No Signal Left to Chance: Driving Browser Extension Analysis by Download Patterns

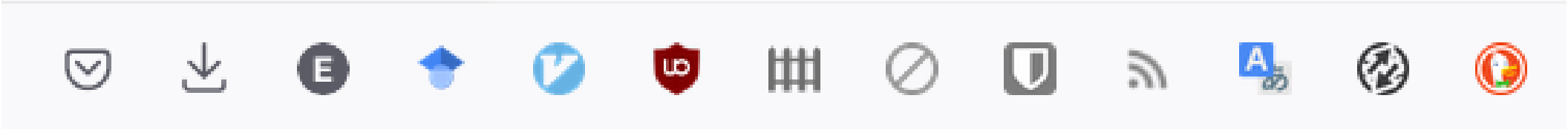
Pablo Picazo-Sanchez
pablop@chalmers.se

Benjamin Eriksson
beneri@chalmers.se

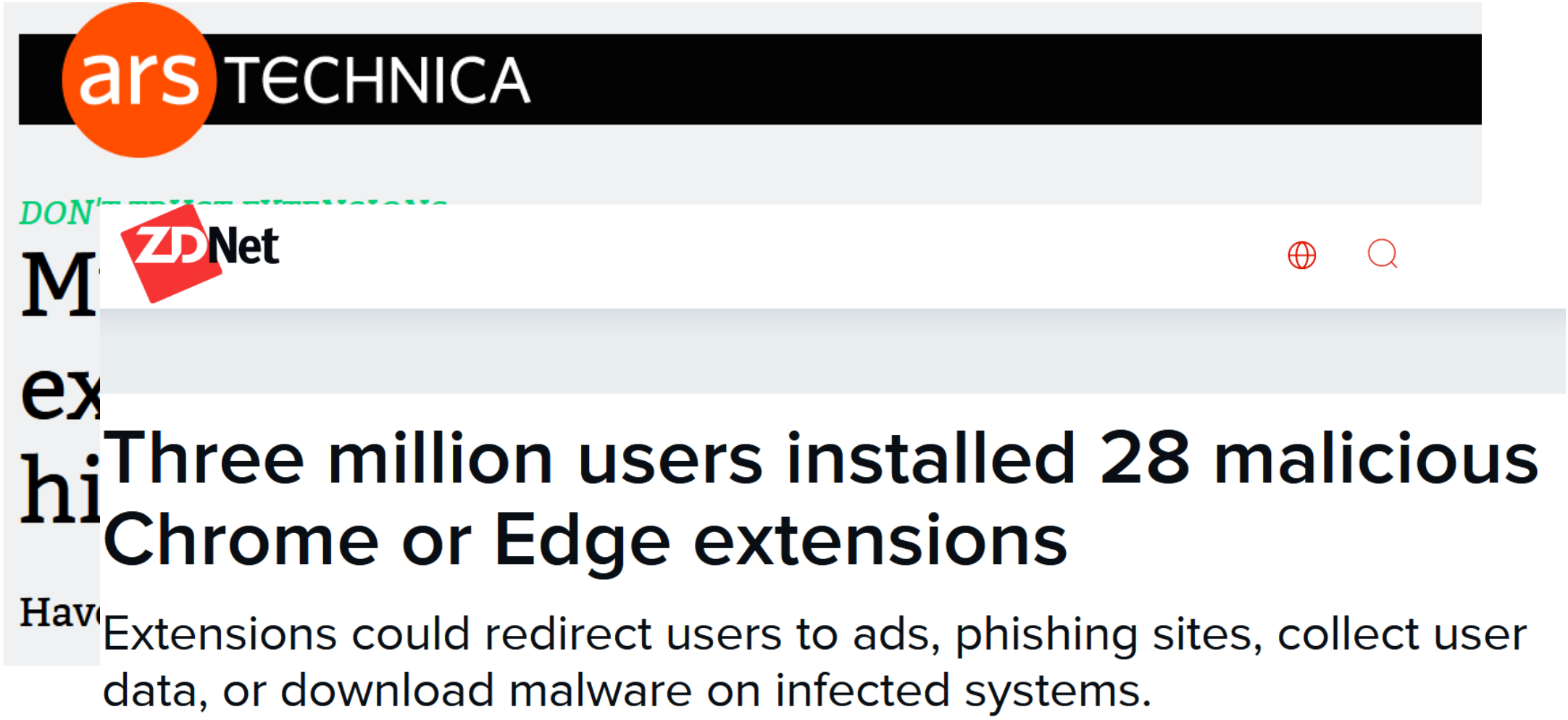
Andrei Sabelfeld
andrei@chalmers.se

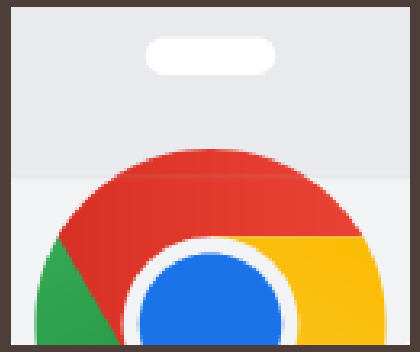
Browser Extensions

- Small JavaScript programs that run in the browser
- Can interact with web pages
- Popular categories:
  - Ad Blockers
  - Password mangers
  - UX extensions



Problem – Malicious Extensions





Home > Extensions > Google Translate

Google Translate

translate.google.com Featured

44,052 | Productivity | 10,000,000+ users

By Google

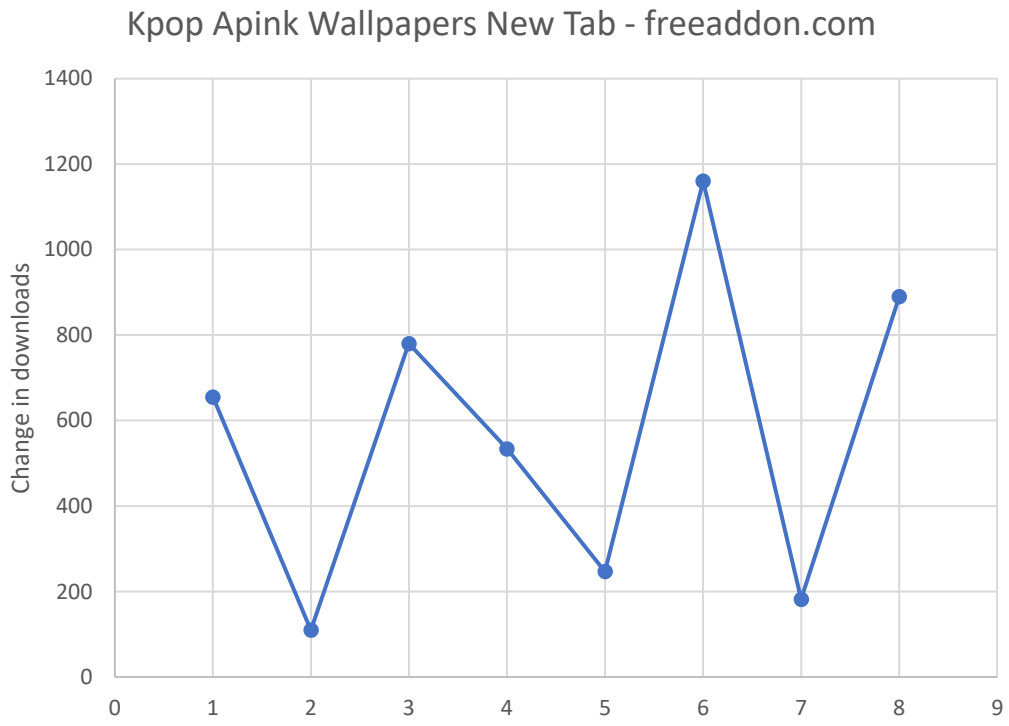
Home > Extensions > Cute Dogs & Puppies Wallpaper New Tab

