

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

Pablo Picazo-Sanchez
pablop@chalmers.se

Benjamin Eriksson
beneri@chalmers.se

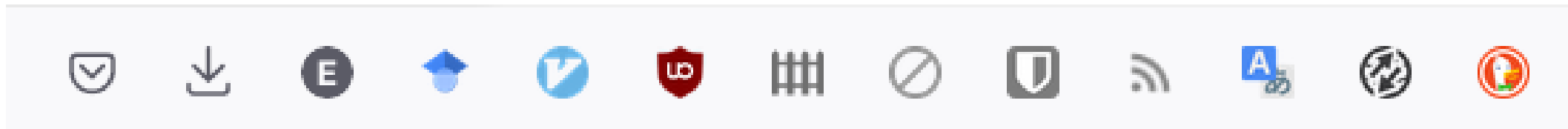
Andrei Sabelfeld
andrei@chalmers.se



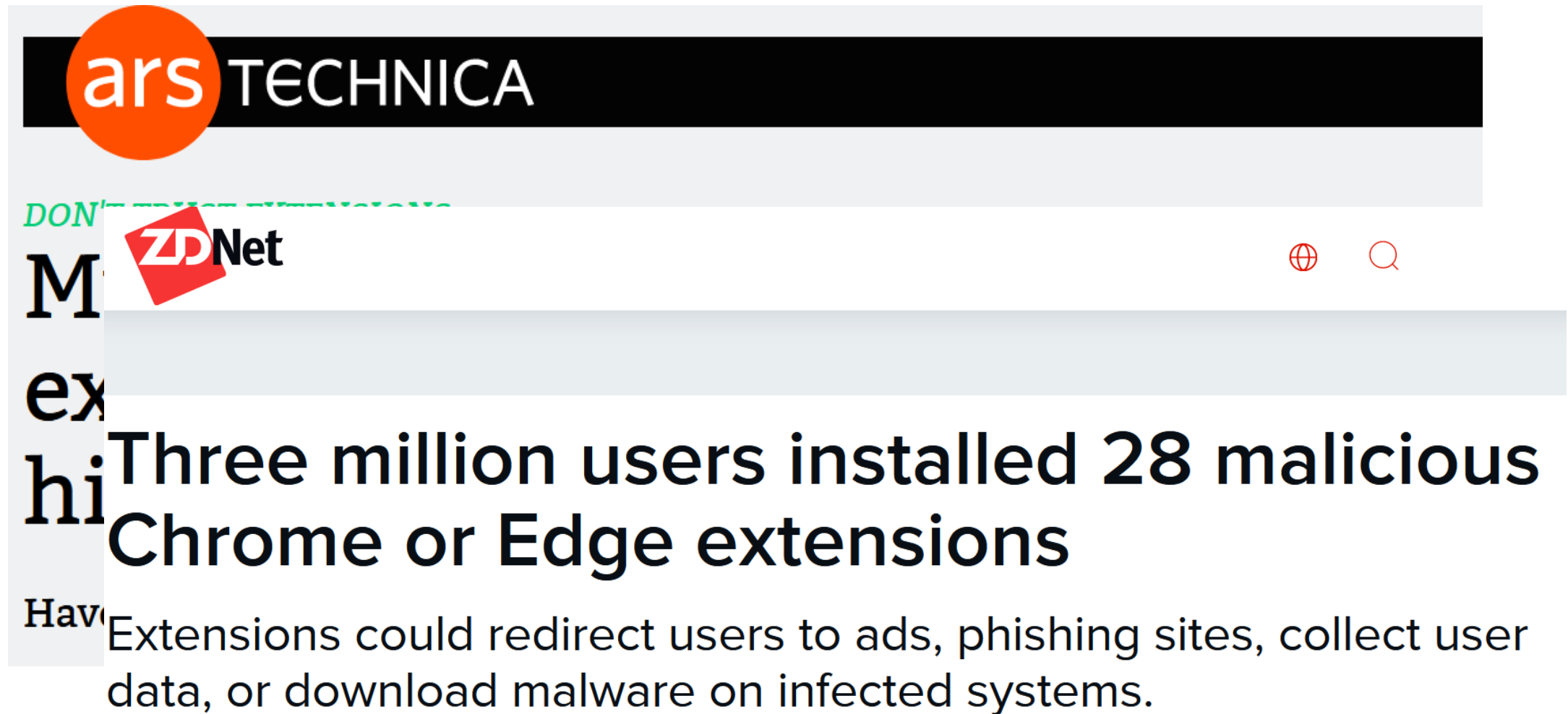
CHALMERS
UNIVERSITY OF TECHNOLOGY

Browser Extensions

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



Problem – Malicious Extensions



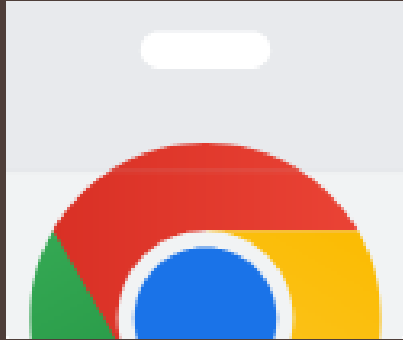
The image shows a screenshot of an Ars Technica article. At the top, the Ars Technica logo is visible, consisting of an orange circle with the word 'ars' in white lowercase letters, followed by the word 'TECHNICA' in white uppercase letters on a black background. Below the logo, the article title is partially visible: 'DON'T... M... ex... hi...'. The main headline reads: 'Three million users installed 28 malicious Chrome or Edge extensions'. Below the headline, the first sentence of the article is visible: 'Have... Extensions could redirect users to ads, phishing sites, collect user data, or download malware on infected systems.' There is also a red 'ZDNet' logo overlaid on the article snippet.

ars TECHNICA

DON'T... M... ex... hi... Have...

Three million users installed 28 malicious Chrome or Edge extensions

Extensions could redirect users to ads, phishing sites, collect user data, or download malware on infected systems.



[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](#)



