP Prevalence

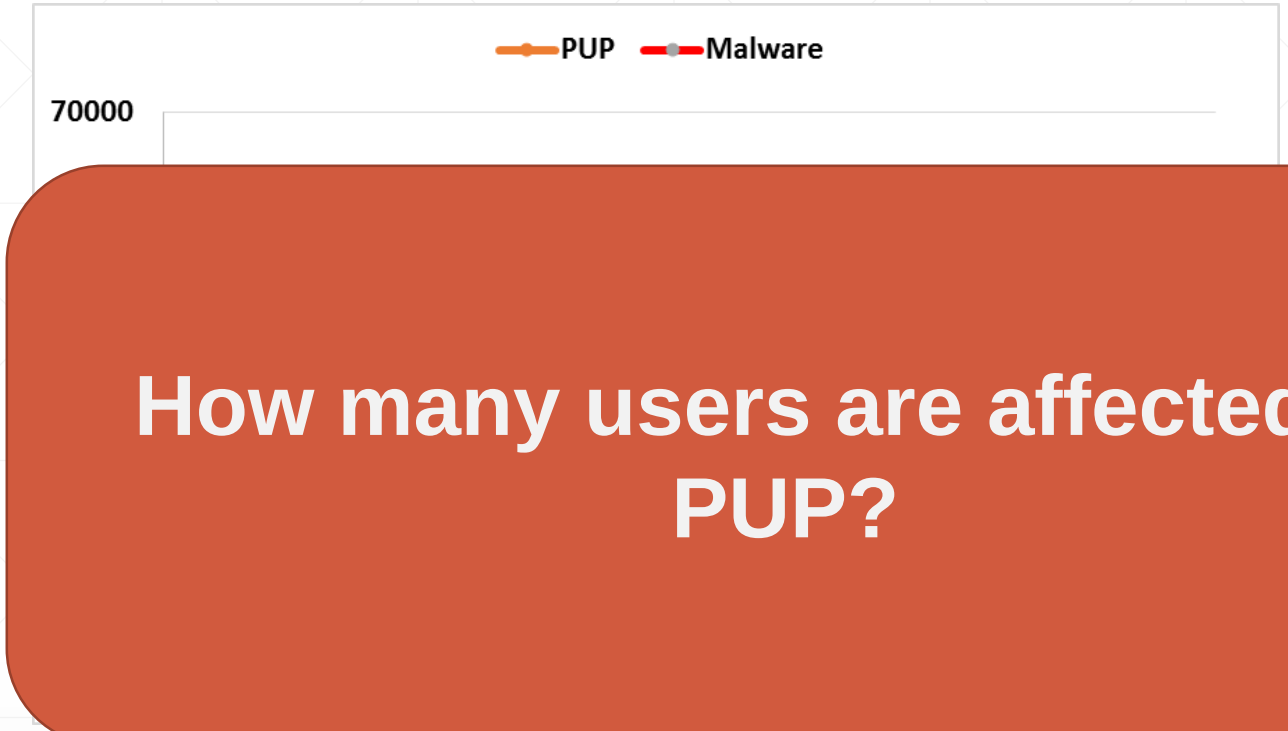


Kotzias et al. Certified PUP: Abuse in Authenticode Code Signing. In Proceedings of the 22nd ACM Conference on Computer and Communication Security, 2015.

- 5% of unique IPs accessing Google have injected advertisements

Thomas et al. Ad injection at scale: Assessing deceptive advertisement modification. In Proceedings of the IEEE Symposium on Security and Privacy, 2015.

Evidence of PUP Prevalence



How many users are affected by PUP?

Kotzias et al. Certified PUP: Abuse in Authenticode Code Signing. In Proceedings of the 22nd ACM Conference on Computer and Communication Security, 2015.

- 5% of unique IPs accessing Google have injected advertisements

Thomas et al. Ad injection at scale: Assessing deceptive advertisement modification. In Proceedings of the IEEE Symposium on Security and Privacy, 2015.