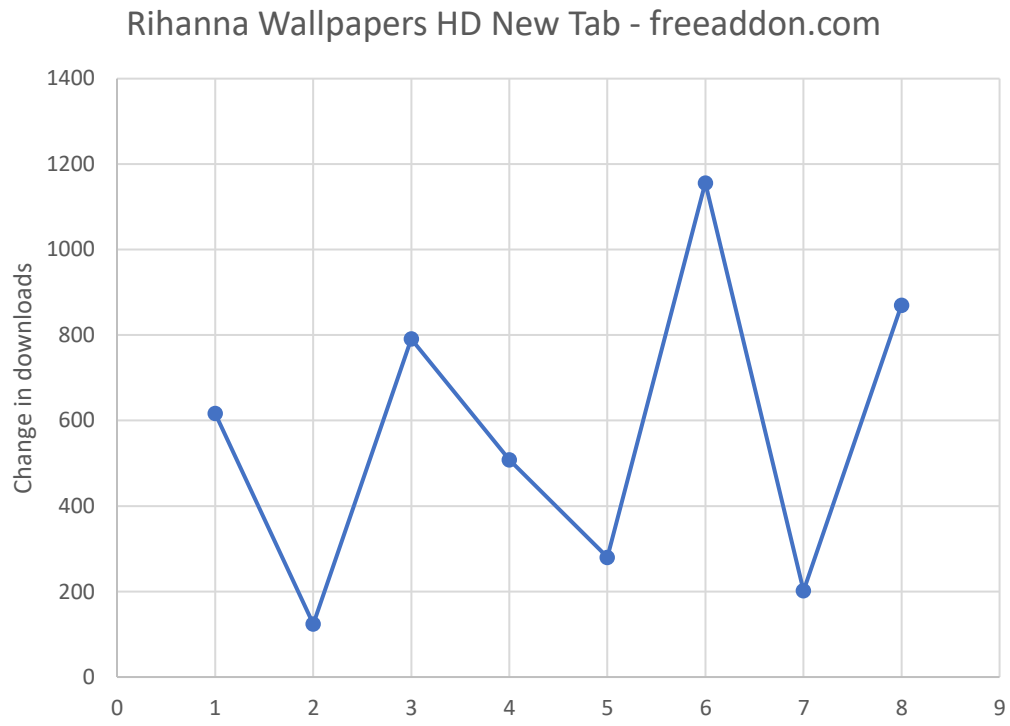
Cute Dogs & Puppies Wallpaper New Tab

coolthemestores.com

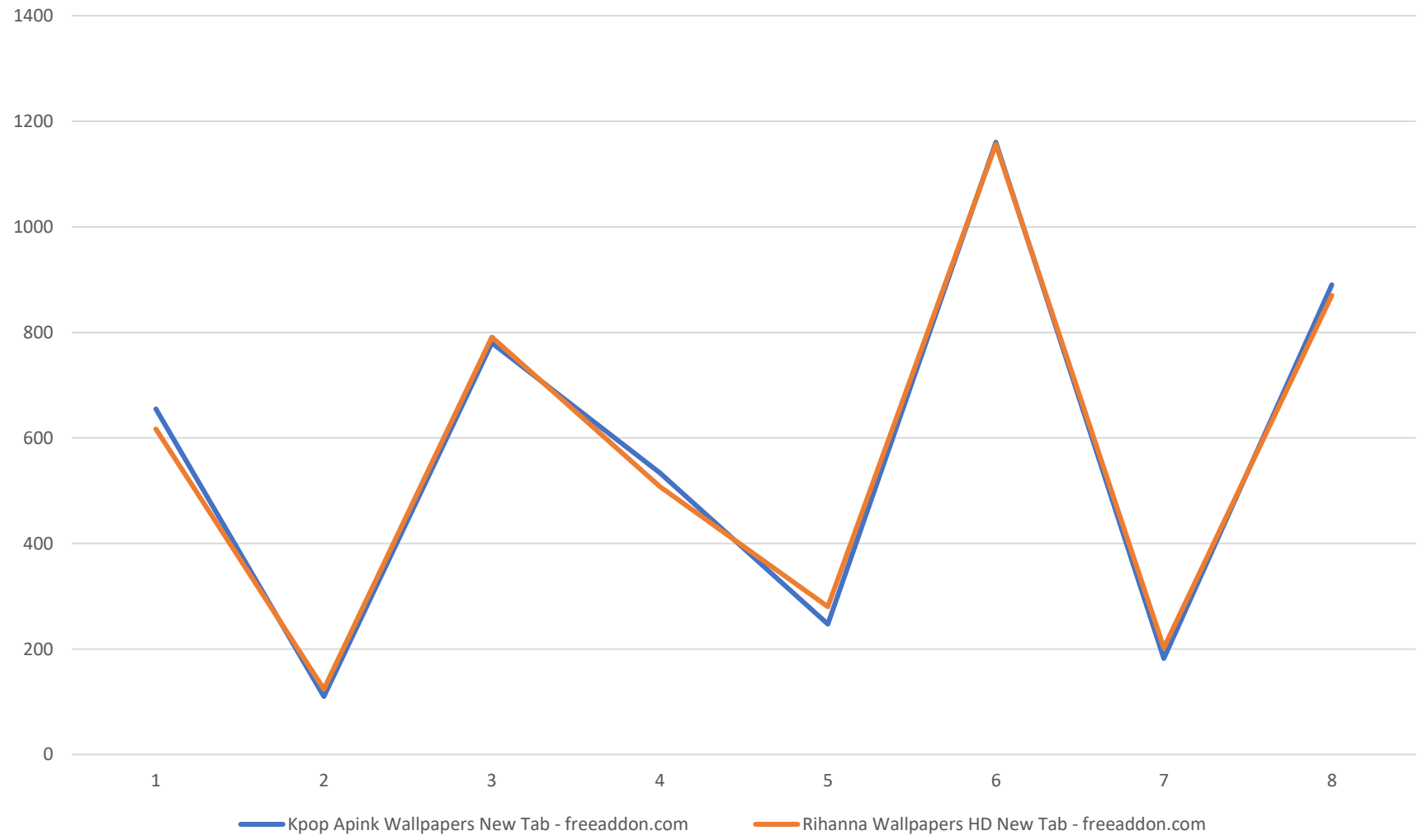
5 | Fun | 1,594 users

Download patterns





Download patterns



Research Questions

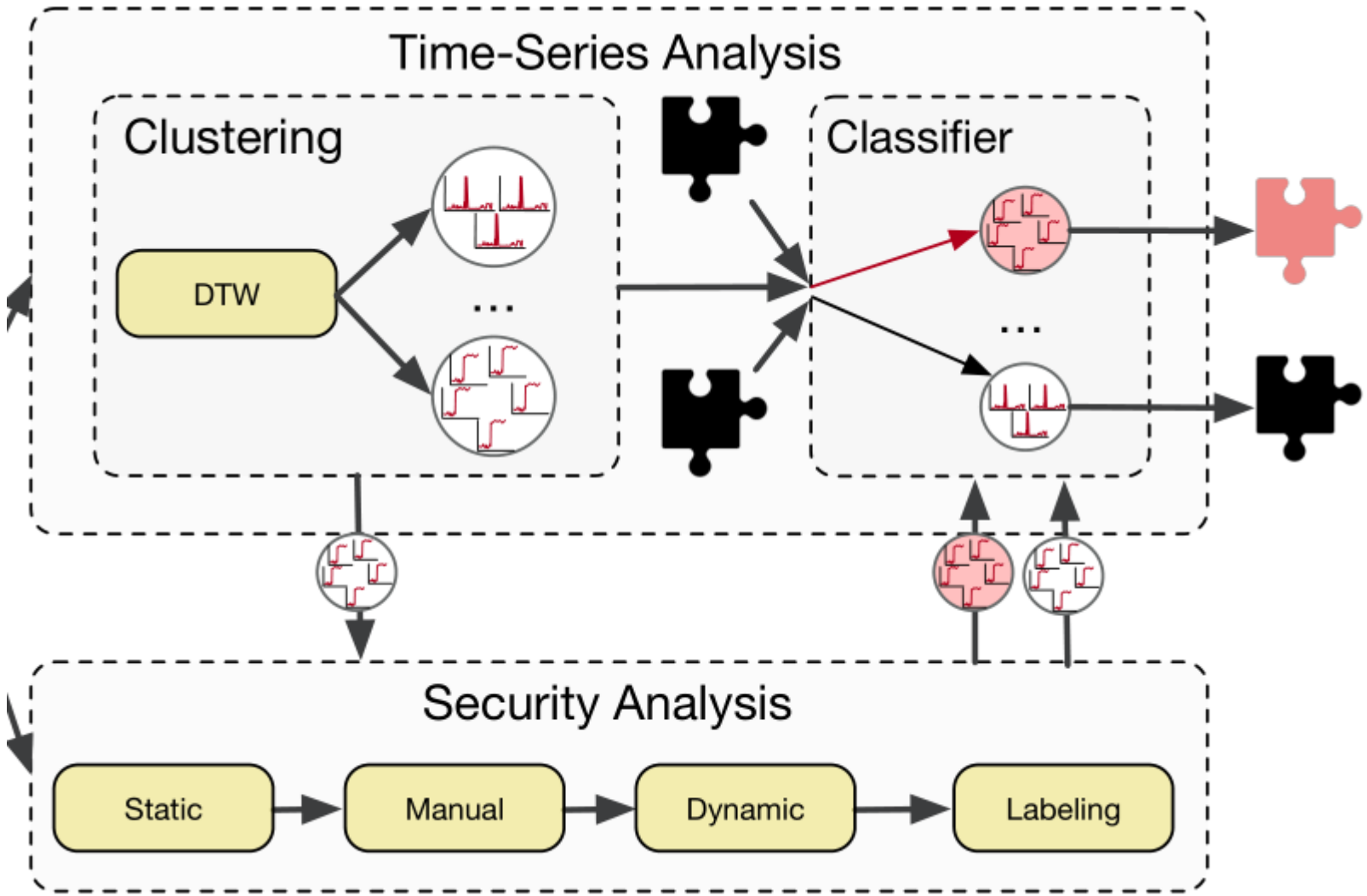
RQ1: Are there extensions that follow similar download patterns?