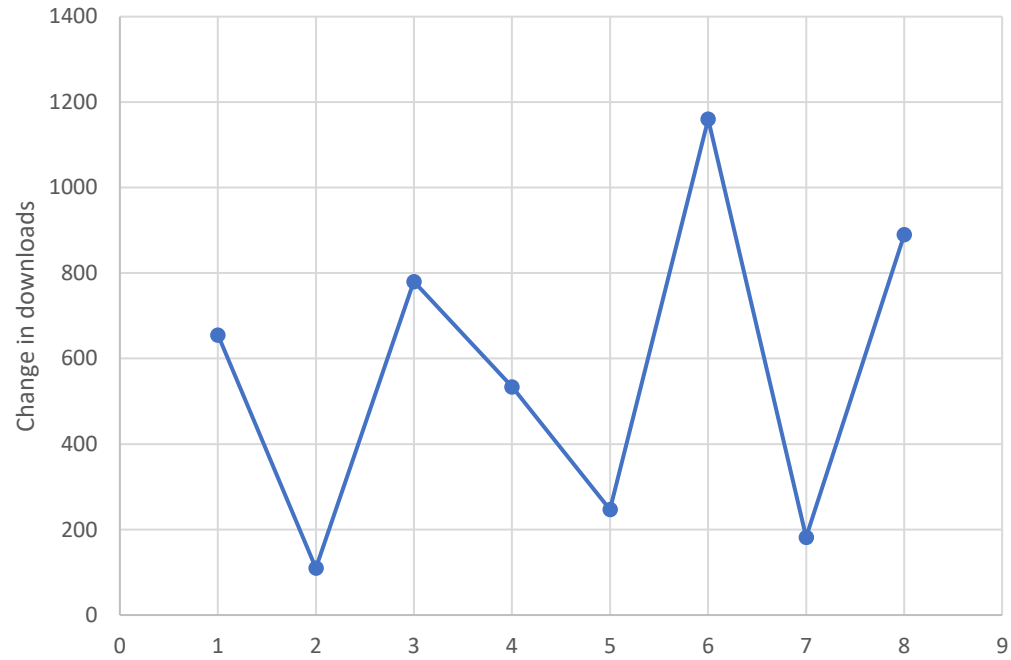
Cute Dogs & Puppies Wallpaper New Tab

coolthemestores.com

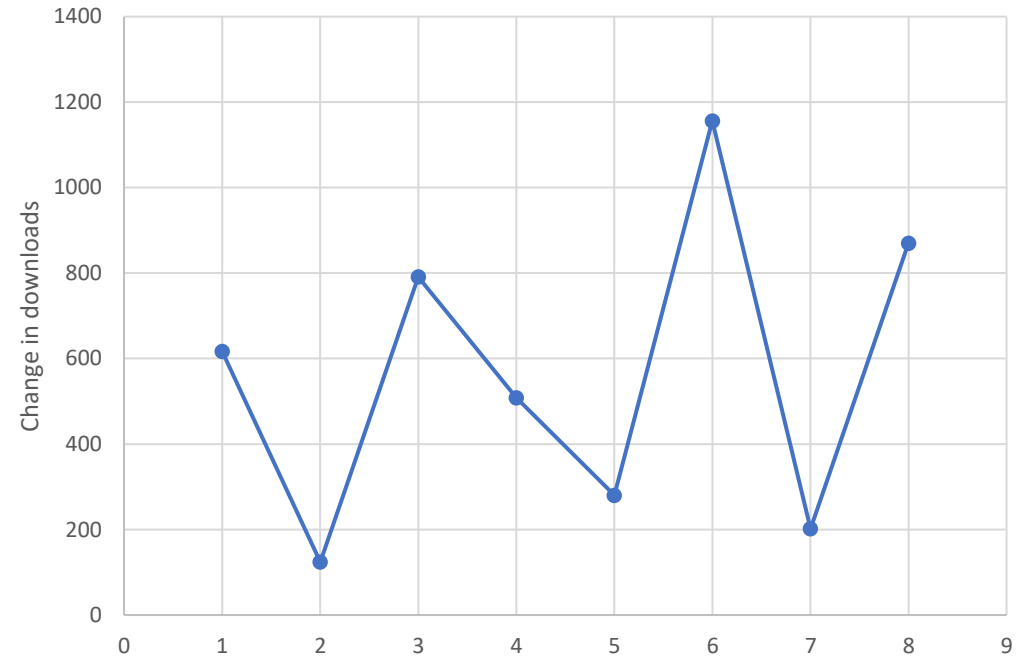