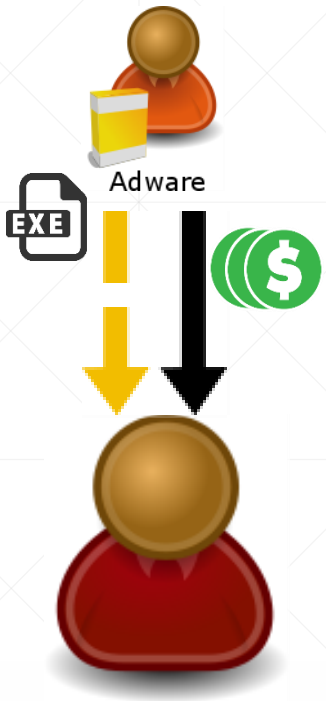
Pay-Per-Install (PPI) Ecosystem



Advertisers



Pay-Per-Install (PPI) Ecosystem

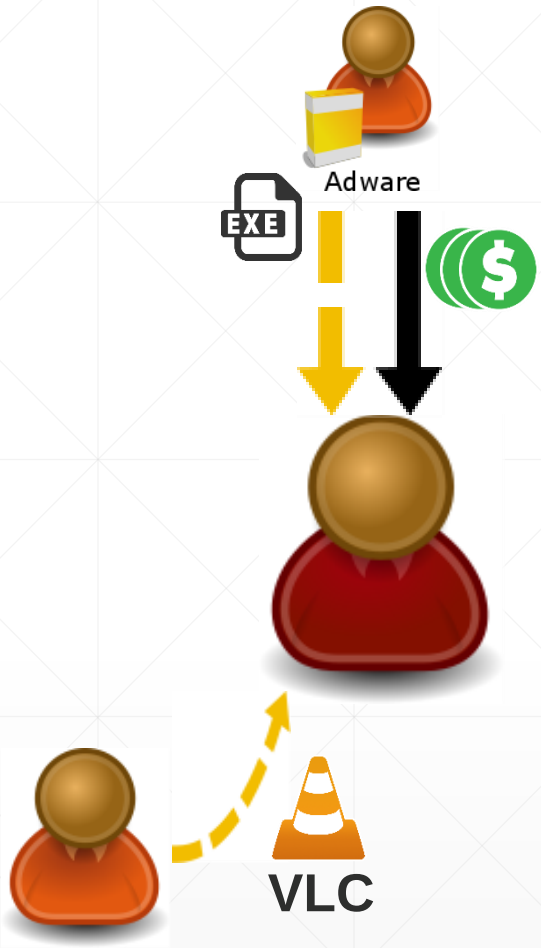


Advertisers



PPI Service

Pay-Per-Install (PPI) Ecosystem

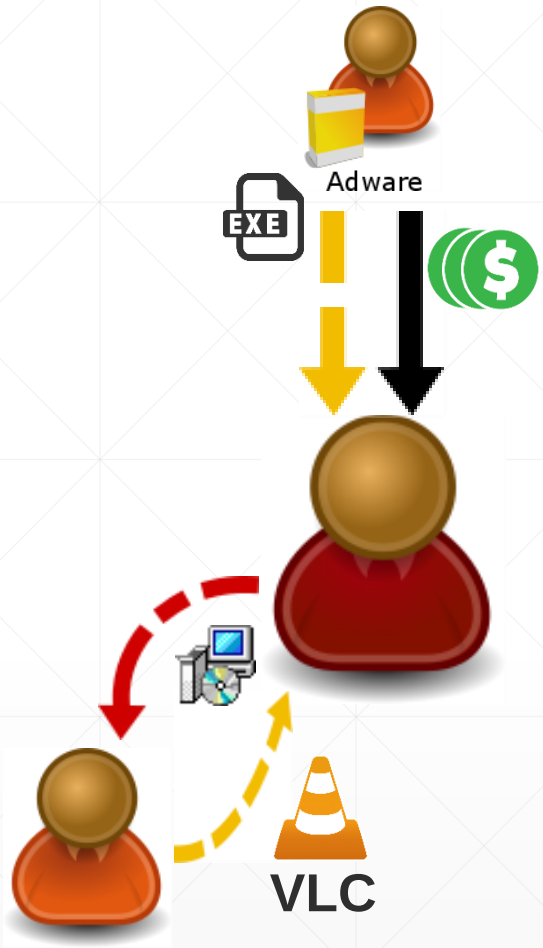


Advertisers

PPI Service

Affiliate Publishers

Pay-Per-Install (PPI) Ecosystem



Advertisers



PPI Service

Affiliate Publishers

Pay-Per-Install (PPI) Ecosystem



Advertisers



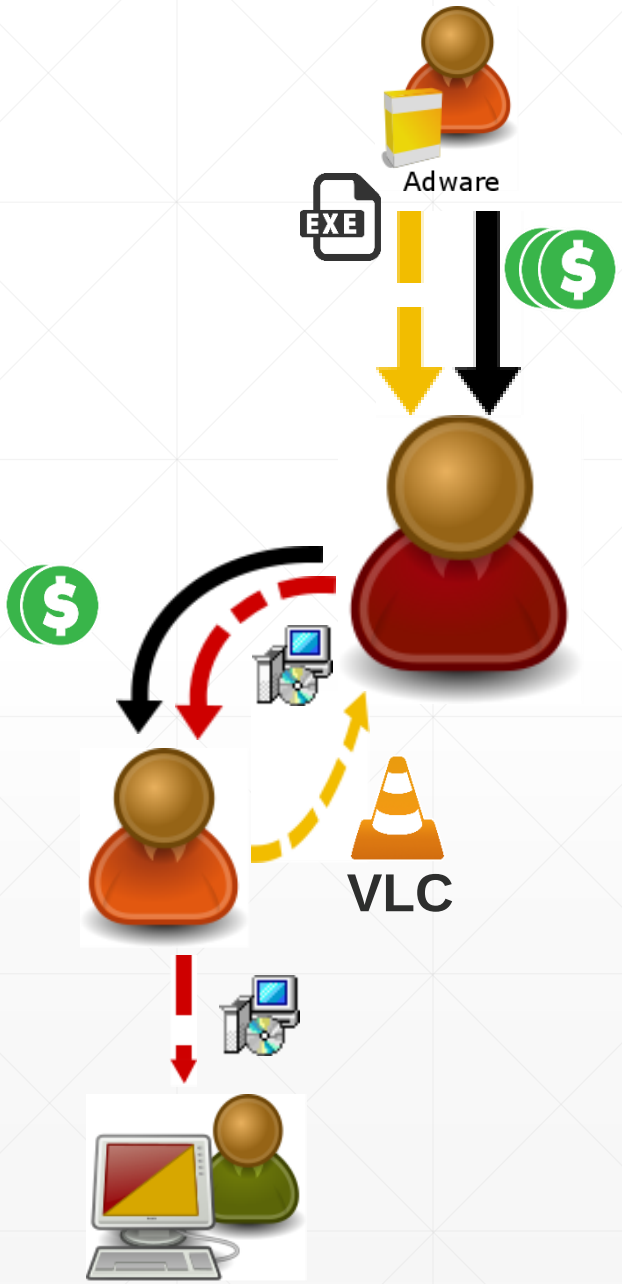
PPI Service

Affiliate Publishers

Target Hosts



Pay-Per-Install (PPI) Ecosystem



Advertisers

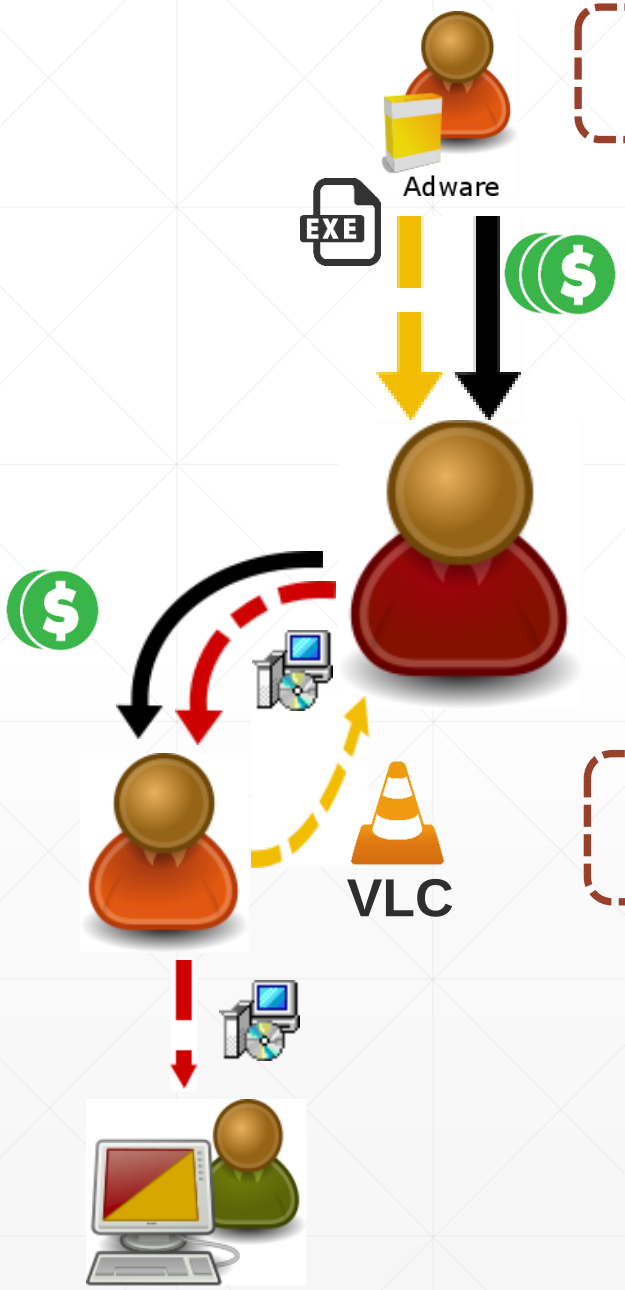
PPI Service

Affiliate Publishers

Target Hosts



Pay-Per-Install (PPI) Ecosystem



Advertisers

PPI Service

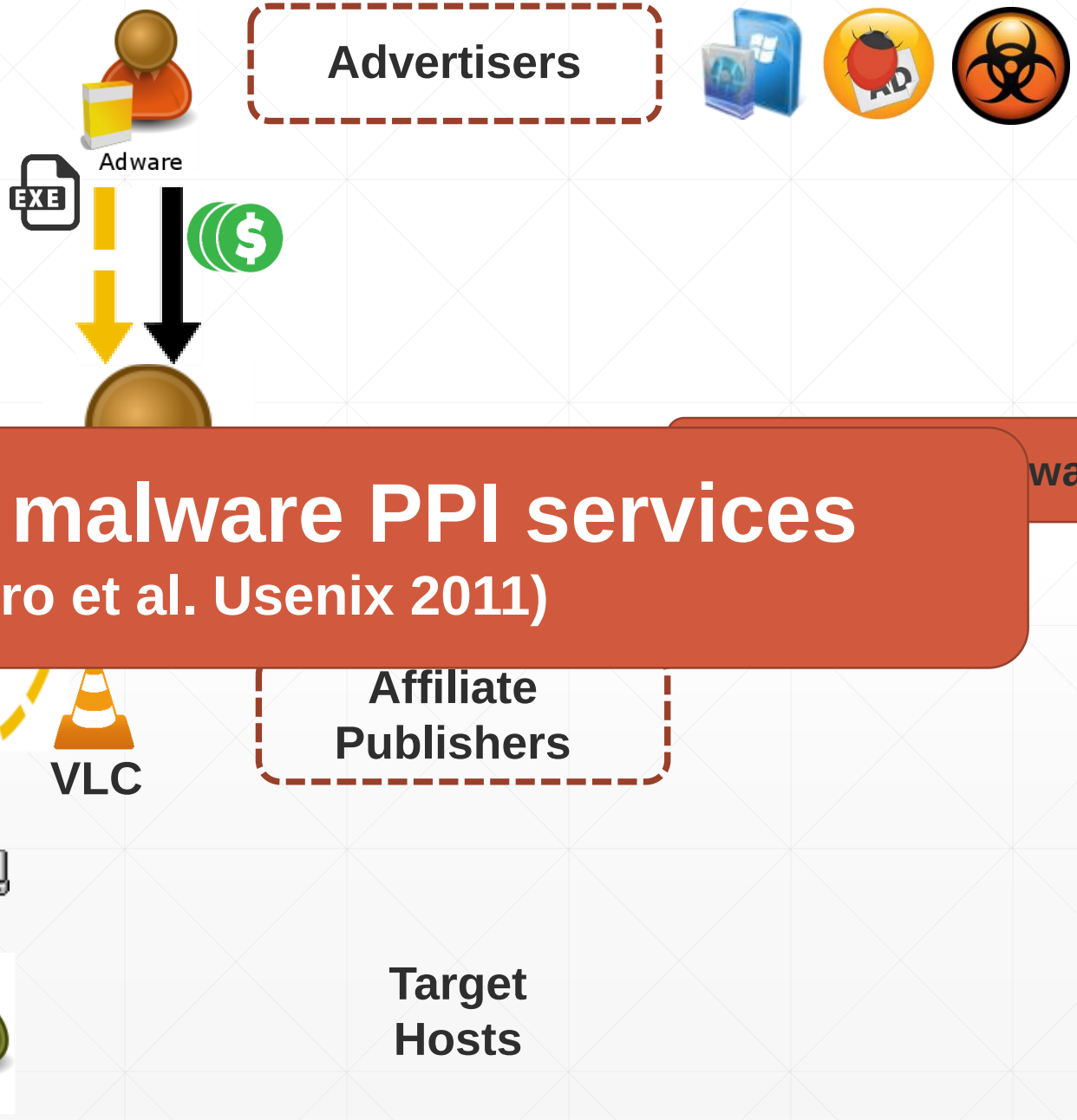
Publishers = Software owners

Affiliate Publishers

Target Hosts



Pay-Per-Install (PPI) Ecosystem





Pay-Per-Install (PPI) Ecosystem



How many PPI services?
What type of PUP is advertised?

Di

ware owners

Publishers

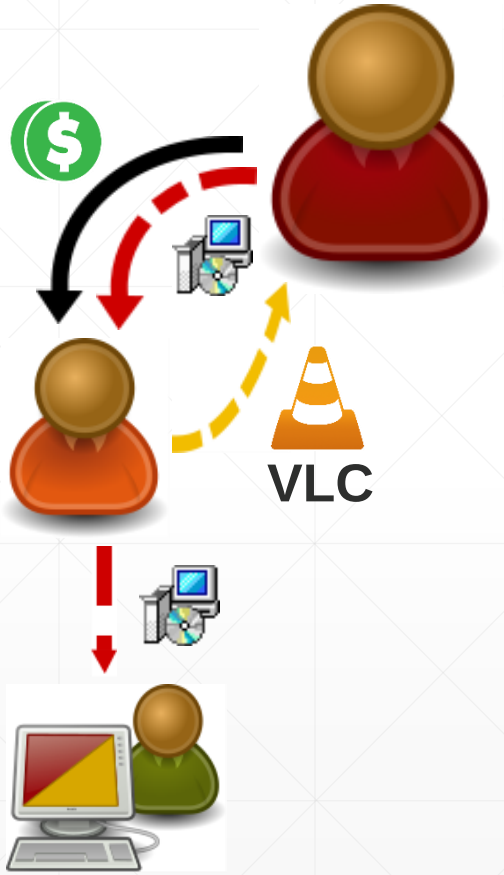
VLC





Target Hosts

Pay-Per-Install (PPI) Ecosystem

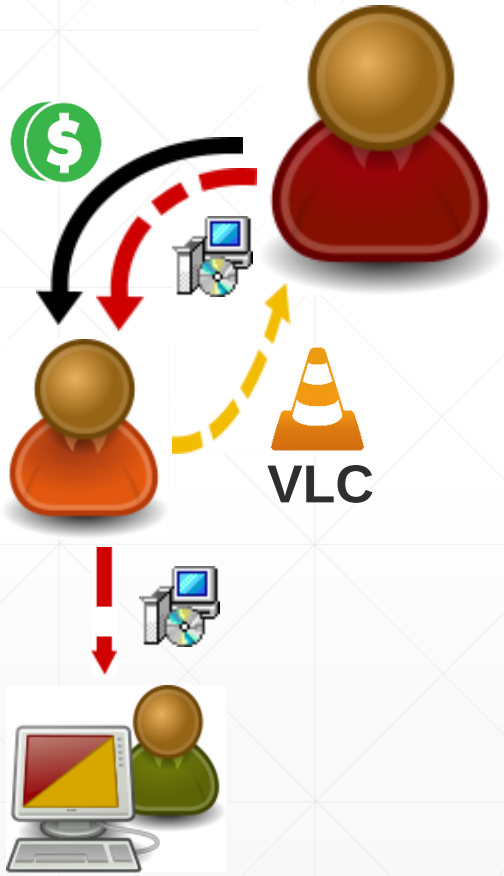


PPI Service

Affiliate Publishers

Target Hosts

Pay-Per-Install (PPI) Ecosystem



PPI Service

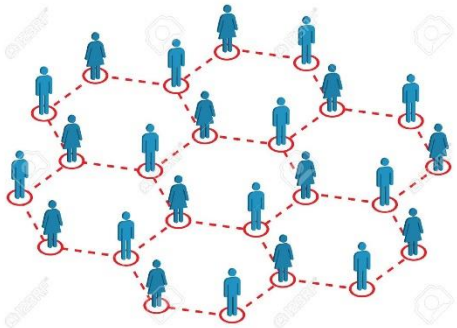
Affiliate Publishers

Target Hosts

Country	PPI (Avg.)	Malware PPI (Avg.)
United States	$1.30	$0.11
United Kingdom	$0.80	$0.16
Australia	$0.40	$0.13
Canada	$0.40	$0.09
France	$0.28	$0.06

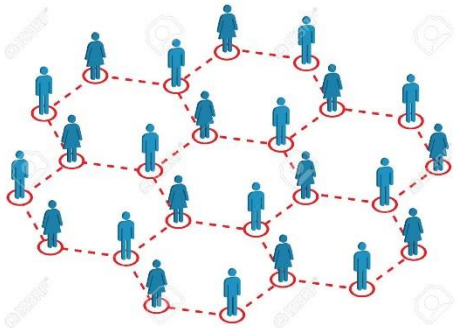
Malware distribution through malware PPIs can be up to an order of magnitude cheaper

Contributions

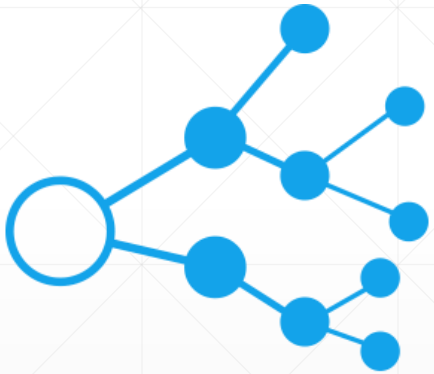


Measure PUP prevalence and its distribution through PPI services

Contributions



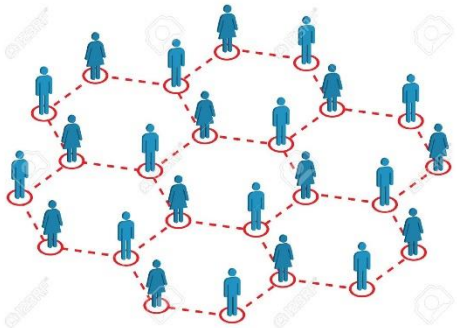
Measure PUP prevalence and its distribution through PPI services



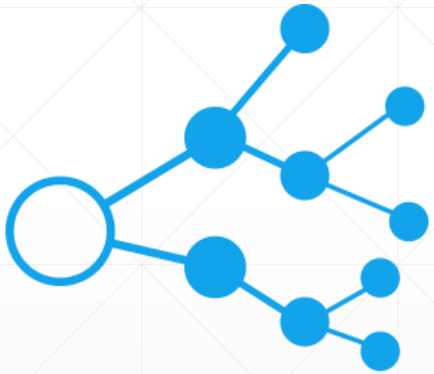
Build publisher graph to captures who-installs-who relationships among PUP Publishers

Identify the prevalent PPI services and advertisers

Contributions



Measure PUP prevalence and its distribution through PPI services



Build publisher graph to captures who-installs-who relationships among PUP Publishers

Identify the prevalent PPI services and advertisers

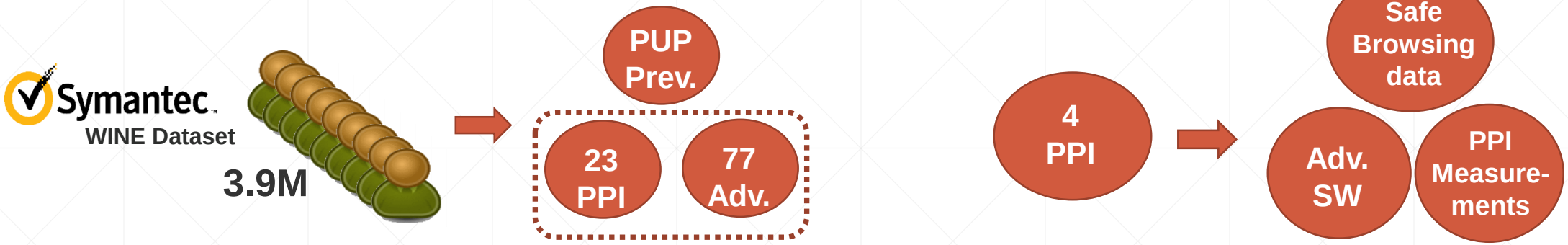




Examine PUP-Malware relationships

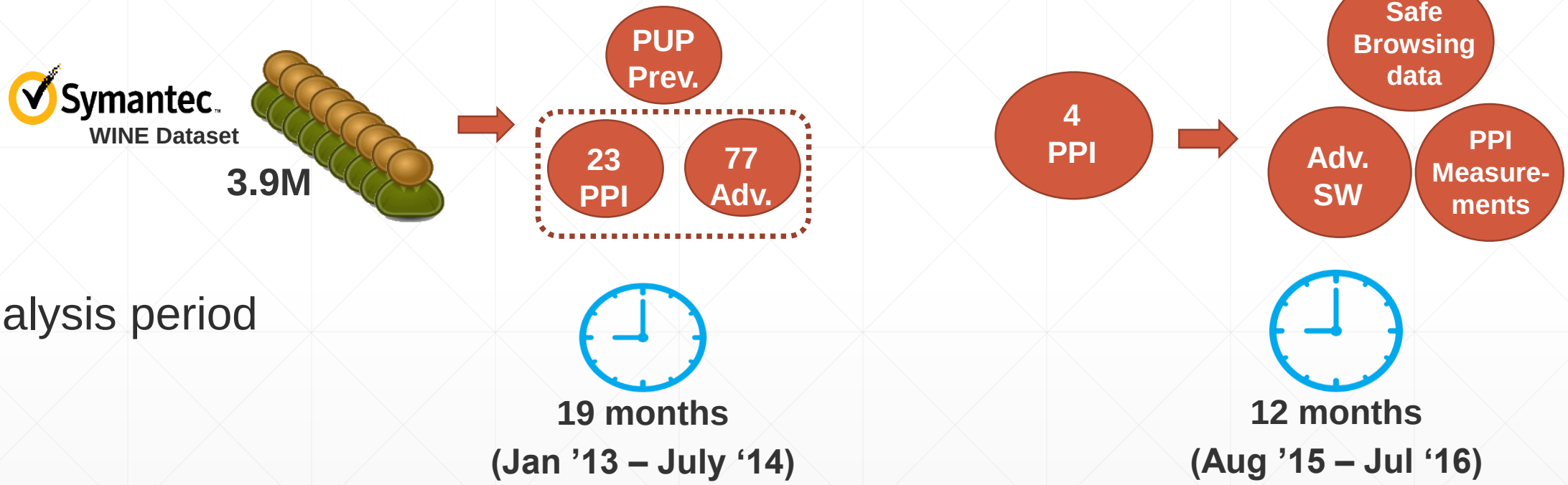
Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach



Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach



- Analysis period

Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach

Symantec
WINE Dataset
3.9M



PUP Prev.
23 PPI
77 Adv.