RQ2: Is there any relationship between download patterns and malicious code?

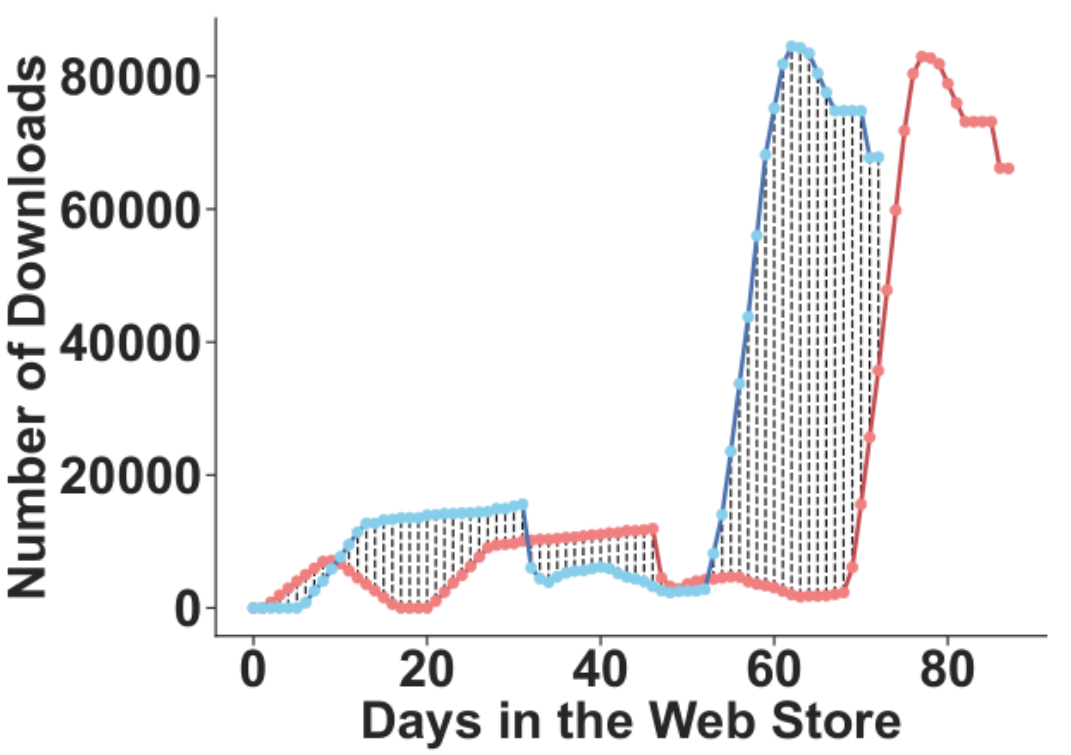
RQ3: Can we find malicious extensions based on their download patterns?

Gathering Data

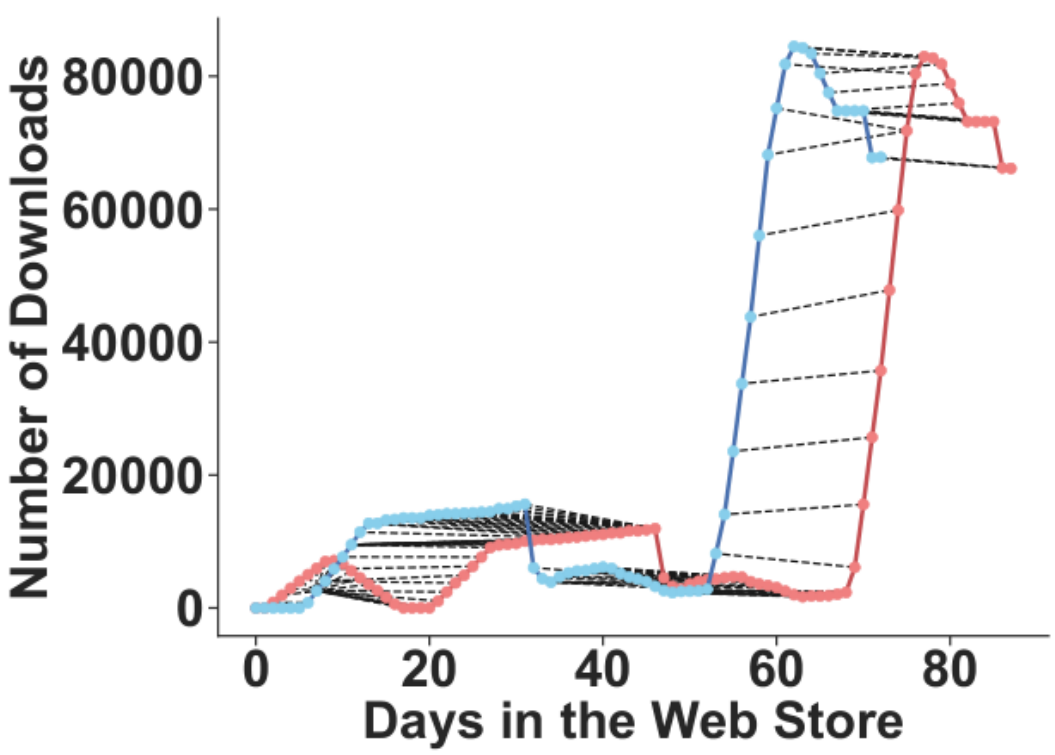
- Crawl Chrome Web Store everyday for six months
- Calculate average change per extension $\overline{\Delta_{d_e}} = \frac{\sum_{i=1}^{n} \Delta_{d_e}}{n}$
- Calculate global average change $\bar{\bar{\Delta}} = \frac{\sum_{i=1}^{e} \Delta_{d_i}}{n}$
- Only keep “interesting” extensions $\overline{\Delta_{d_e}} \geq \bar{\bar{\Delta}}$


Time-Series Analysis
Clustering
DTW
...
Classifier
...
Security Analysis
Static
Manual
Dynamic
Labeling

Similar patterns?