★★★★★ 5 ⓘ | **Fun** | **1,594** users

Download patterns

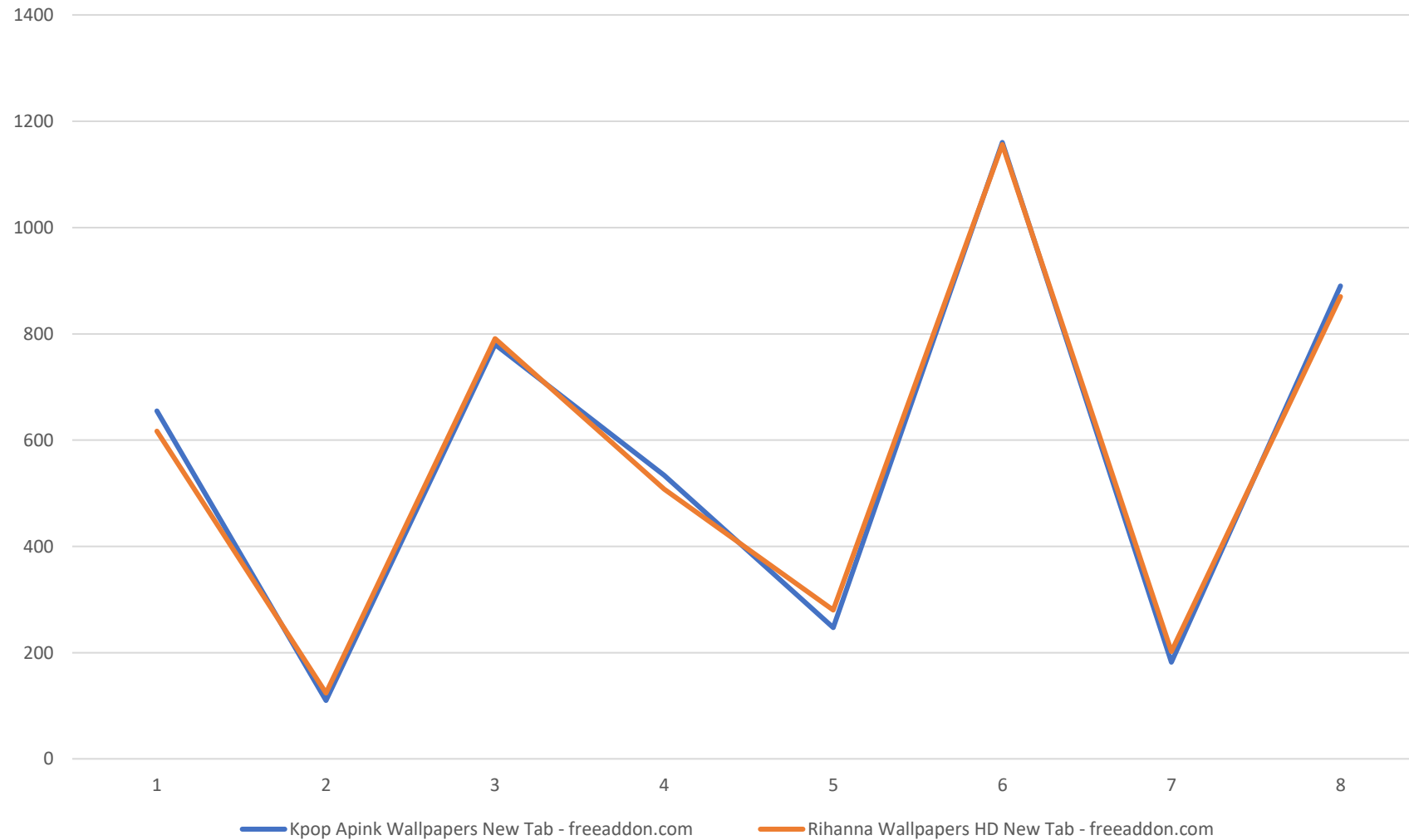
Kpop Apink Wallpapers New Tab - freeaddon.com