4 PPI

Safe Browsing data
Adv. SW
PPI Measure-ments

- Analysis period



19 months
(Jan ’13 – July ‘14)



12 months
(Aug ’15 – Jul ‘16)

- Geographical coverage





Datasets



11M reports of malicious/undesirable software

Datasets



11M reports of malicious/undesirable software

Malsign dataset

[Kotzias et al. CCS ’15]

142K signed malware and PUP (binaries & clustering families)

Datasets



11M reports of malicious/undesirable software

Malsign dataset

[Kotzias et al. CCS ’15]

142K signed malware and PUP (binaries & clustering families)



AV telemetry from **3.9M** real Windows hosts

8B events for **19 months** (Jan ‘13 – July ‘14)

Datasets

virustotal

11M reports of malicious/undesirable software

Malsign dataset

[Kotzias et al. CCS ’15]

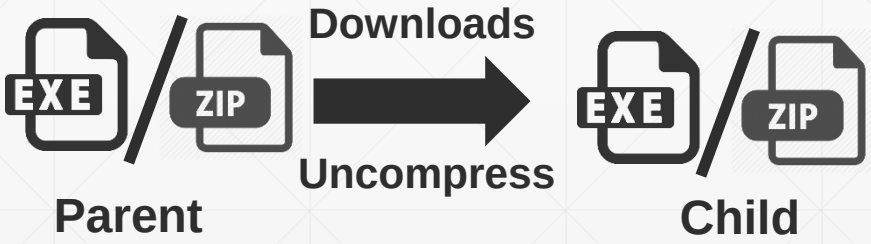
142K signed malware and PUP (binaries & clustering families)

Symantec™

WINE Dataset

AV telemetry from **3.9M** real Windows hosts

8B events for **19 months** (Jan ‘13 – July ‘14)



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]

Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

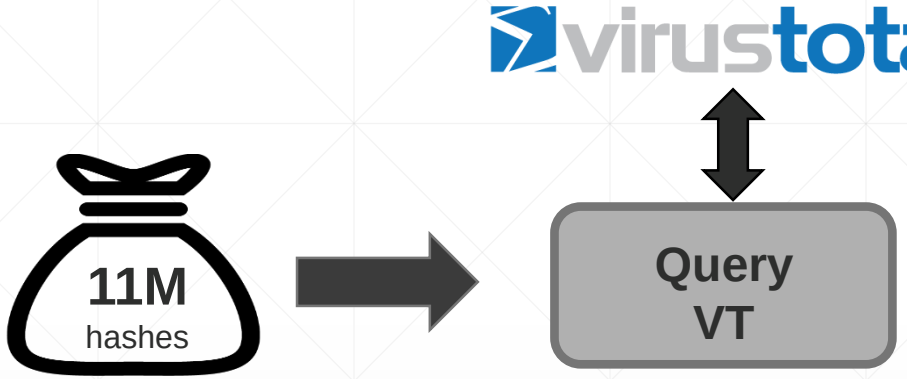
Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

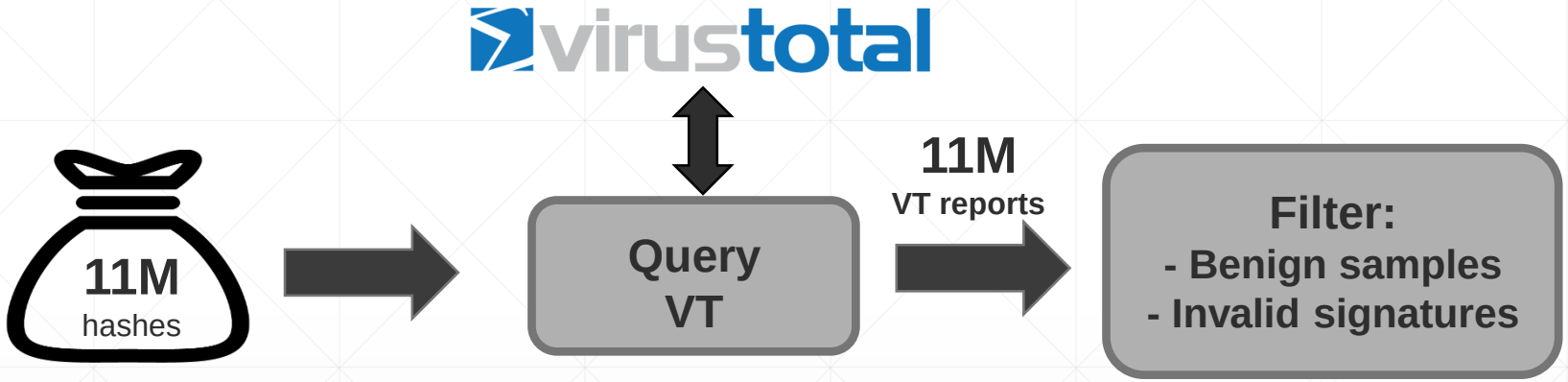
Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

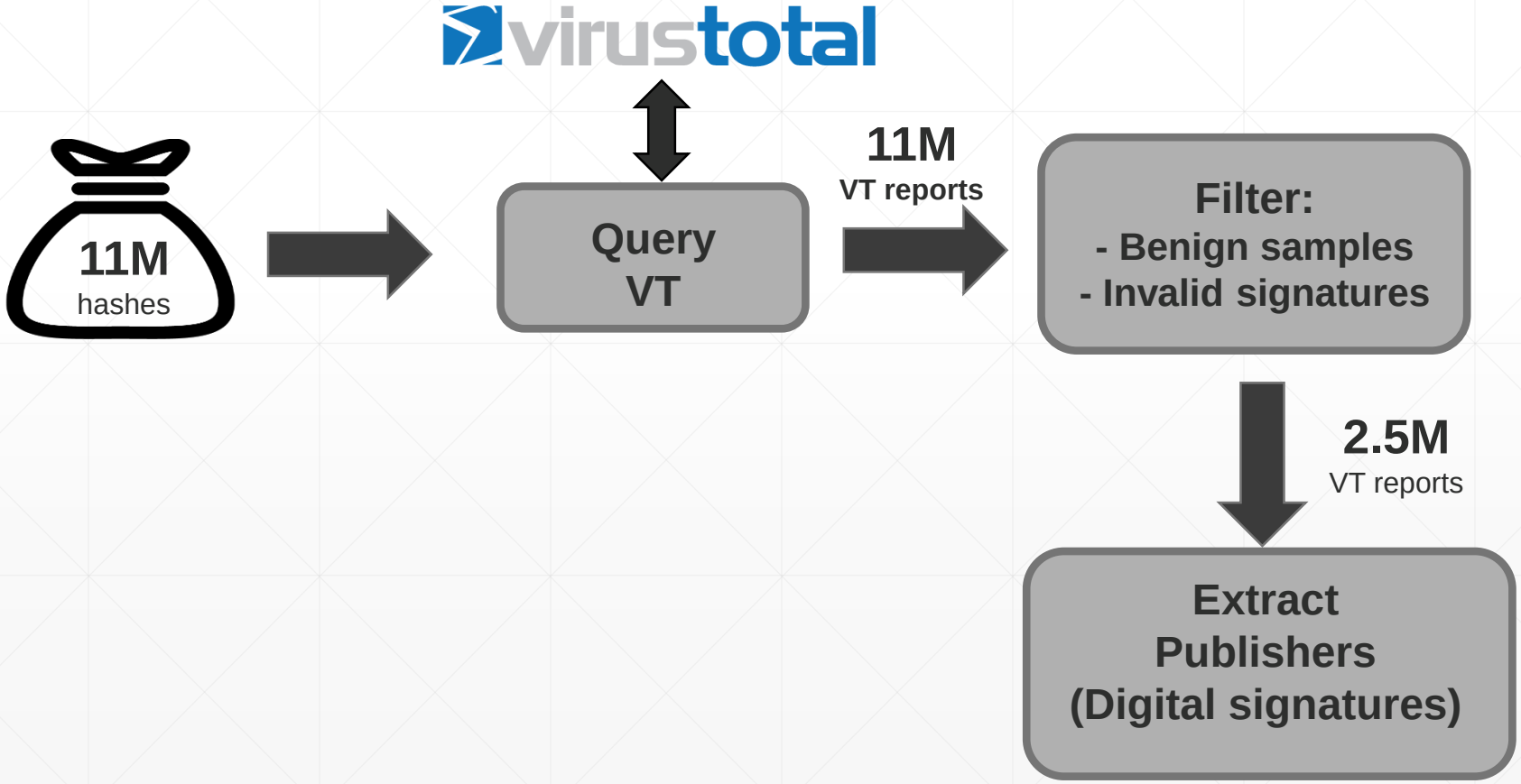
Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

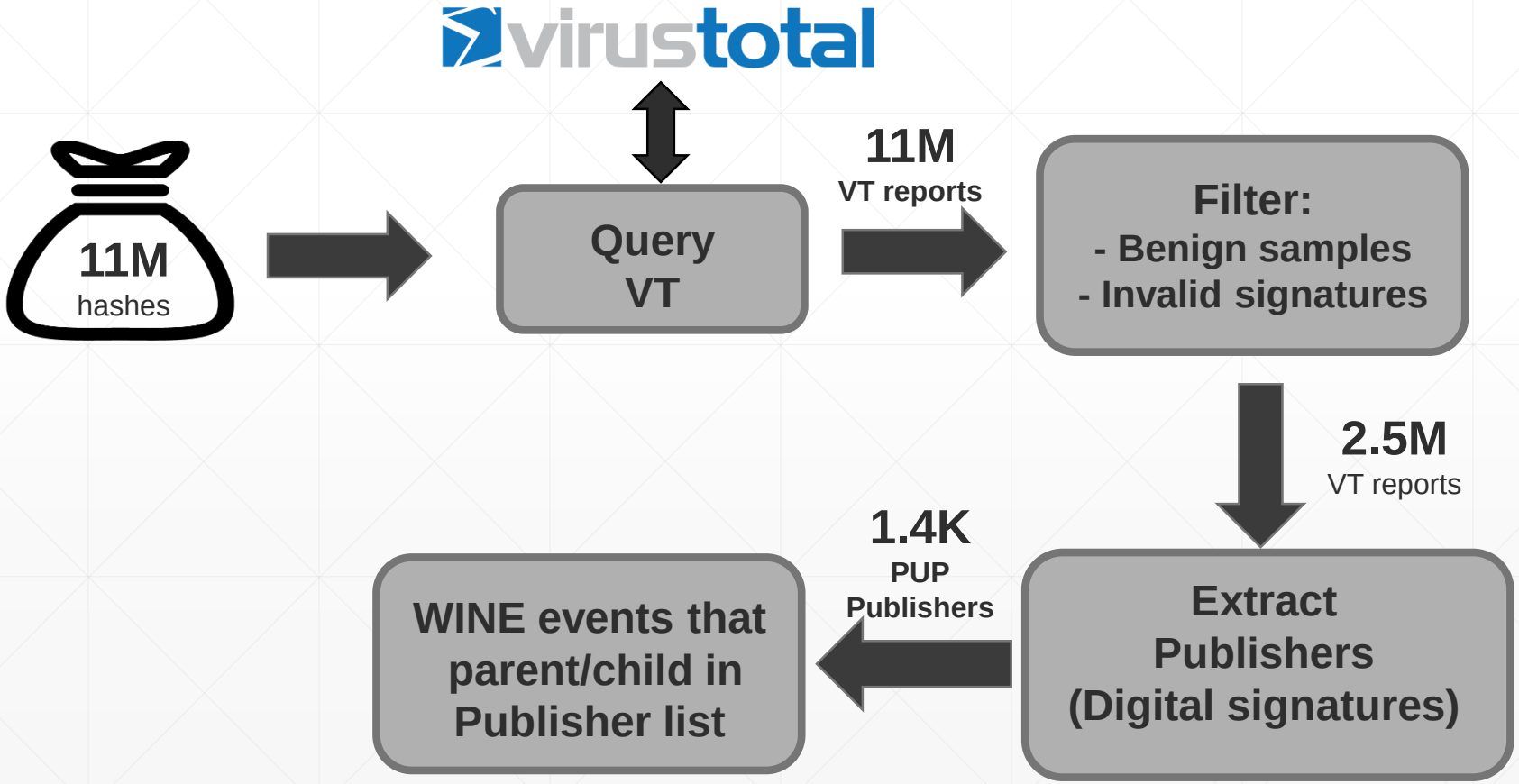
Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