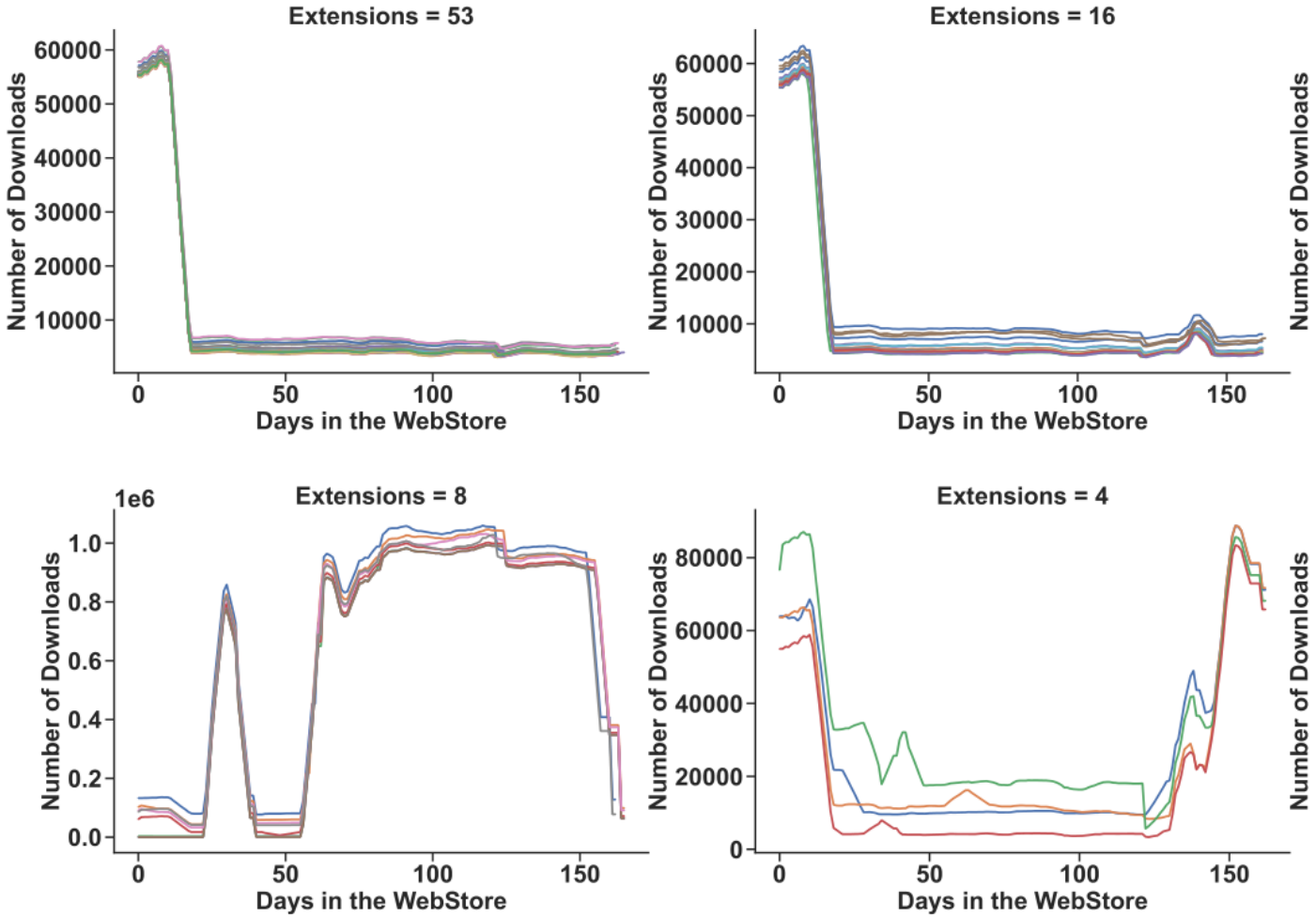


Euclidean distance

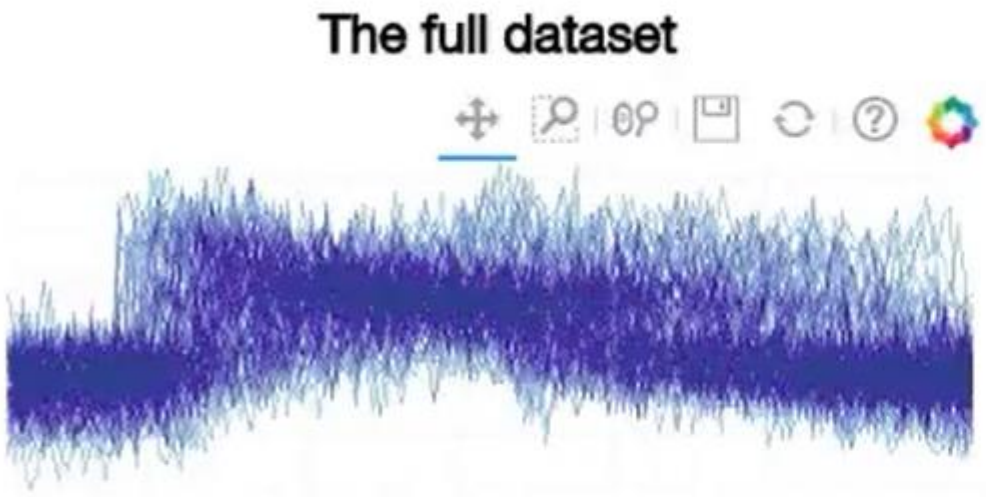


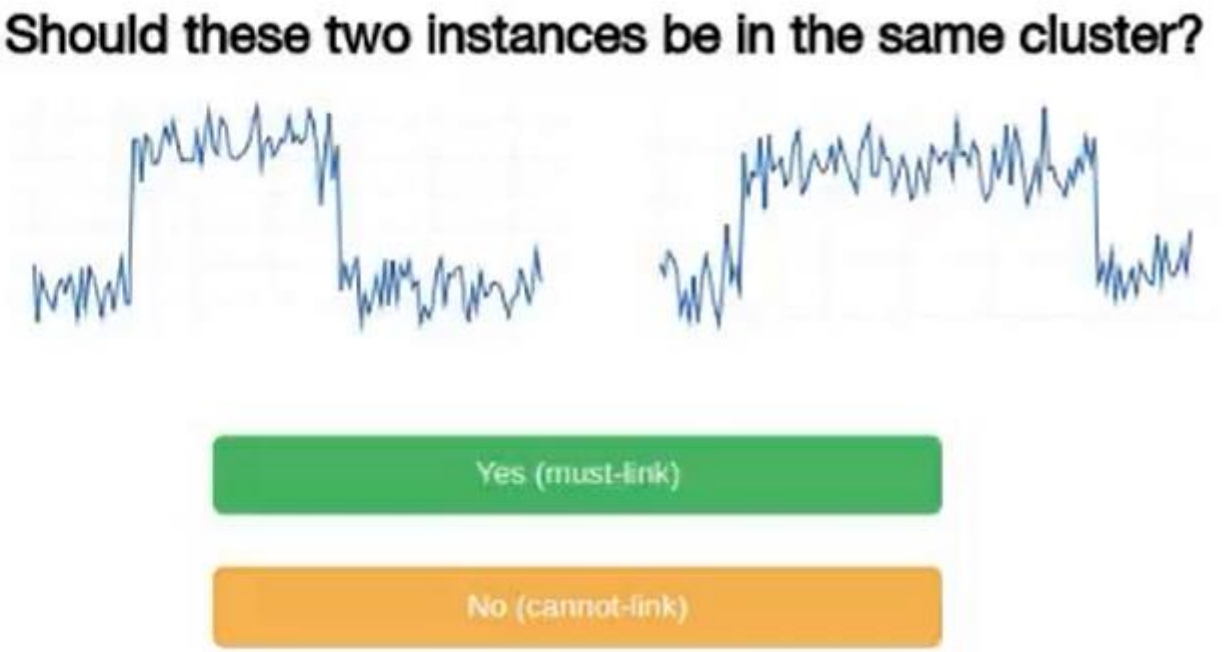
DTW distance

Clustering

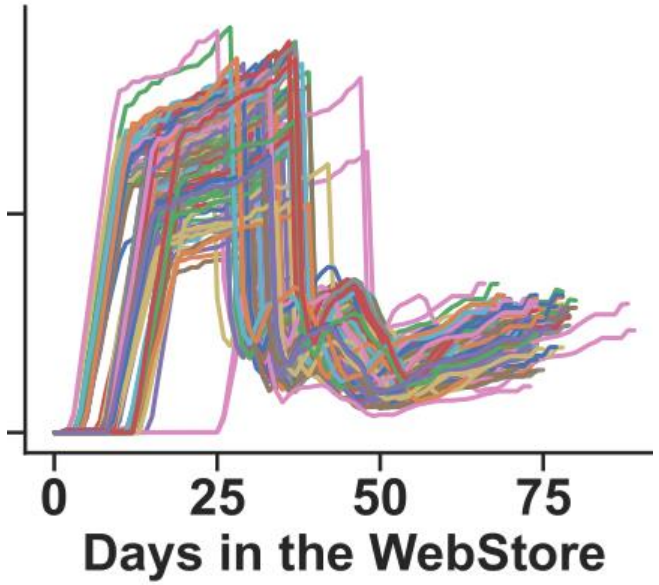

Extensions = 53
Number of Downloads
60000
50000
40000
30000
20000
10000
0
50
100
150
Days in the WebStore
Extensions = 16
Number of Downloads
60000
50000
40000
30000
20000
10000
0
50
100
150
Days in the WebStore
Number of Downloads
1e6
Extensions = 8