Rihanna Wallpapers HD New Tab - freeaddon.com



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?

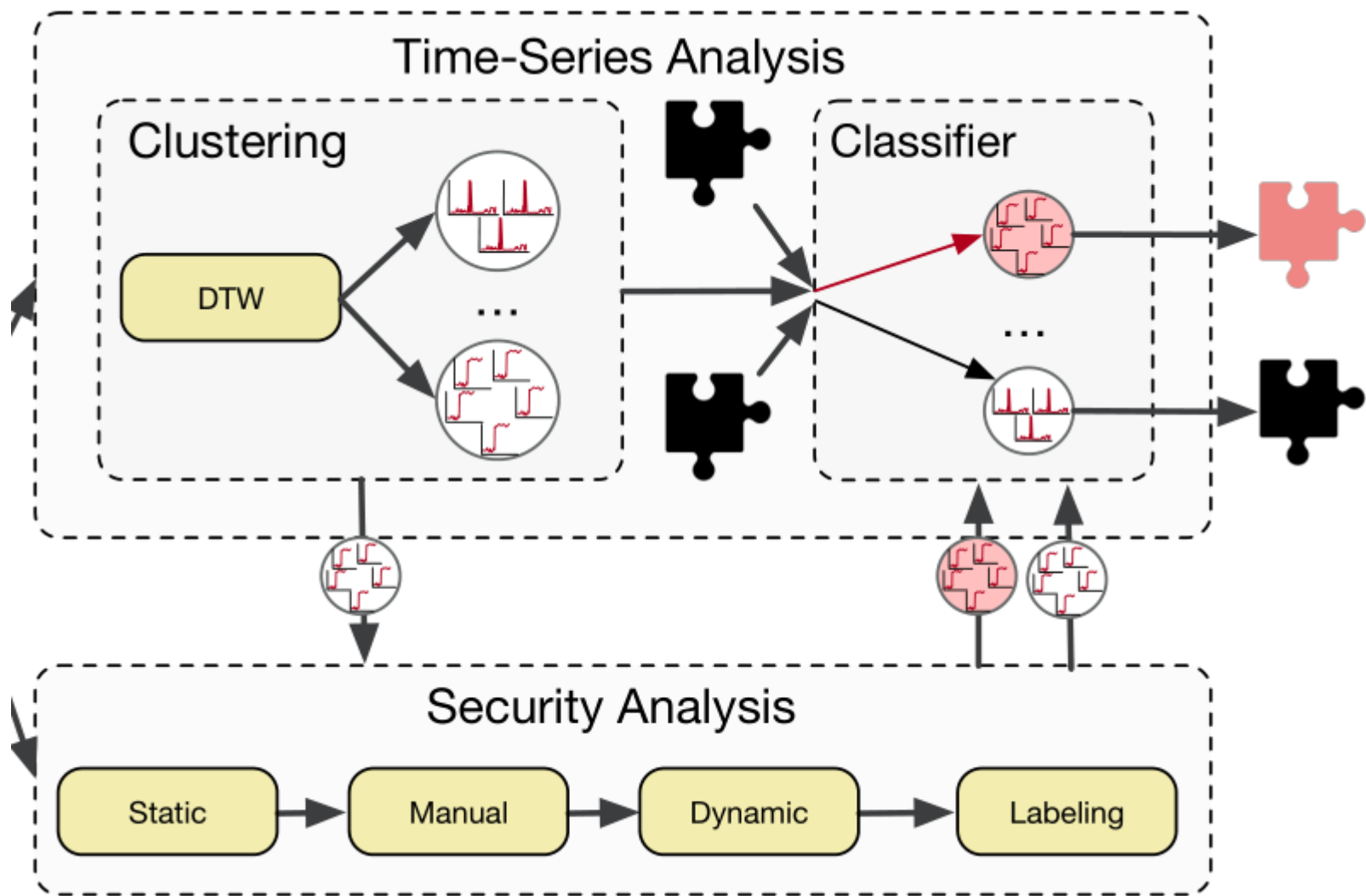
Gathering Data

- Crawl Chrome Web Store everyday for six months
- Calculate average change per extension
- Calculate global average change
- Only keep “interesting” extensions