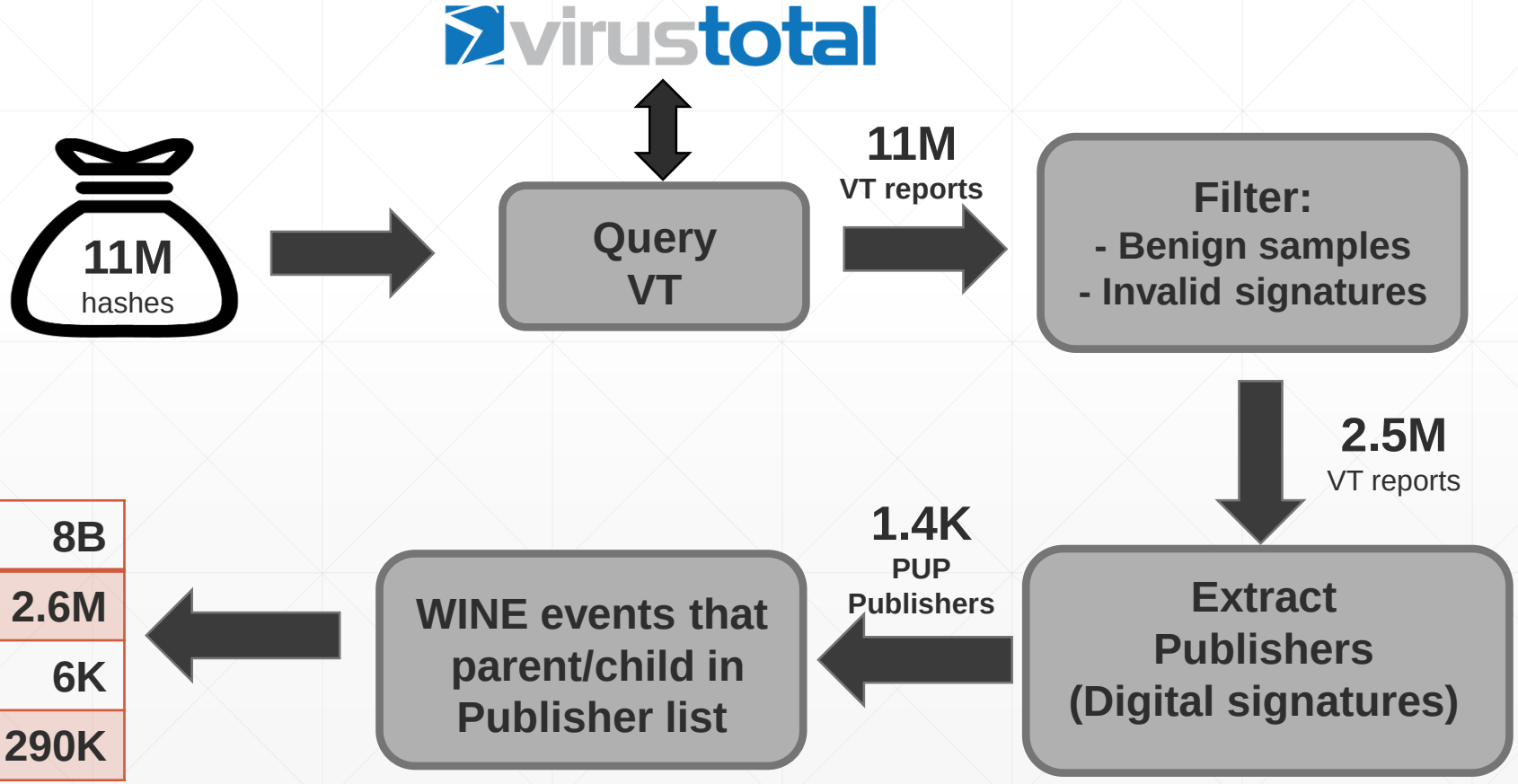
Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [*Kotzias et al. CCS '15*]



Events	8B
Files	2.6M
Publishers	6K
URLs	290K

Clustering Publishers

Publisher name similarity

Tuguu Israel Ltd
TUGUU SLU
Tuguu sl
Tuguu S.L.U.



Tuguu

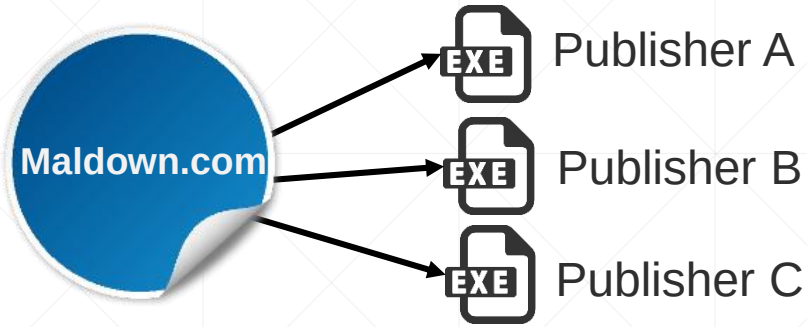
Clustering Publishers

Publisher name similarity

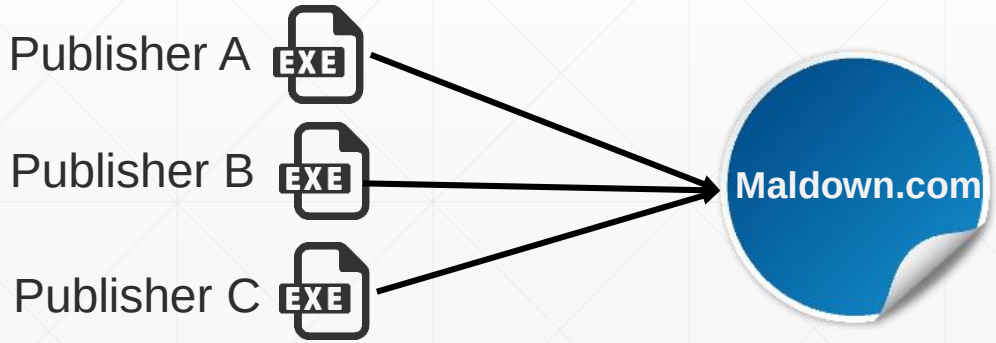
Tuguu Israel Ltd
TUGUU SLU
Tuguu sl
Tuguu S.L.U.

→ *Tuguu*

Child download domains



Parent download domains



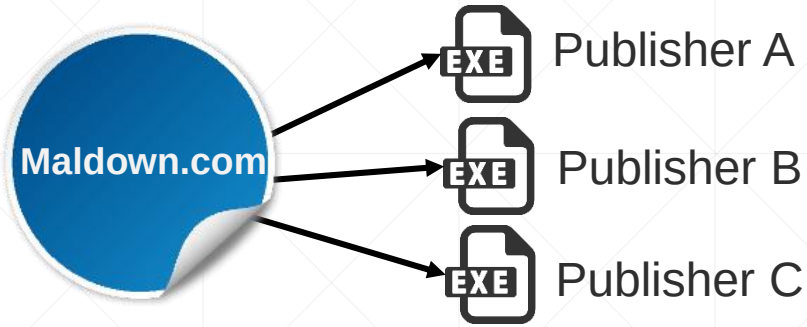
Clustering Publishers

Publisher name similarity

Tuguu Israel Ltd
TUGUU SLU
Tuguu sl
Tuguu S.L.U.