Number of Downloads
1.0
0.8
0.6
0.4
0.2
0.0
0
50
100
150
Days in the WebStore
Extensions = 4
Number of Downloads
80000
60000
40000
20000
0
0
50
100
150
Days in the WebStore
Number of Downloads

Clustering using COBRAS-TS





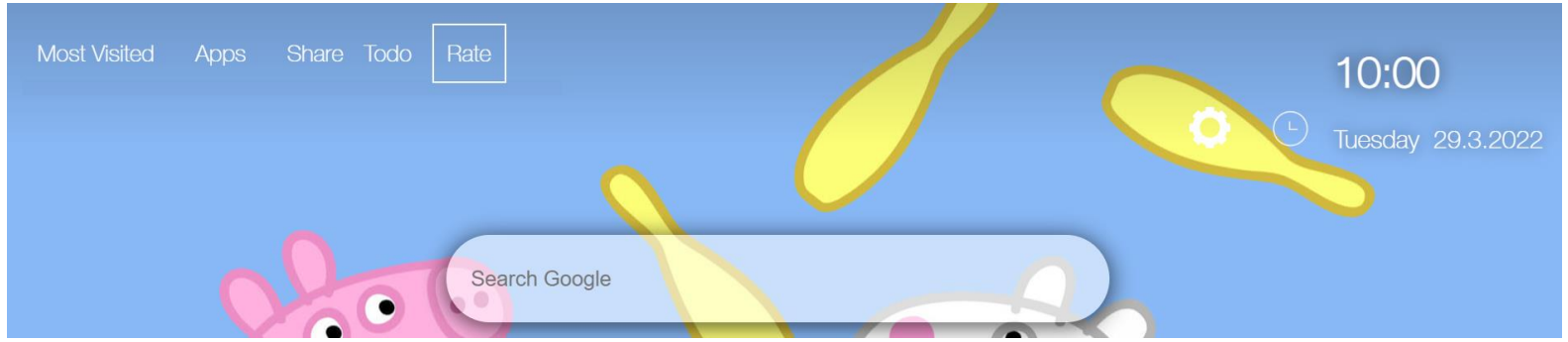
Clustering results

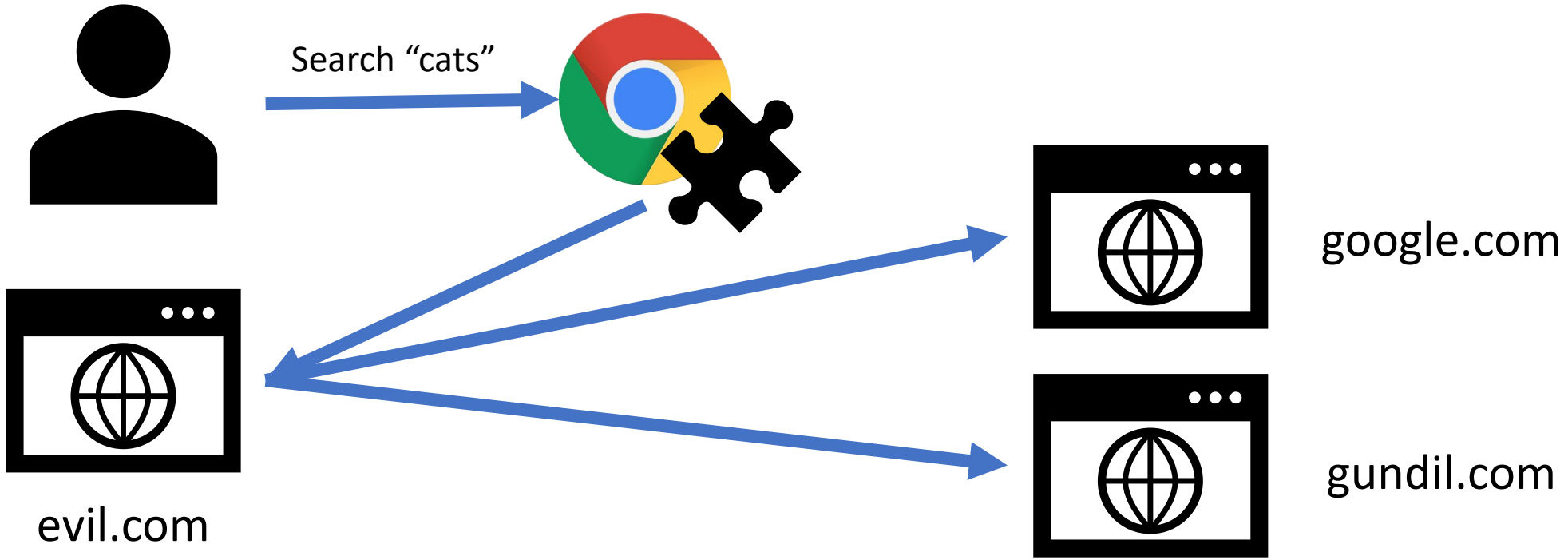


- 3,271 Extensions
- 135 Clusters
- 24 Per cluster

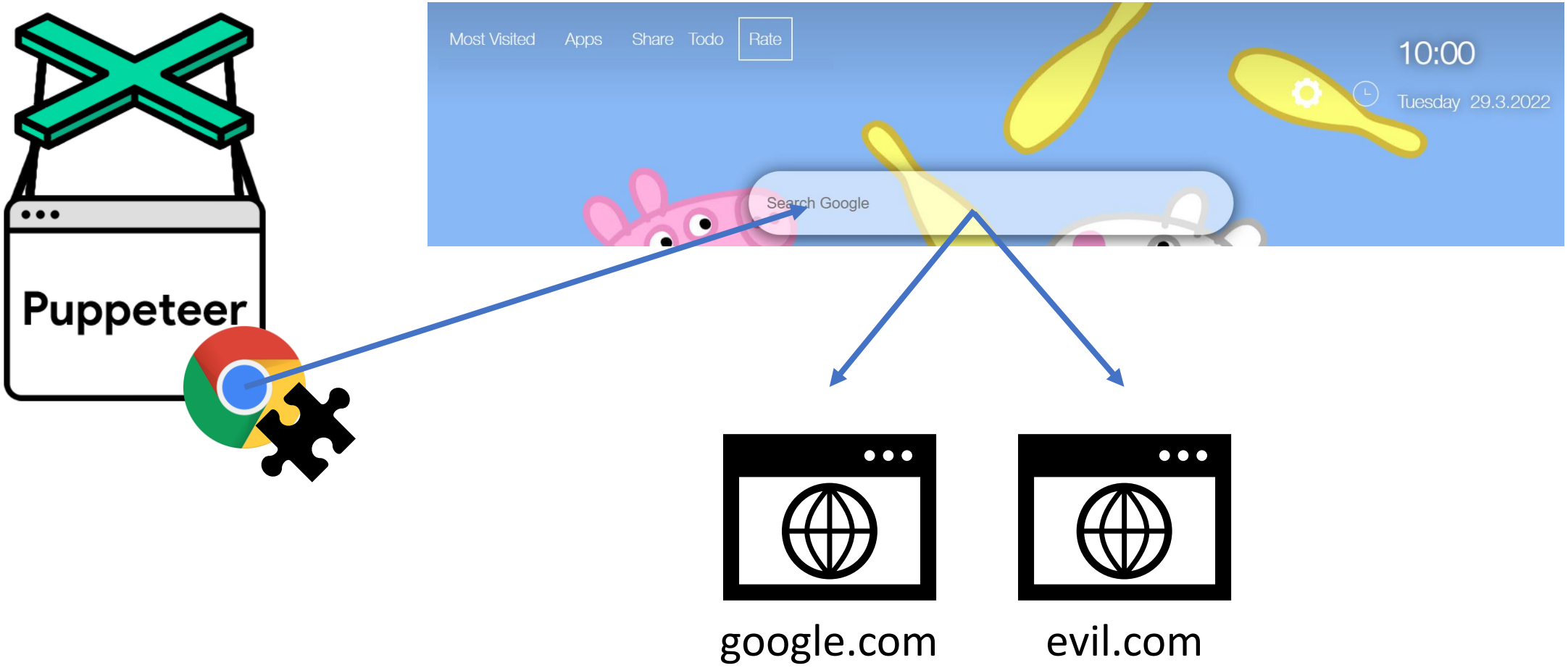
- Correlation between clusters and source code.