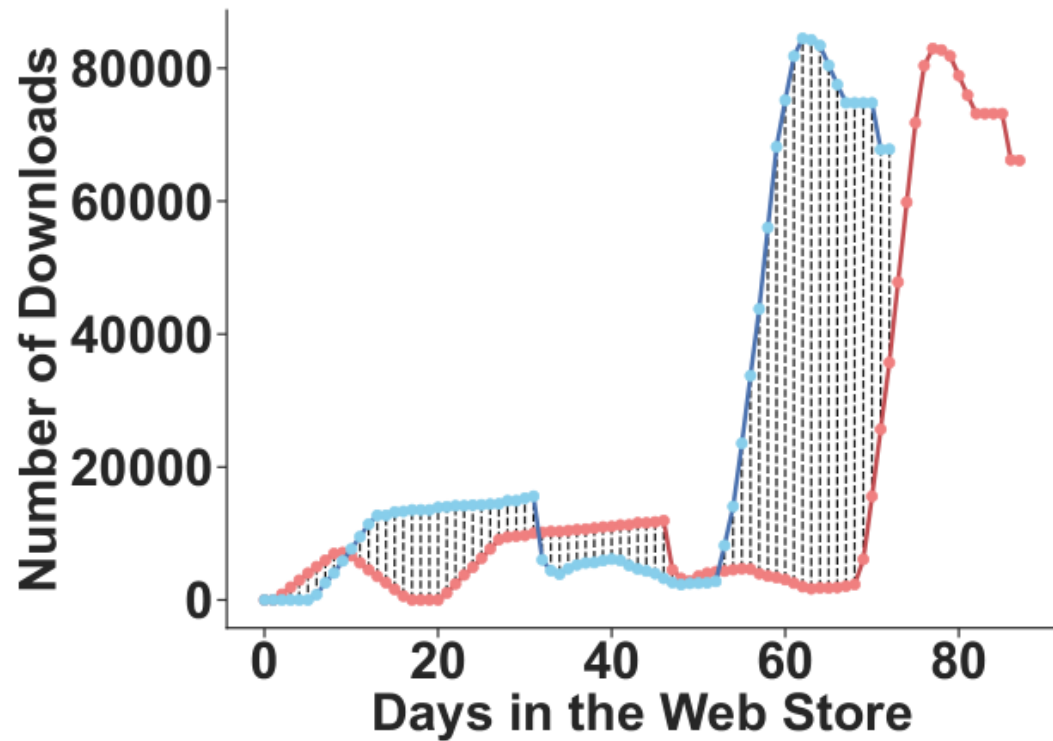
$$\overline{\Delta}_{d_e} = \frac{\sum_{i=1}^n \Delta_{d_e}}{n}$$