→ *Tuguu*

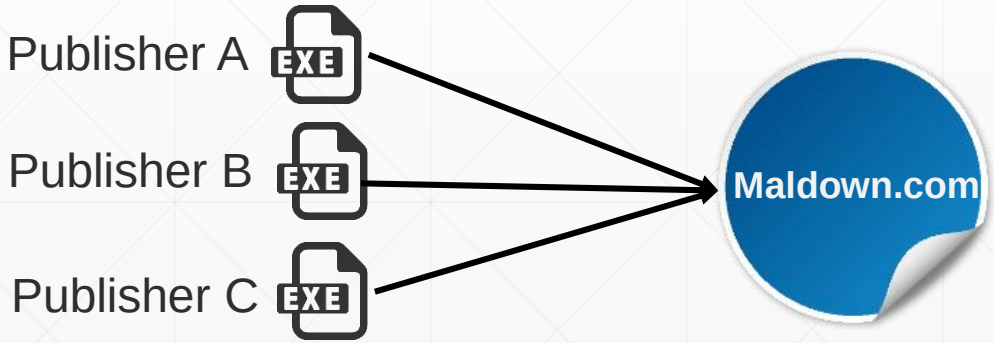
Child download domains



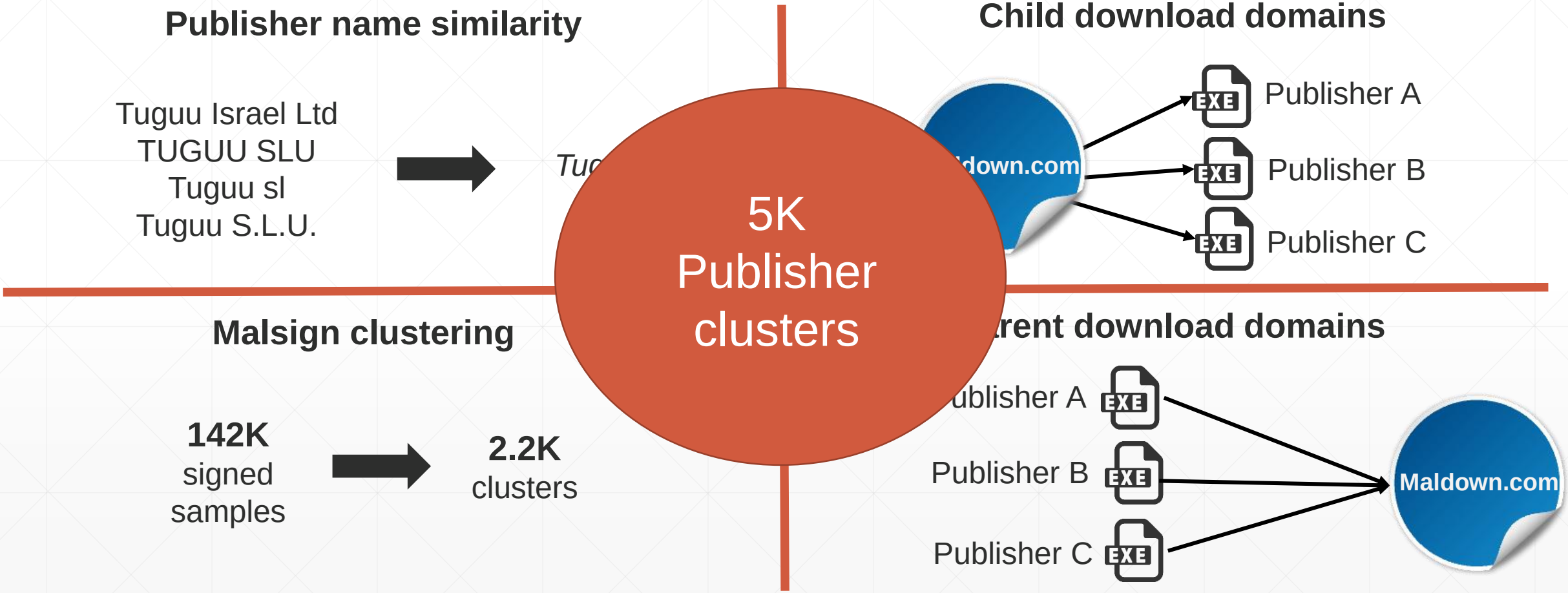
Malsign clustering

142K signed samples → **2.2K** clusters

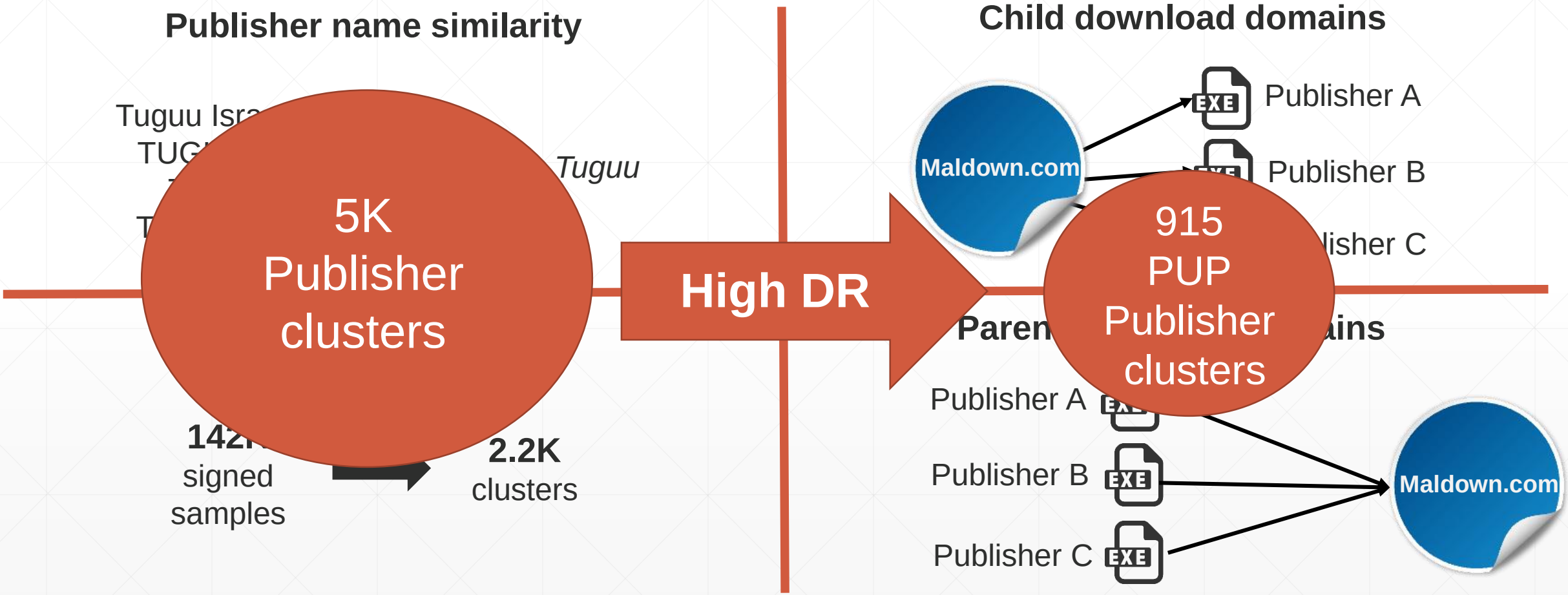
Parent download domains



Clustering Publishers

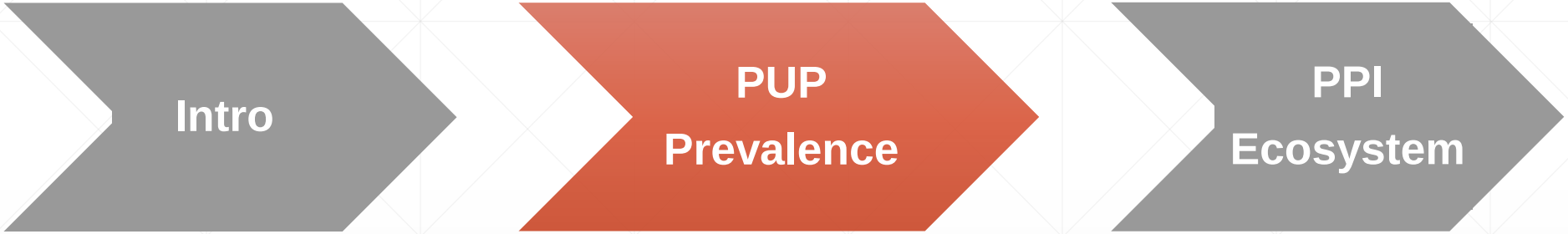


Clustering Publishers

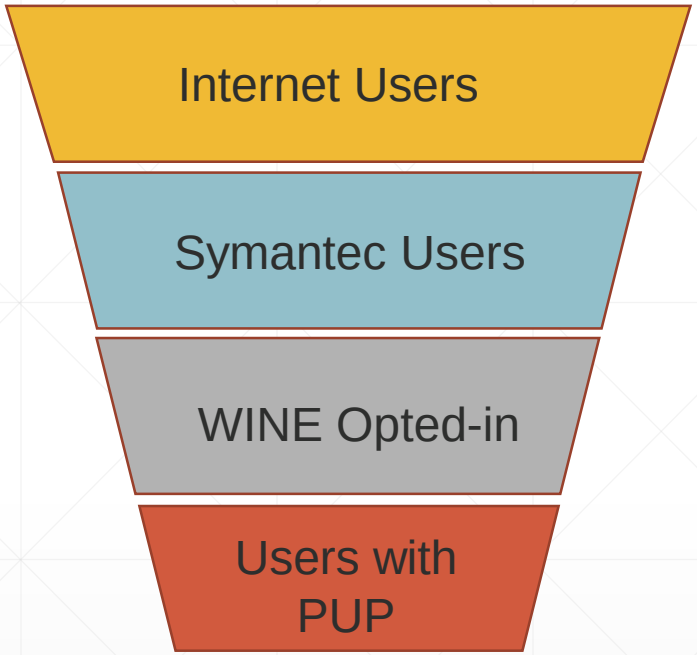


Publisher Detection Ratio (DR) = # EXEs flagged by AVs / All EXEs

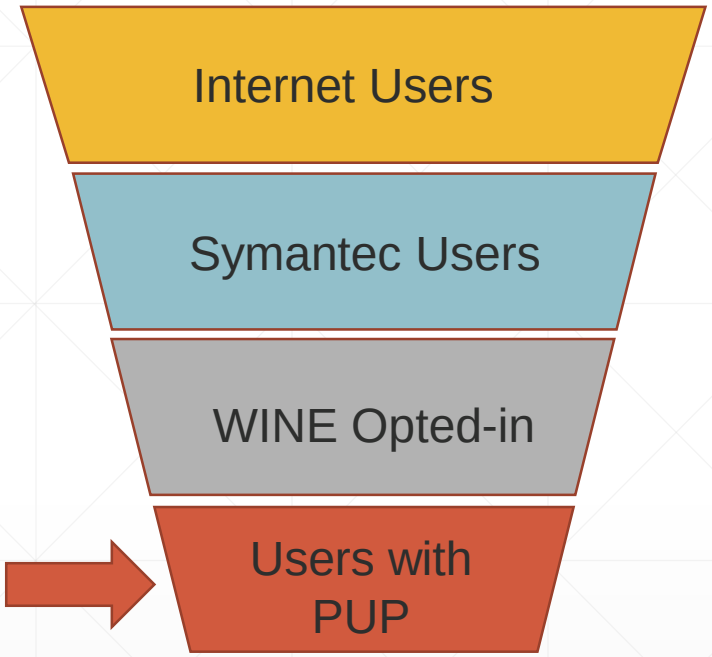
Road Map



PUP Prevalence



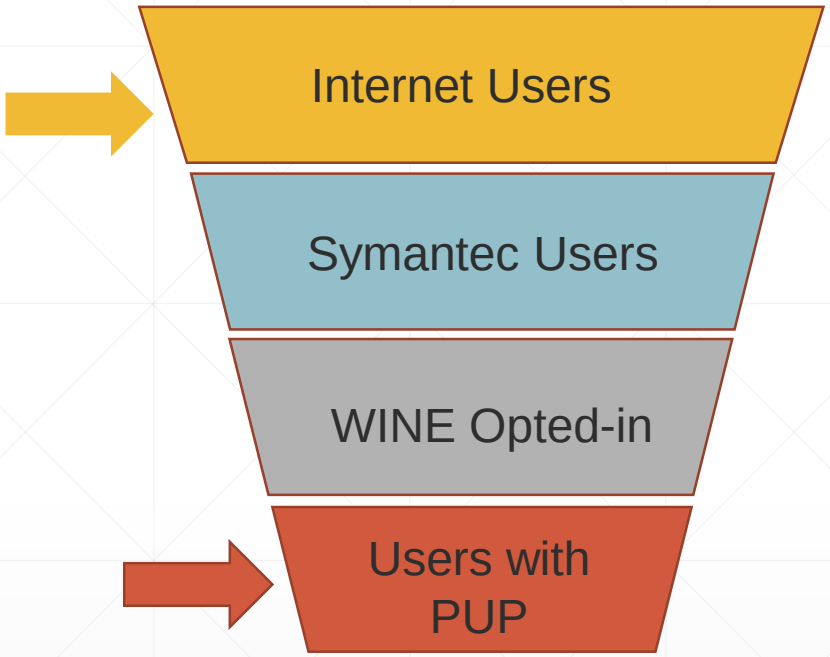
PUP Prevalence



54% (2.1M) of WINE hosts

have at least one PUP executable installed

PUP Prevalence



~210M Internet users affected

54% (2.1M) of WINE hosts

have at least one PUP executable installed

Publisher Ranking

#	Cluster	Hosts
1	Microsoft	3.9M
2	Symantec	3.8M
3	Adobe Systems	3.5M
4	Google	3.1M
5	Apple	1.8M
6	Intel	1.6M
7	Sun Microsystems	1.6M
8	Cyberlink	1.6M
9	GEAR Software	1.5M
10	Hewlett-Packard	1.5M

#	Cluster	Hosts
11	Oracle	1.4M
12	Skype Technologies	1.3M
13	Mozilla Corporation	1.0M
14	McAfee	1.0M
15	**Perion Network/Conduit**	**1.0M**

. . .

24	**Mindspark**	**533K**

Publisher Ranking

#	Cluster	Hosts
1	Microsoft	3.9M
2	Symantec	3.8M
3	Adobe Systems	3.5M
4	Google	3.1M
5	Apple	1.8M
6	Intel	1.6M
7	Sun Microsystems	1.6M
8	Cyberlink	1.6M
9	GEAR Software	1.5M
10	Hewlett-Packard	1.5M

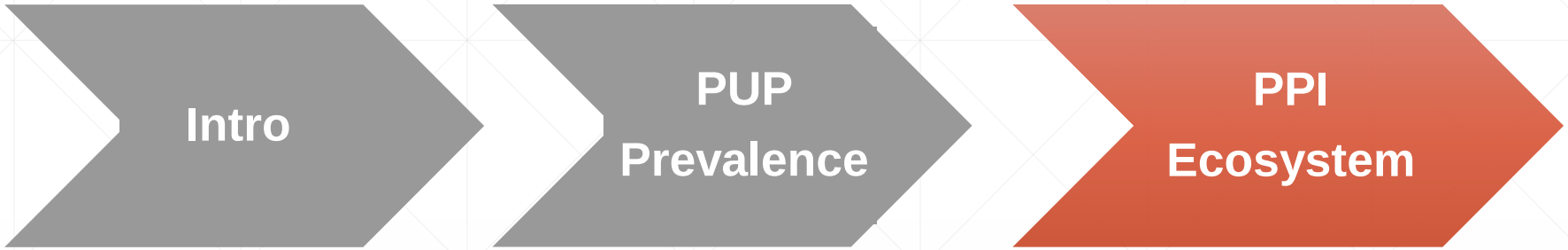
#	Cluster	Hosts
11	Oracle	1.4M
12	Skype Technologies	1.3M
13	Mozilla Corporation	1.0M
14	McAfee	1.0M
15	**Perion Network/Conduit**	**1.0M**

. . .