Security Analysis – Search Query Stealing

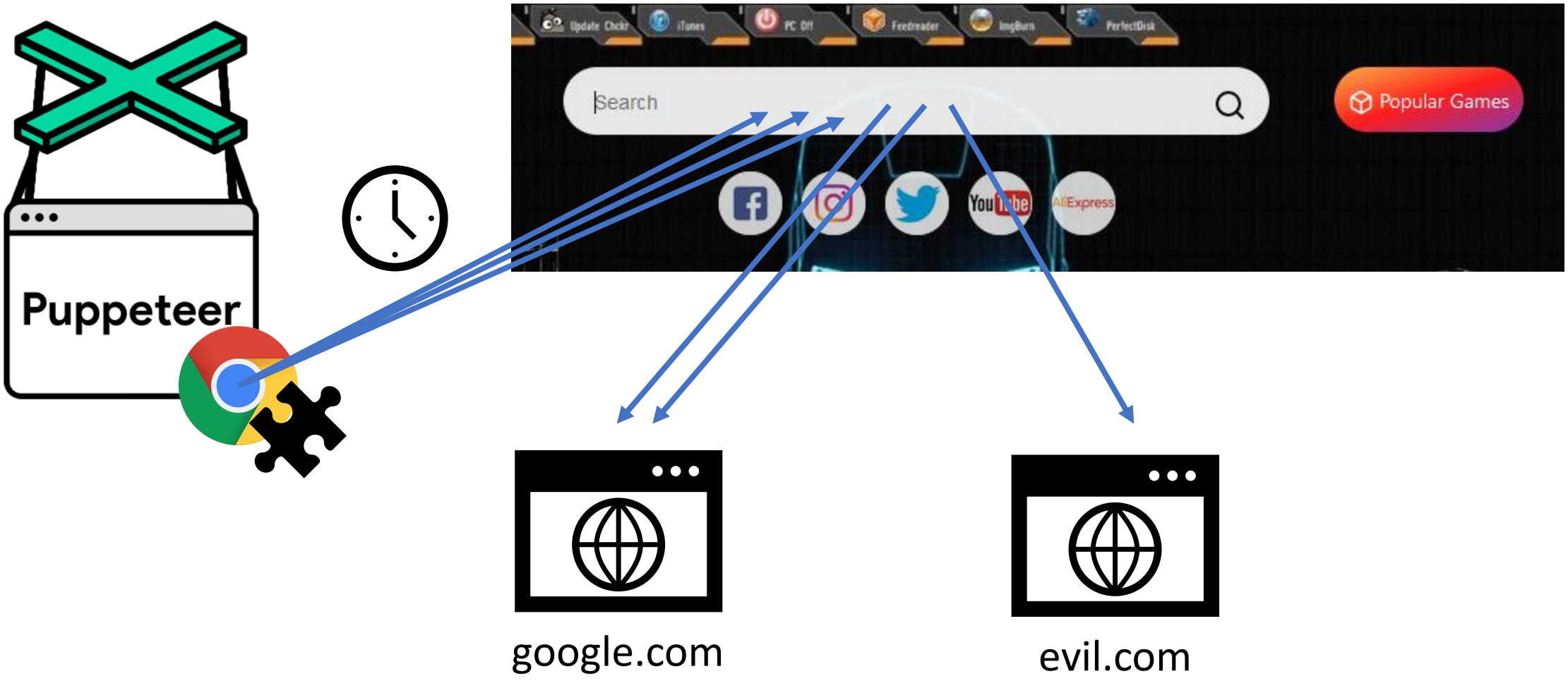




Security Analysis

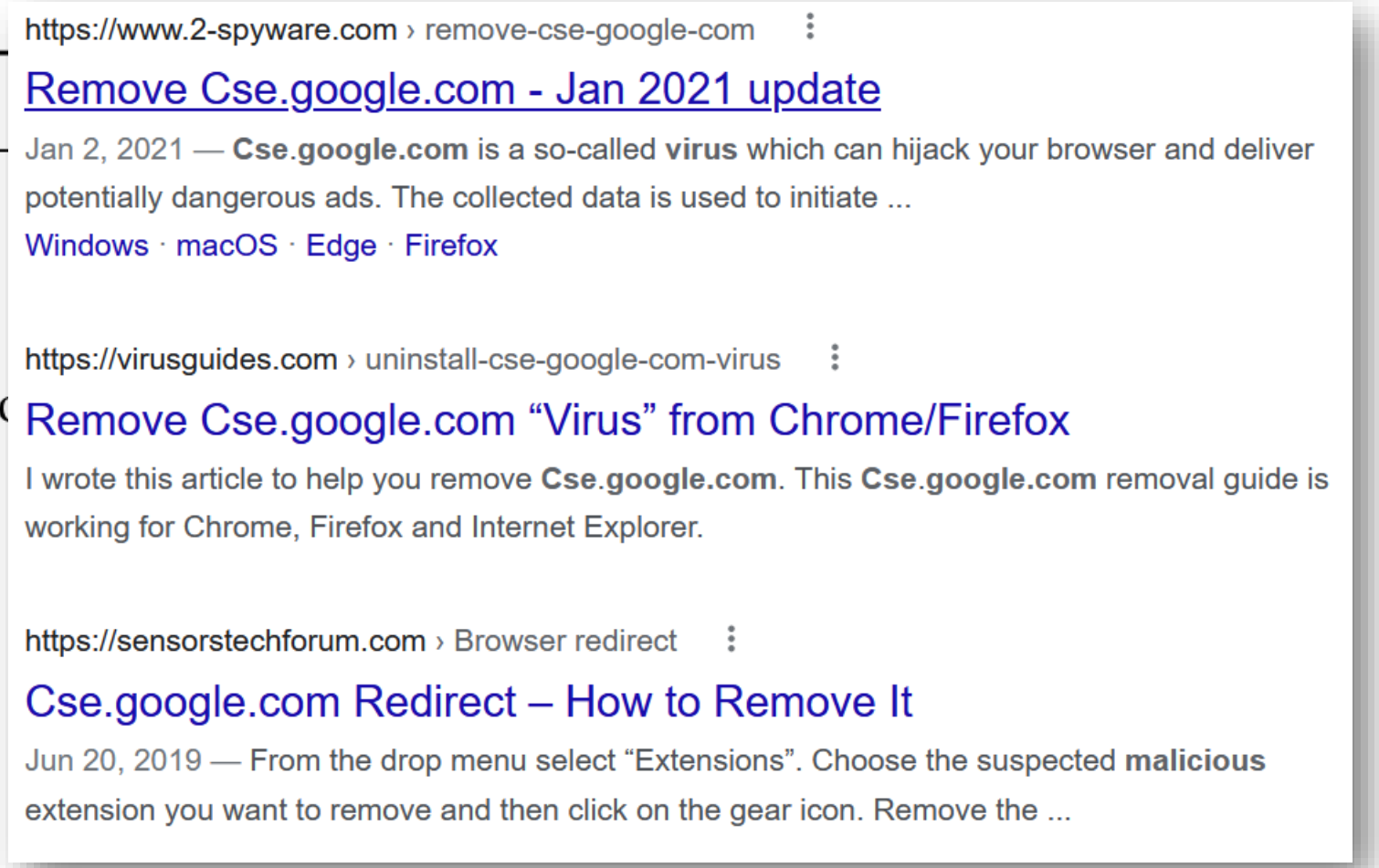


Security Analysis – Long scan



Security Analysis – Results

Domain
cse.google.com
mc.yandex.ru
gundil.com
cors-anywhere.herokuapp.c
www.google-analytics.com
completion.amazon.com
s.bingparachute.com
addiyos.com
the-theme-factory.com
chromethemesonline.net