$$\overline{\overline{\Delta}} = \frac{\sum_{i=1}^e \Delta_{d_i}}{n}$$

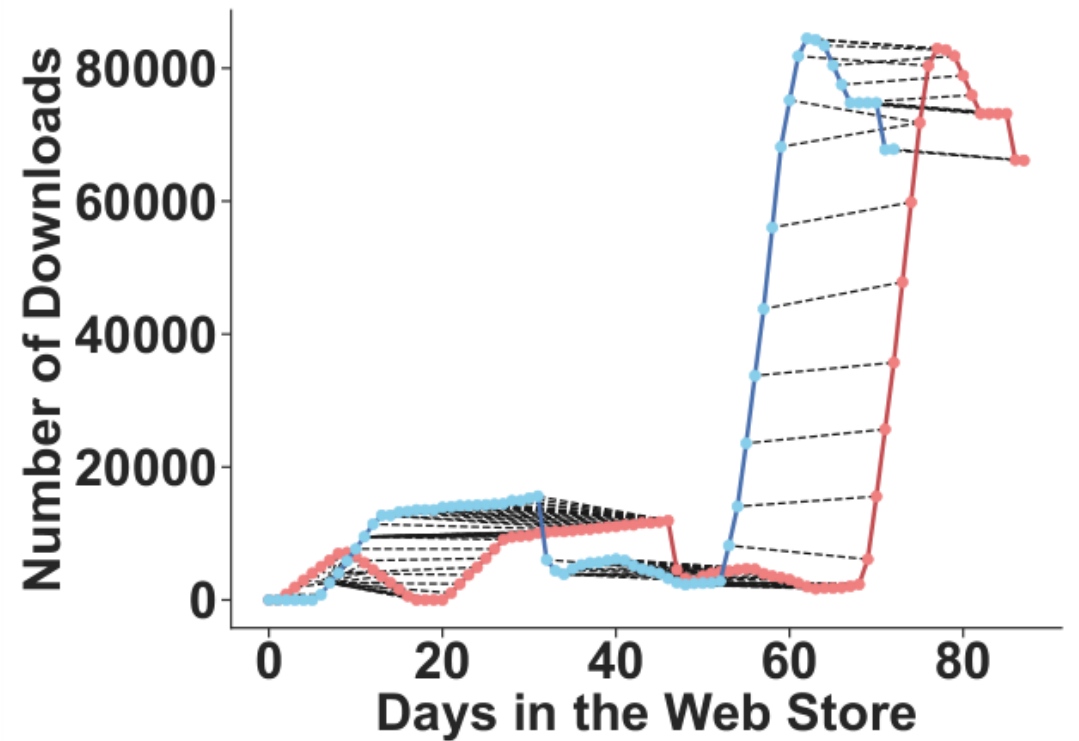
$$\overline{\Delta}_{d_e} \geq \overline{\overline{\Delta}}$$



Similar patterns?

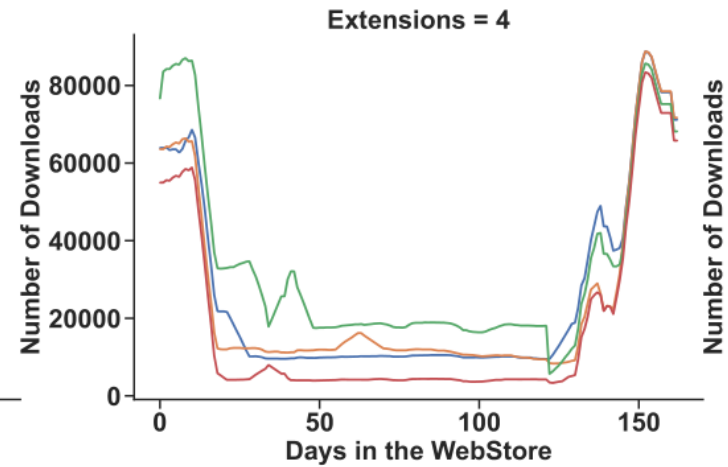
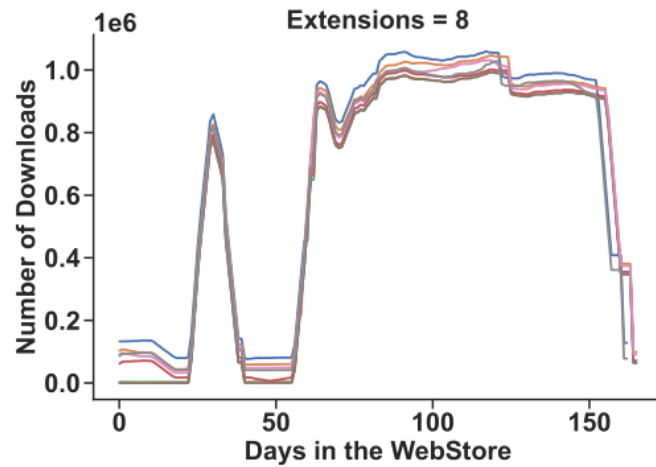
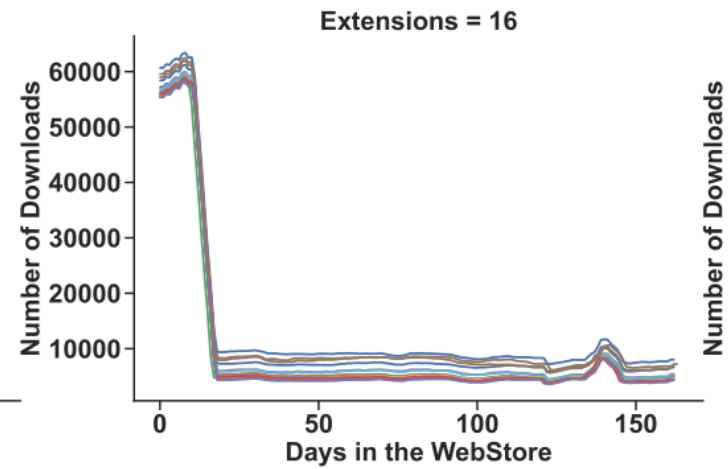
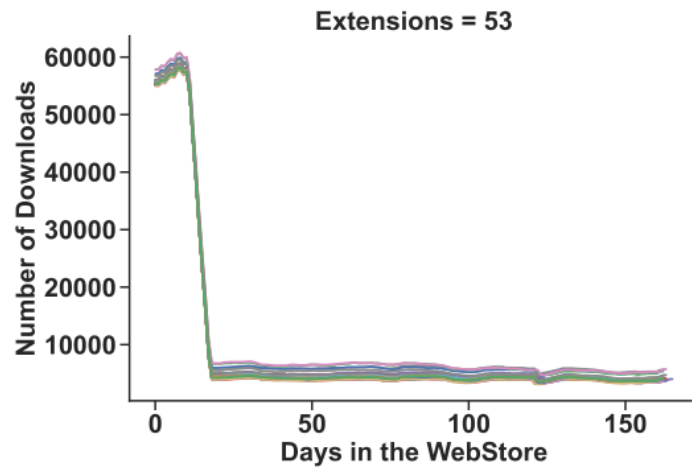