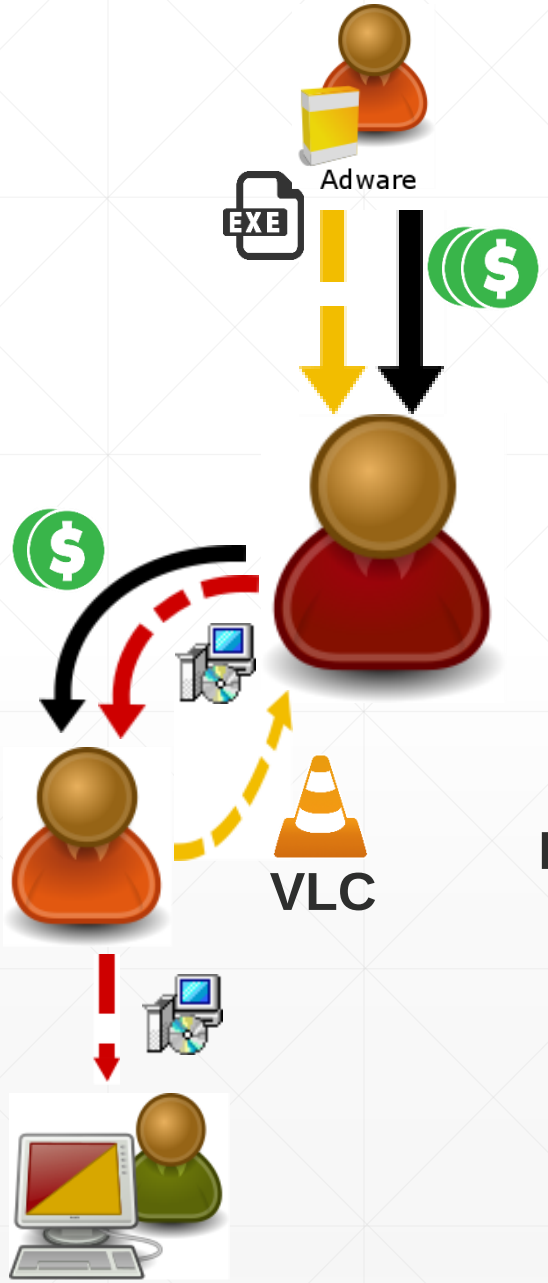
24	**Mindspark**	**533K**

PUP publishers are among the most widely installed software publishers

Road Map



PPI Ecosystem



Advertisers

PPI Service

Affiliate Publishers

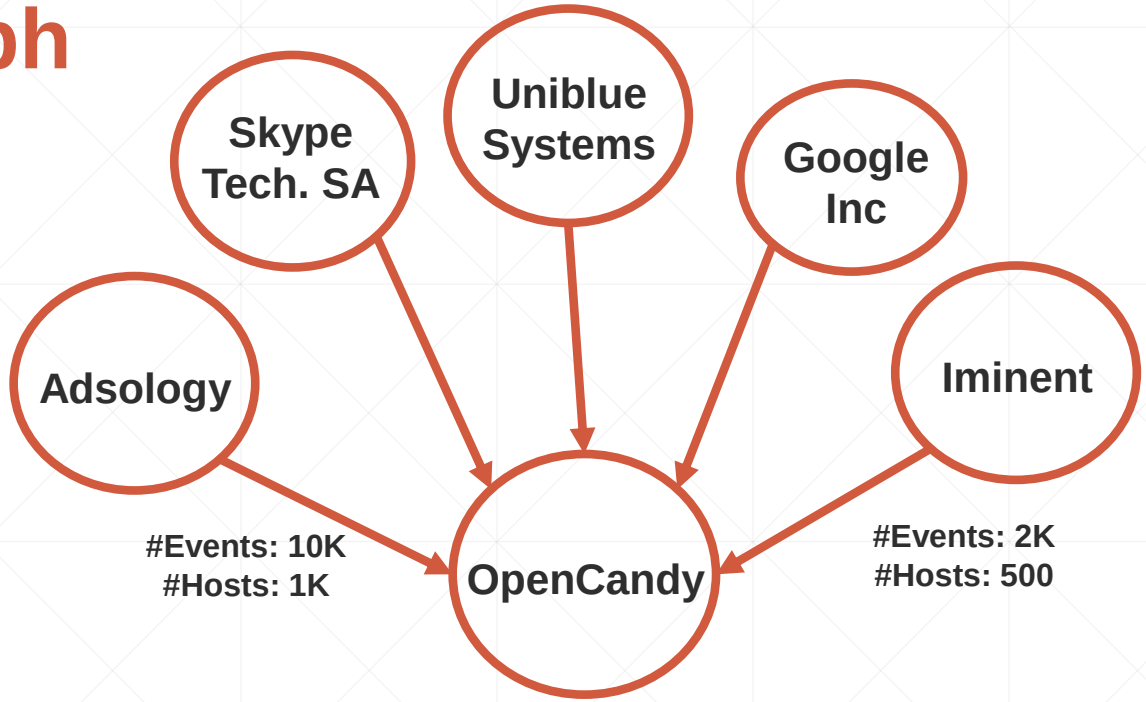
Target Hosts

- How many PPI services exist?
- What type of PUP is distributed?
- How is PUP distributed?
- PUP – Malware relationship?

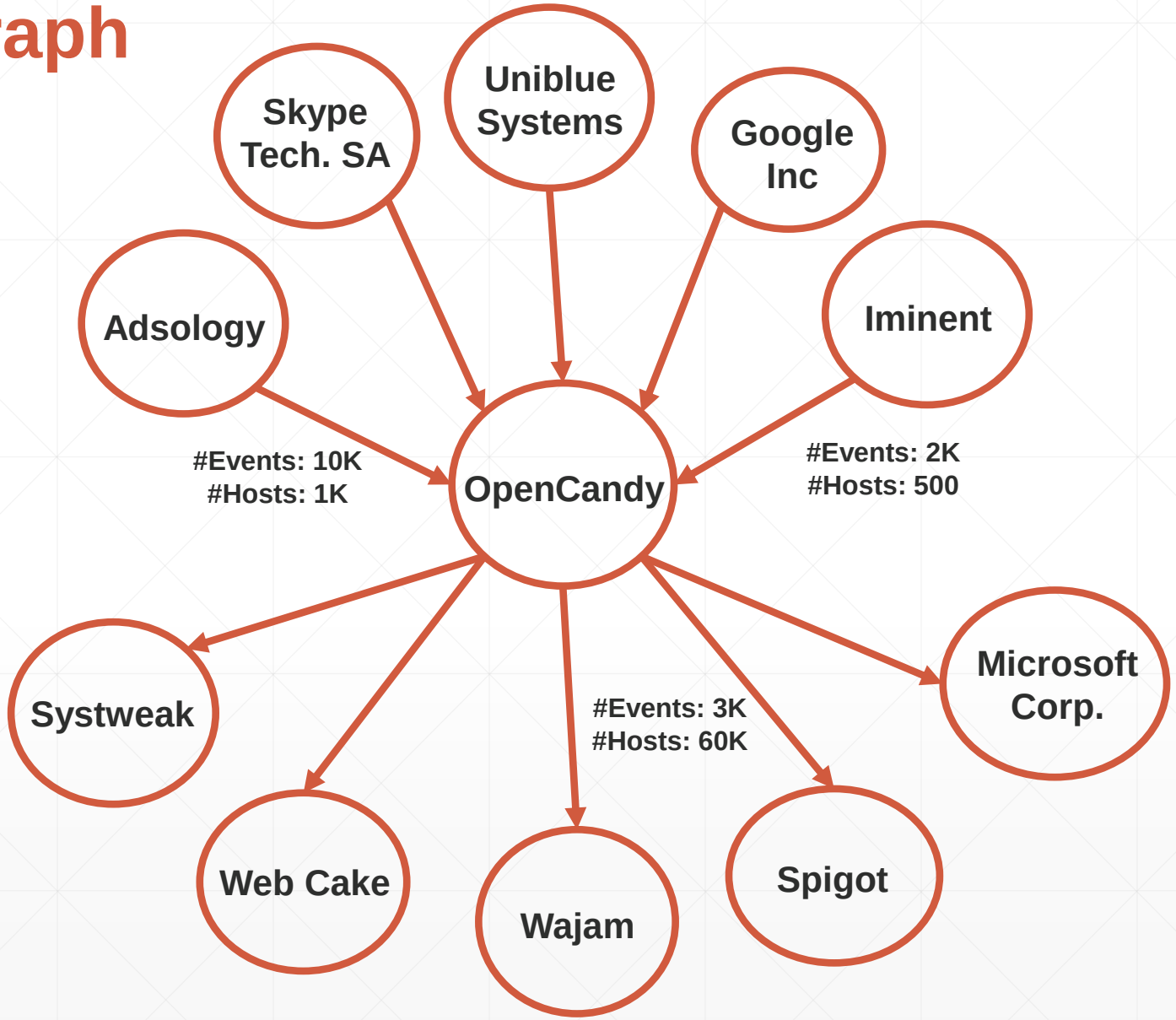
Publisher Graph



Publisher Graph

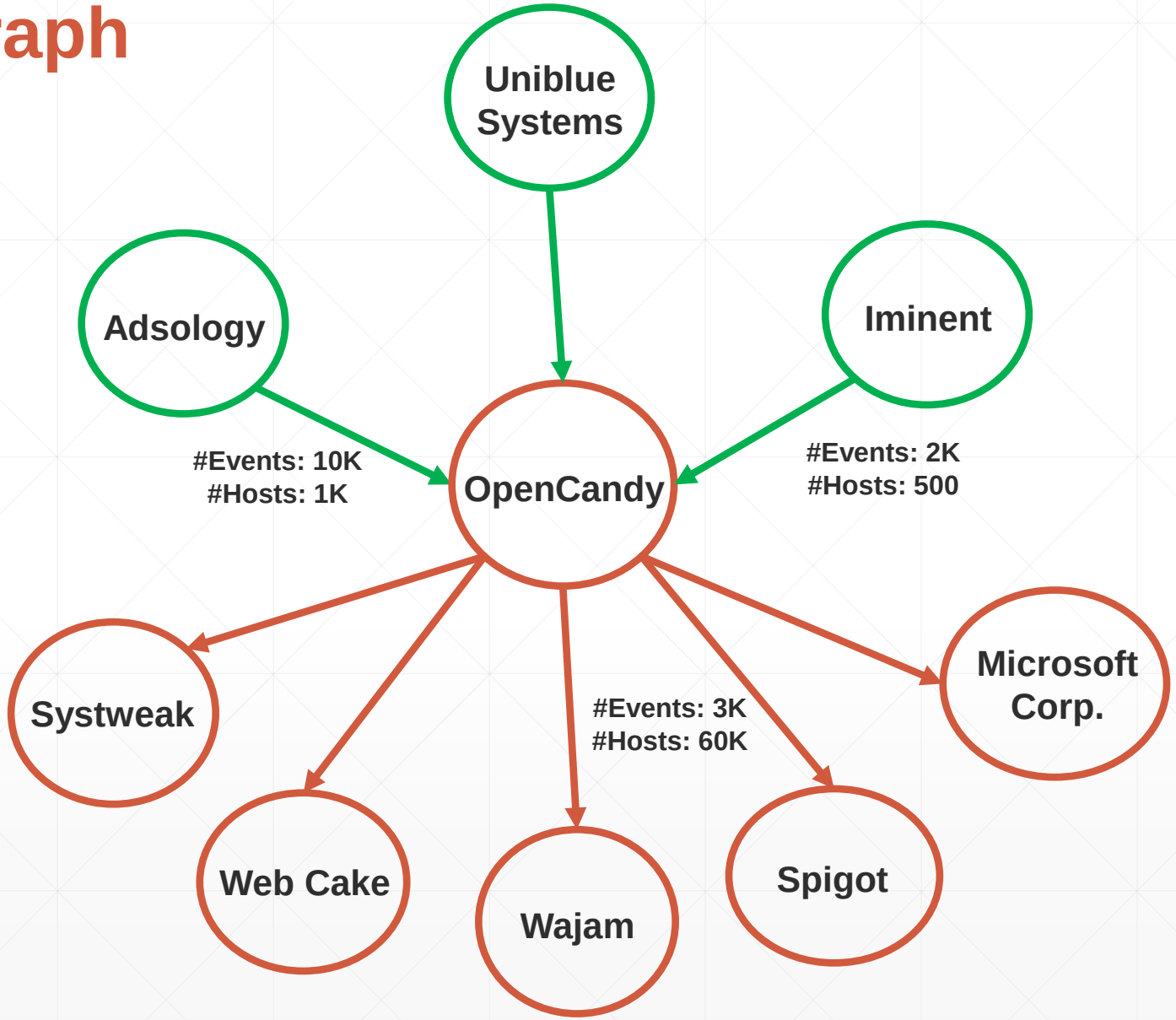


Publisher Graph



Publisher graph captures the who-installs-who relationships

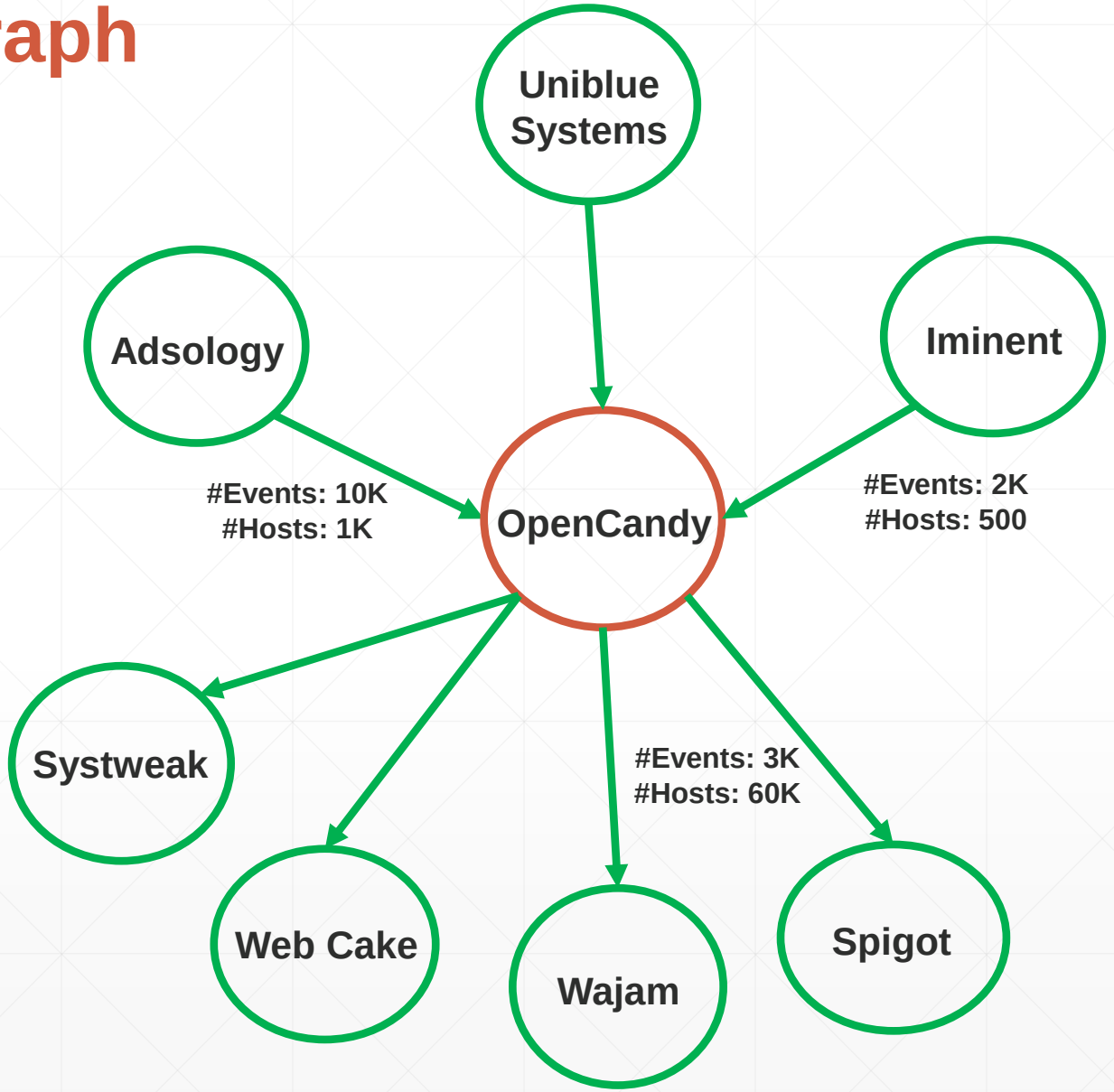
Publisher Graph



In-Degree (ID): 3

Publisher graph captures the who-installs-who relationships

Publisher Graph



In-Degree (ID): 3

Out-Degree (OD): 4

Publisher graph captures the who-installs-who relationships

How many PPI services exist?