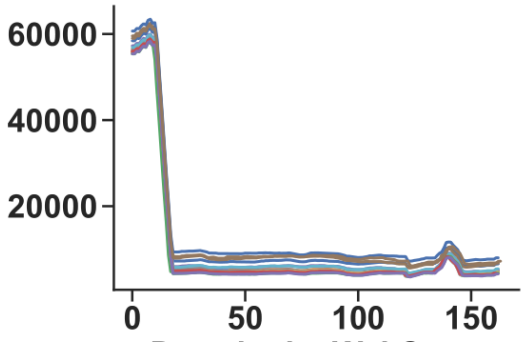


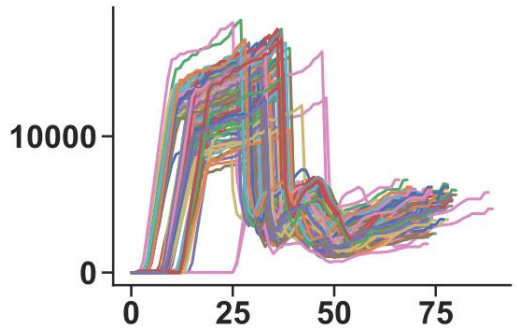
Security Analysis – Results

Domain	Malicious?	#Extensions
www.tabhd.com	Yes	667
www.ultitab.com	Yes	184
themes.wallpaperaddons.com	No	1

Security Analysis – Results

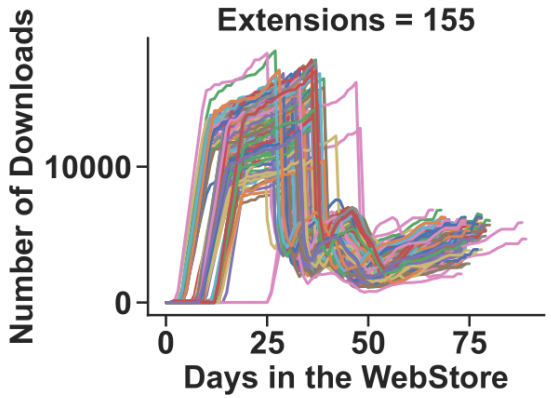
Malicious	0%	0%-50%	50%-80%	80%-100%	100%
Clusters	52	15	7	6	55
Extensions	902	1130	299	401	539