Euclidean distance



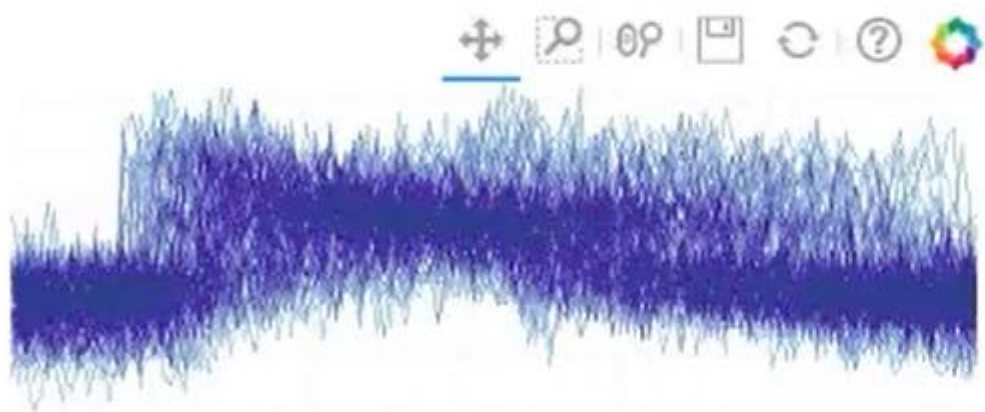
DTW distance

Clustering



Clustering using COBRAS-TS

The full dataset



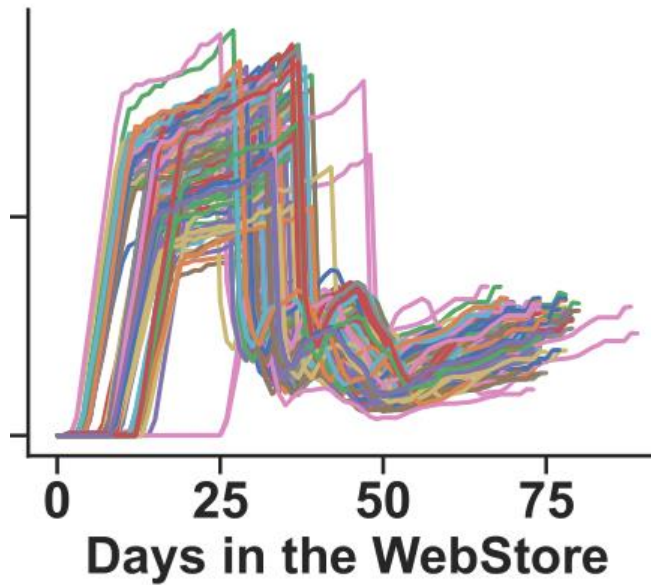
Should these two instances be in the same cluster?