High DR and **High ID** and **High OD**

How many PPI services exist?

High DR and **High ID** and **High OD**



How many PPI services exist?

High DR and **High ID** and **High OD**



PPI cluster	DR	ID	OD	Hosts
Perion Network/Conduit	52%	168	63	1M
Web Pick	79%	65	22	346K
iBario	84%	62	36	336K
IronSource	81%	73	112	332K
OpenCandy	55%	91	36	311K

How many PPI services exist?

High DR and **High ID** and **High OD**



PPI cluster	DR	ID	OD	Hosts
Perion Network/Conduit	52%	168	63	1M
Web Pick	79%	65	22	346K
iBario	84%	62	36	336K
IronSource	81%	73	112	332K
OpenCandy	55%	91	36	311K

❑ 3/Top 5 most popular PUP publishers are PPI services

How many PPI services exist?

High DR and **High ID** and **High OD**



PPI cluster	DR	ID	OD	Hosts
Perion Network/Conduit	52%	168	63	1M
Web Pick	79%	65	22	346K
iBario	84%	62	36	336K
IronSource	81%	73	112	332K
OpenCandy	55%	91	36	311K

- 3/Top 5 most popular PUP publishers are PPI services
- 12 other PPIs not seen:
  - Not popular or gain popularity later
  - Distribute unsigned bundles
  - Resellers

What type of PUP is distributed?

High DR and **High ID** and **Low OD** and **Parent PPI > 0**

What type of PUP is distributed?

High DR and **High ID** and **Low OD** and **Parent PPI > 0**

77
Advertisers

What type of PUP is distributed?

High DR and **High ID** and **Low OD** and **Parent PPI > 0**

77
Advertisers

18/30
Add-ons



Delta Search

iminent

Modify default search engine

PRICEGONG
we compare, you save

Supreme Savings

Inject shopping deals & price comparisons

What type of PUP is distributed?

High DR and **High ID** and **Low OD** and **Parent PPI > 0**

77
Advertisers

18/30
Add-ons



Delta Search

iminent

Modify default search engine

PRICEGONG
we compare, you save

Supreme Savings

Inject shopping deals & price comparisons

6/30
Rogueware



Uniblue SpeedUpMyPC

Systweak Regclean Pro

Performance Optimizers

What type of PUP is distributed?

High DR and **High ID** and **Low OD** and **Parent PPI > 0**

77
Advertisers

18/30
Add-ons



Delta Search

iminent

Modify default search engine

PRICEGONG
we compare, you save

Supreme Savings

Inject shopping deals & price comparisons

6/30
Rogueware

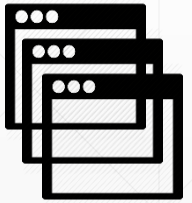


Uniblue SpeedUpMyPC

Systweak Regclean Pro

Performance Optimizers

6/30
Other



myPCBackup.com

Backup tools

Gom Player

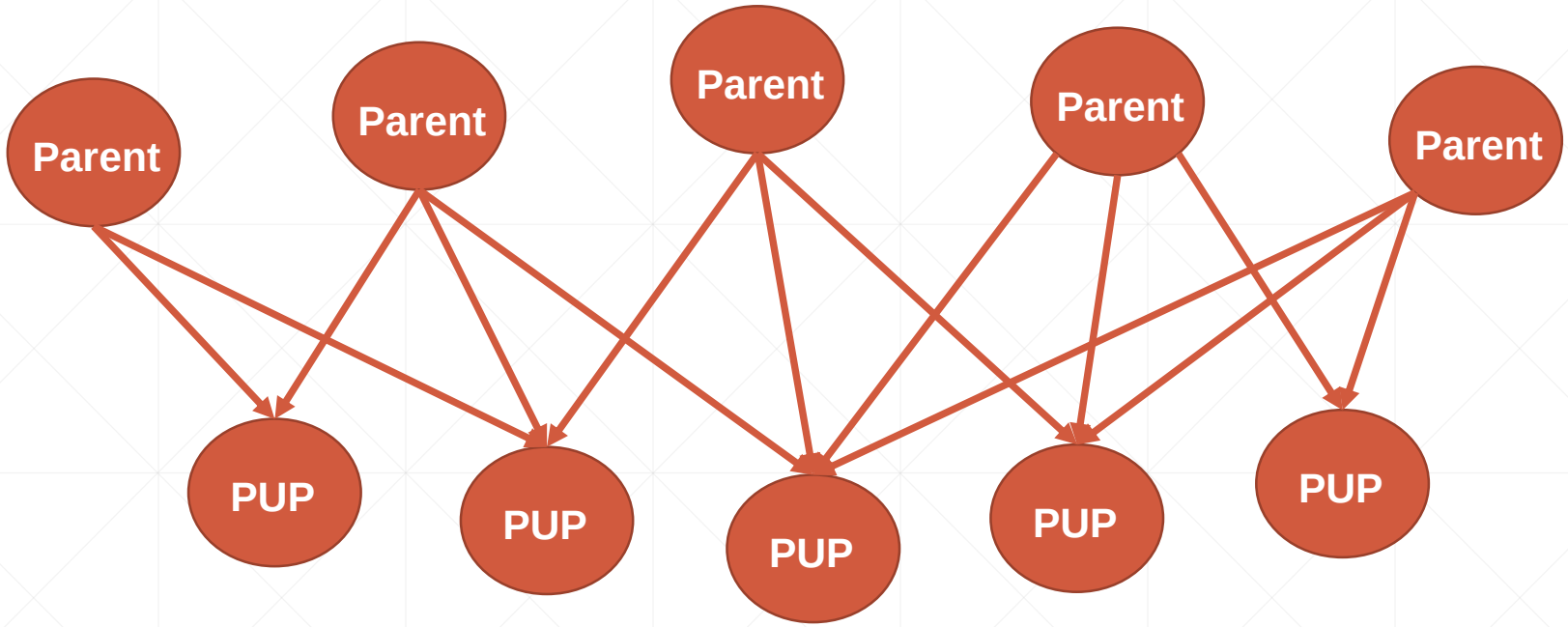
FS

Multimedia players

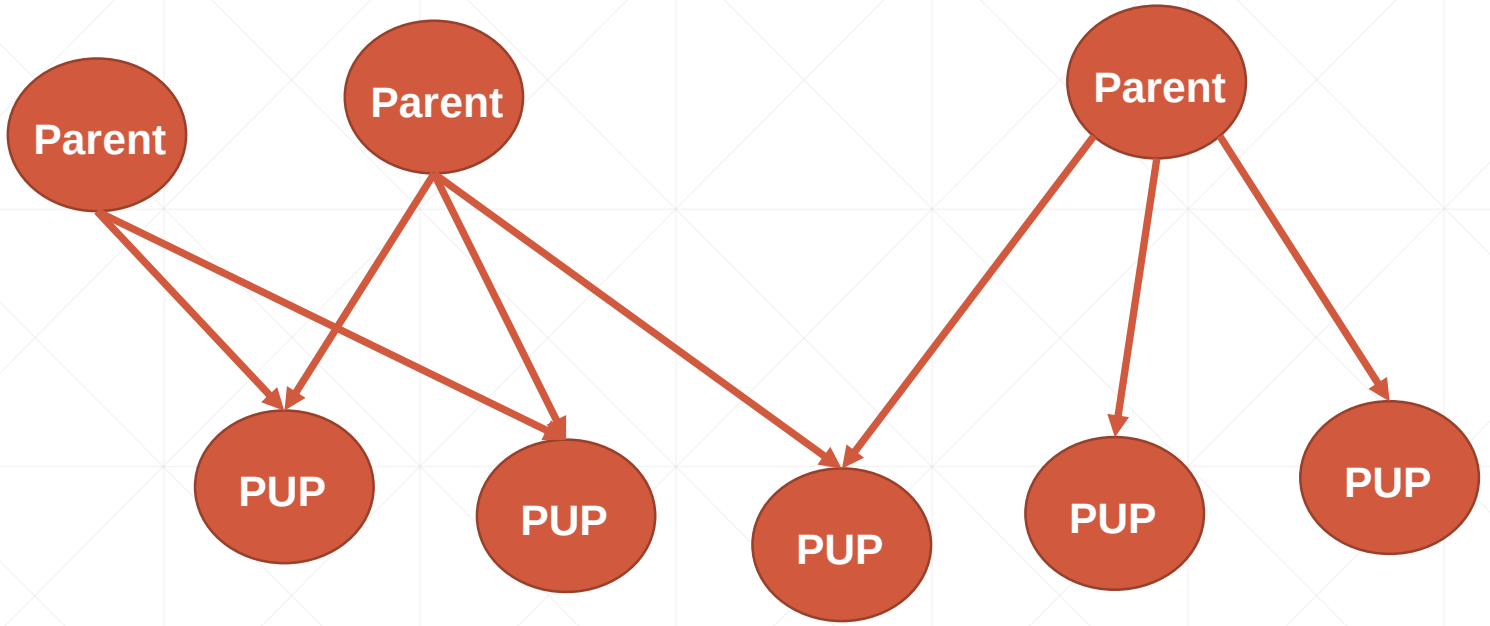
How is PUP distributed?



How is PUP distributed?

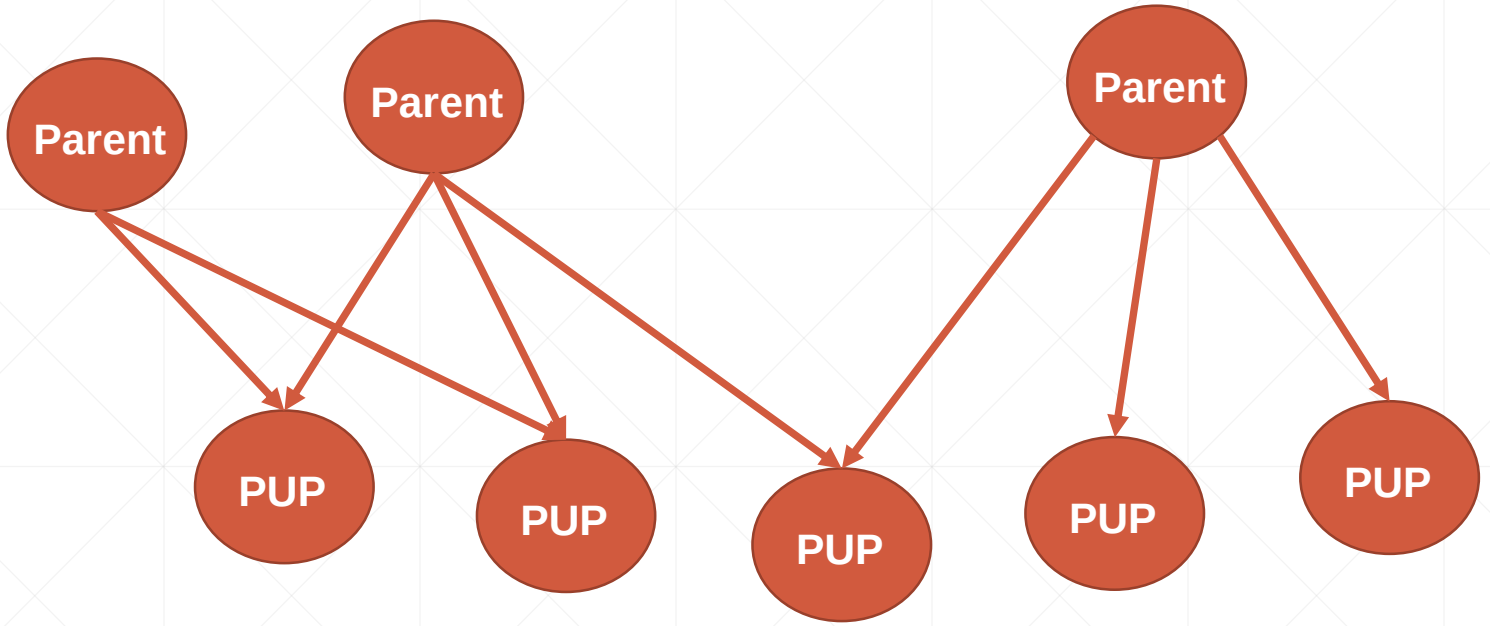


How is PUP distributed?