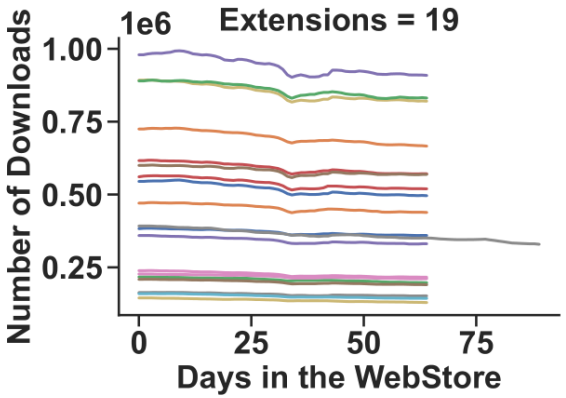


Classifier

Malicious

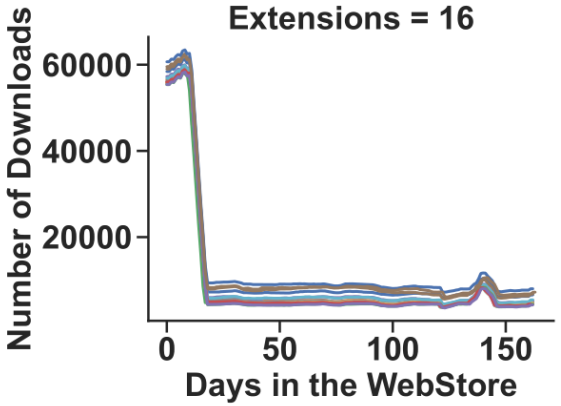


(a) TabHD extensions

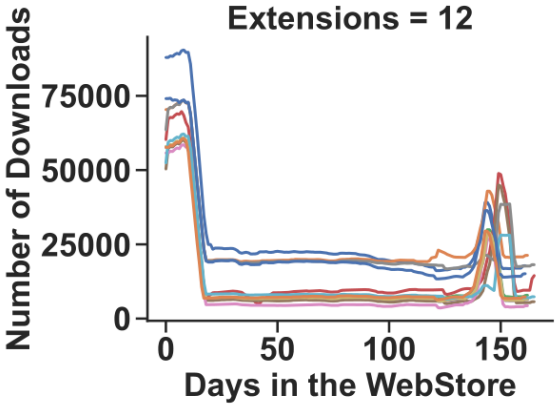


(b) MyWay extensions

Benign



(a) FreeAddon extensions



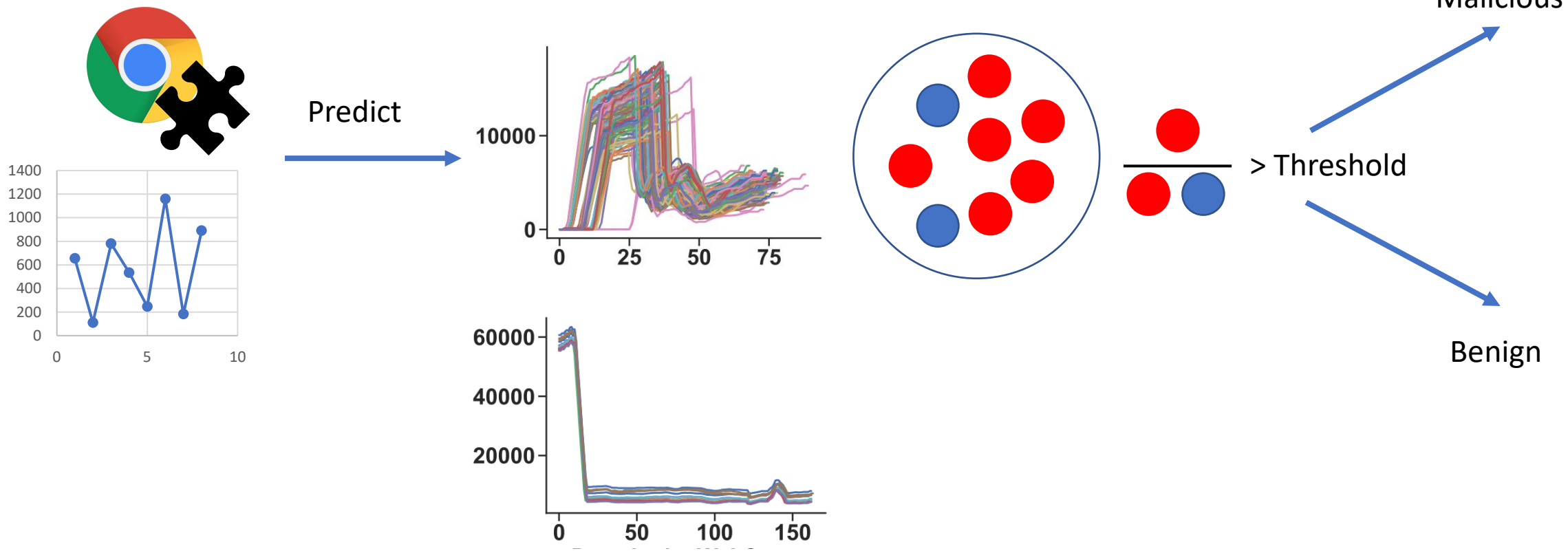
(b) FreeAddon extensions

Classifier - MiniRocket

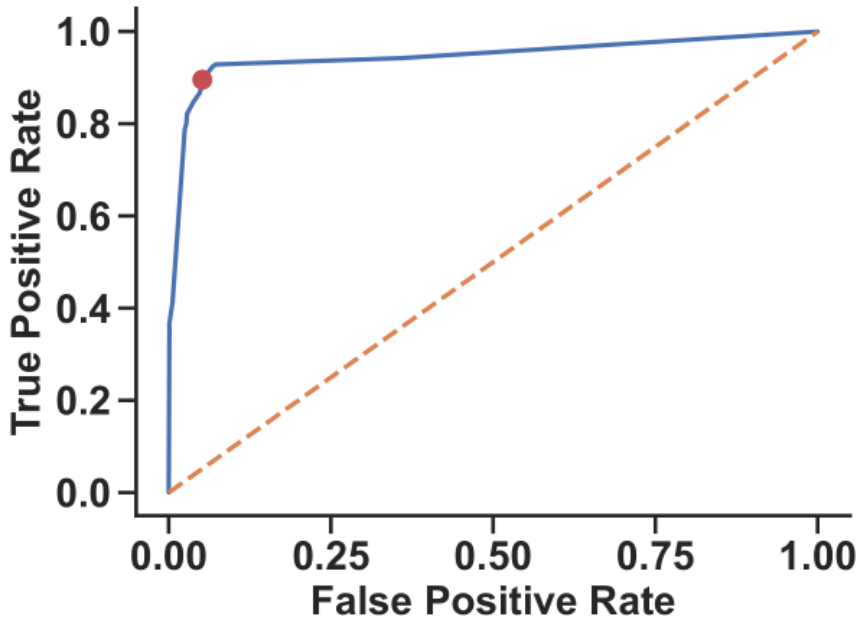
Use already removed extensions for training. (2,059)

Use active extensions for testing (1,212)

Classifier

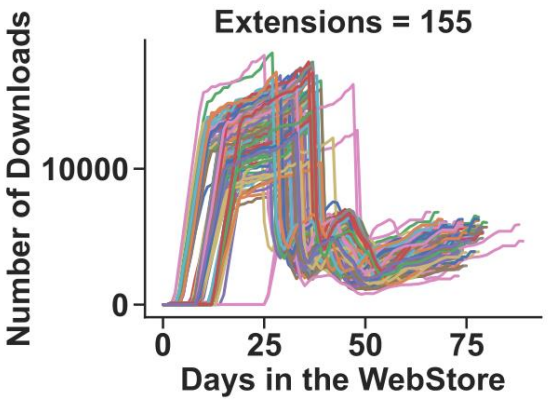

1400
1200
1000
800
600
400
200
0
0
5
10
Predict
10000
0
0
25
50
75
60000
40000
20000
0
50
100
150
> Threshold
Malicious
Benign

Classifier - Results



- Find 326 out of 364 malicious extensions
- F-score of 0.89
- Maliciousness threshold of 0.26

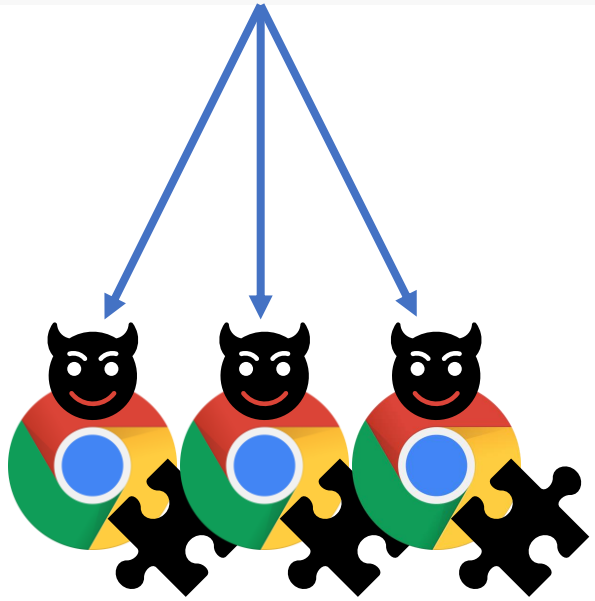
Combining with static analysis



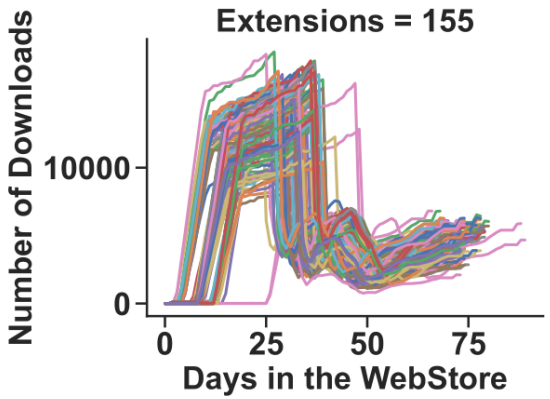
```
window.app= {
  domain: 'https://mytab.me',
  name: 'anime1-6'
}

(() => {
  location.href = `${app.domain}/${app.name}/`;
})();
```

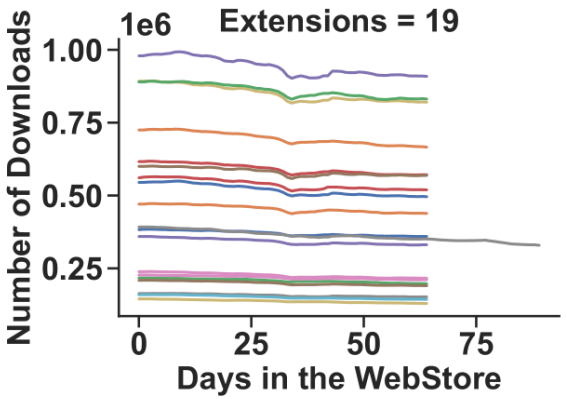
- We found 6,579 additional extensions
- 4,858 have been removed so far



Conclusion

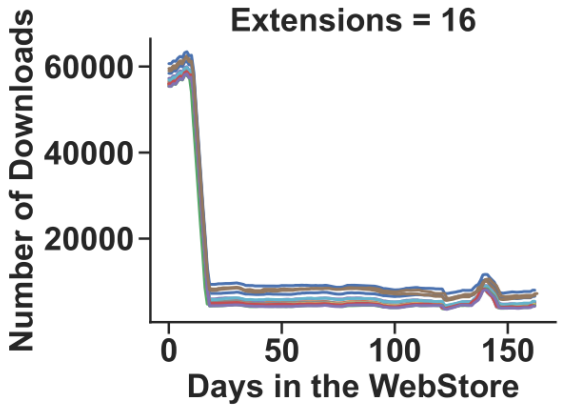


(a) TabHD extensions

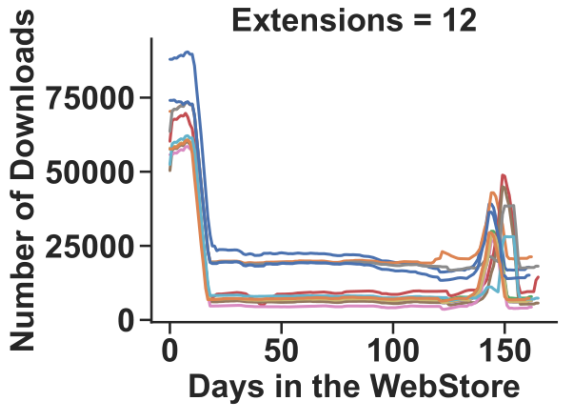


(b) MyWay extensions

Malicious



(a) FreeAddon extensions



(b) FreeAddon extensions

Benign