71%
signed parents

How is PUP distributed?



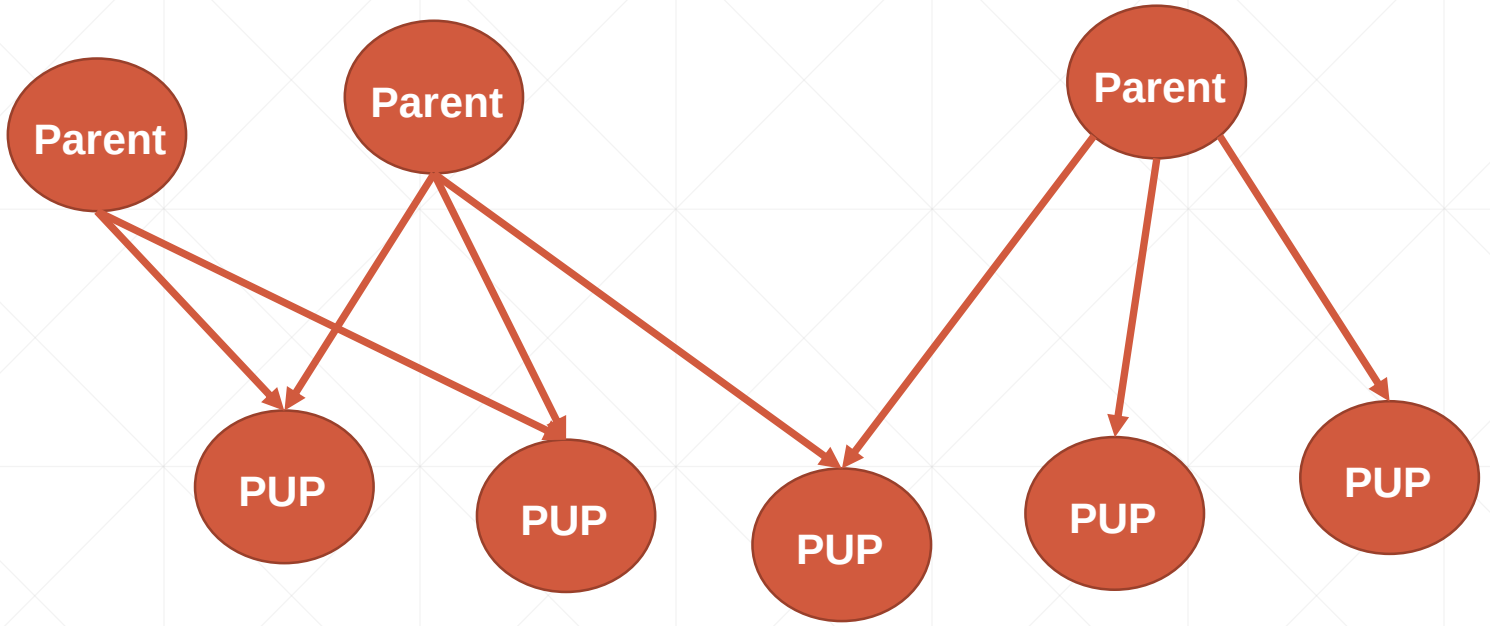
71%
signed parents

74% are

PUP parents

PUPs are generally installed by other PUPs

How is PUP distributed?



71%
signed parents

74% are

PUP parents

PUPs are generally installed by other PUPs

26% are

PPI services

PPI services play an important role in the distribution of PUP

PUP - Malware Relationship

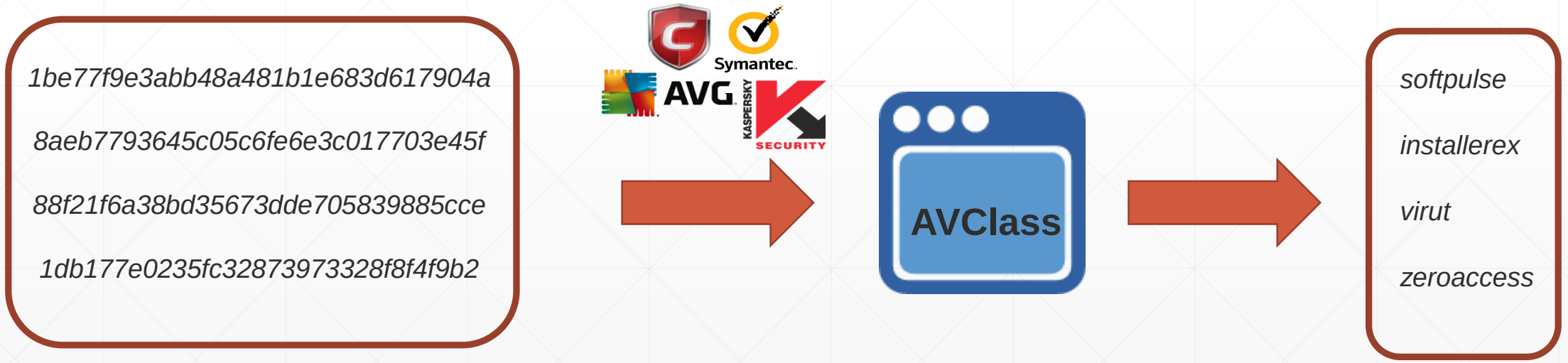
- **Challenge**: Accurately label malware in WINE dataset

PUP - Malware Relationship

- **Challenge**: Accurately label malware in WINE dataset

- **AVClass** malware labeling tool *[Sebastián et al. RAID ´16]*:

github.com/malicialab/avclass

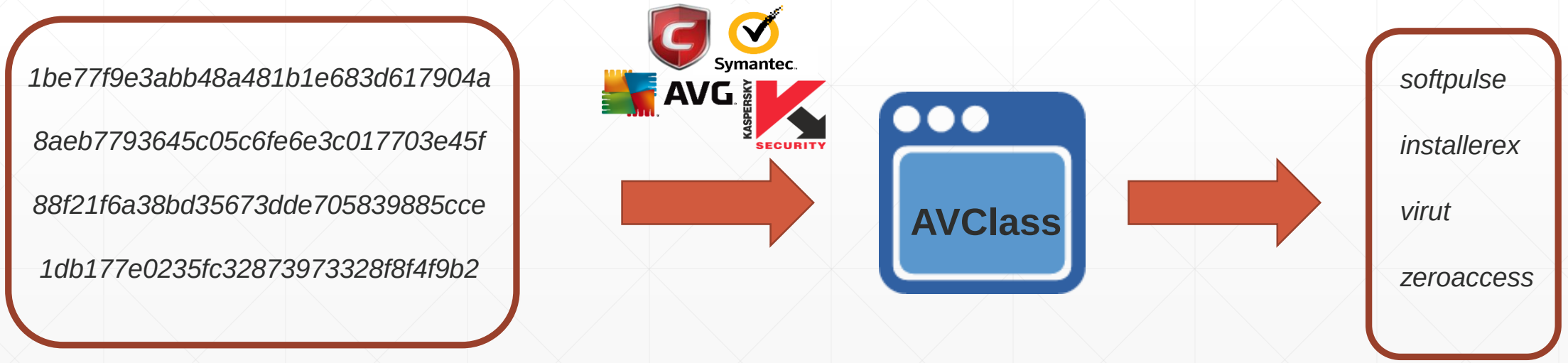


PUP - Malware Relationship

- **Challenge**: Accurately label malware in WINE dataset

- **AVClass** malware labeling tool *[Sebastián et al. RAID ´16]*:

github.com/malicialab/avclass



- Selected 70 popular malware families (e.g., zbot, zeroaccess, reveton, virut, sality)

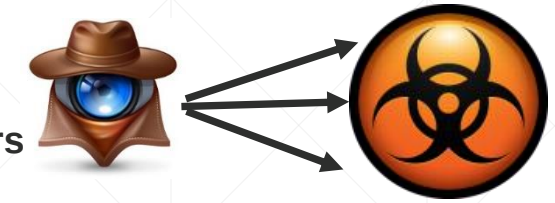
PUP - Malware Relationship



PUP - Malware Relationship

Does PUP download malware?

71
PUP Publishers



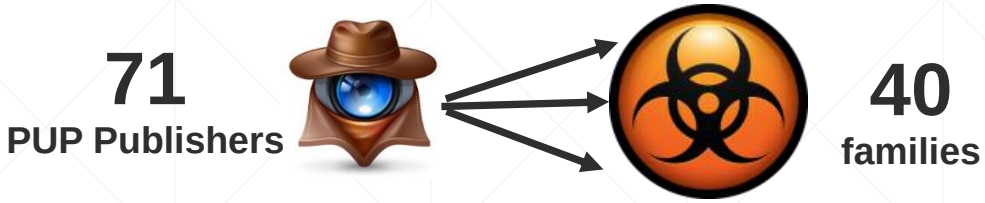
40
families

5.6K (0.01%)
download events

- Examples:
  - Perion Network dropping Zbot, Shylock trojans
  - InstallBrain downloading Mevade/Sefnit as reported by TrendMicro

PUP - Malware Relationship

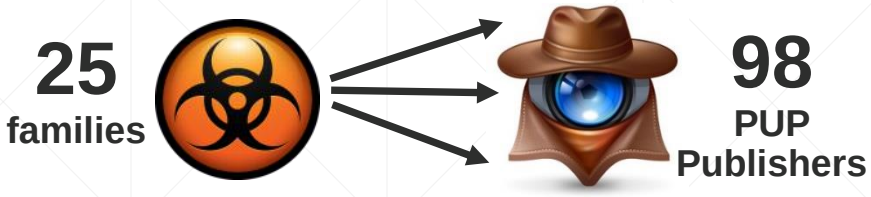
Does PUP download malware?



5.6K (0.01%)
download events

- Examples:
  - Perion Network dropping Zbot, Shylock trojans
  - InstallBrain downloading Mevade/Sefnit as reported by TrendMicro

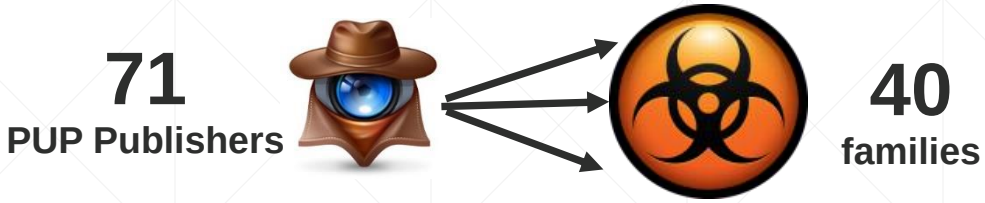
Does malware download PUP?



11K (0.03%)
download events

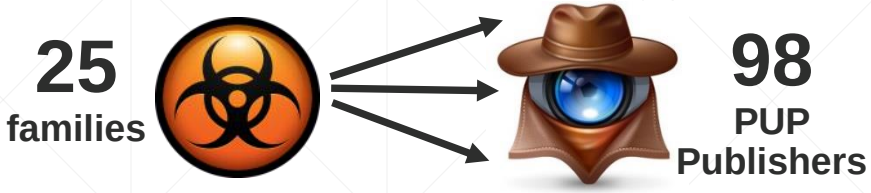
PUP - Malware Relationship

Does PUP download malware?



5.6K (0.01%)
download events

Does malware download PUP?



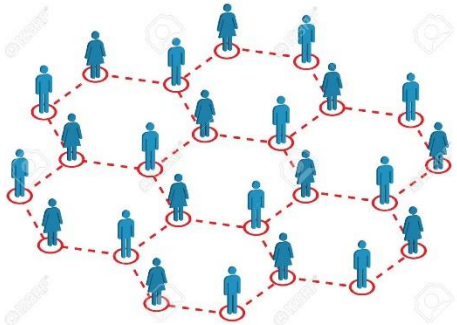
11K (0.03%)
download events

- Examples:
  - Perion Network dropping Zbot, Shylock trojans
  - InstallBrain downloading Mevade/Sefnit as reported by TrendMicro

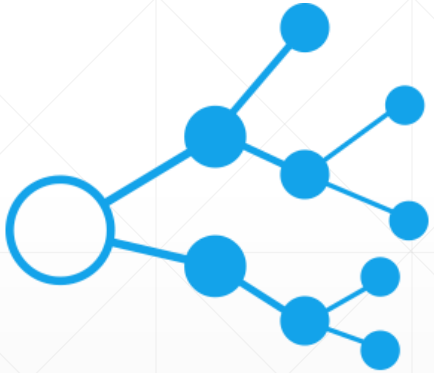
Malware distribution seems disjoint from PUP distribution

Summary

- **54%** of **3.9M** real hosts examined have PUP installed



- Birds-eye view of the PPI ecosystem
  - **24** PPI services that distribute **26%** of all signed PUP
  - **77** advertiser clusters (mostly BAO) that monetize in various ways



- Malware distribution seems disjoint from PUP distribution





Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services

Platon Kotzias, Leyla Bilge, Juan Caballero