Yes (must-link)

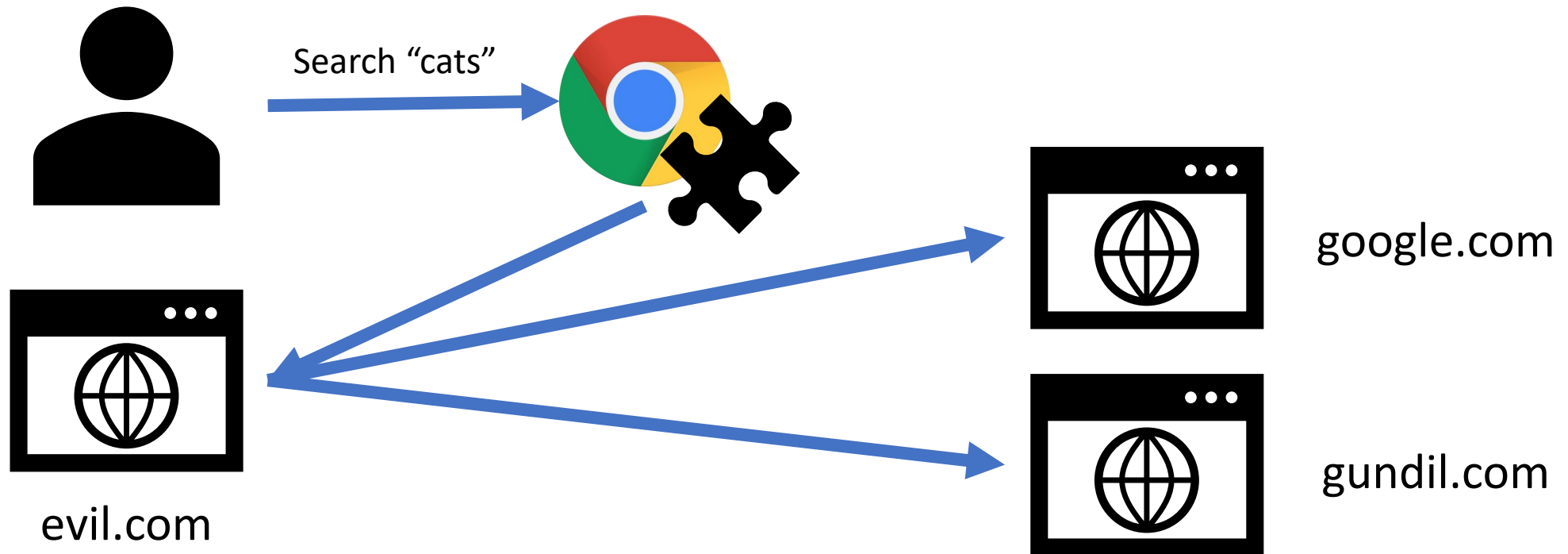
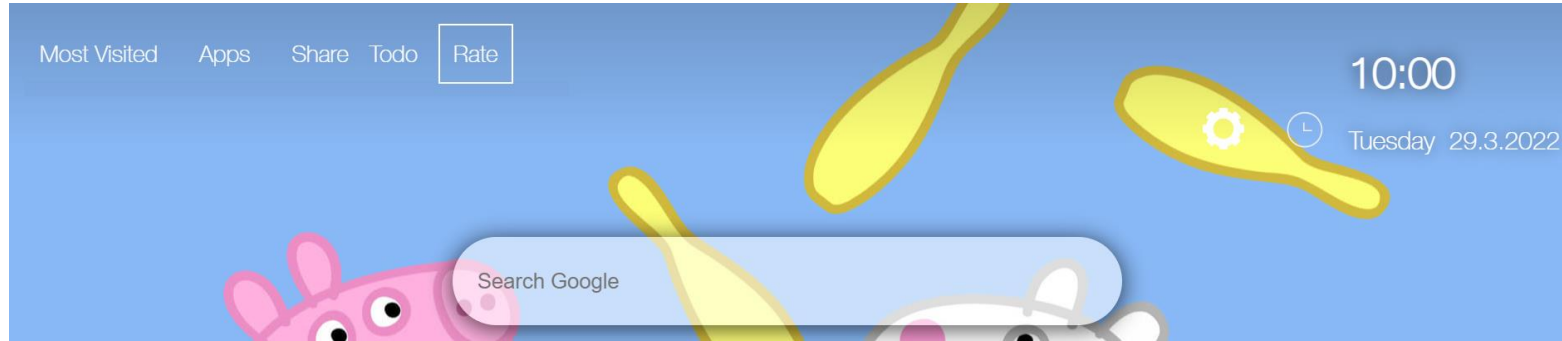
No (cannot-link)

Clustering results

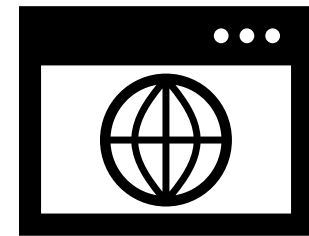
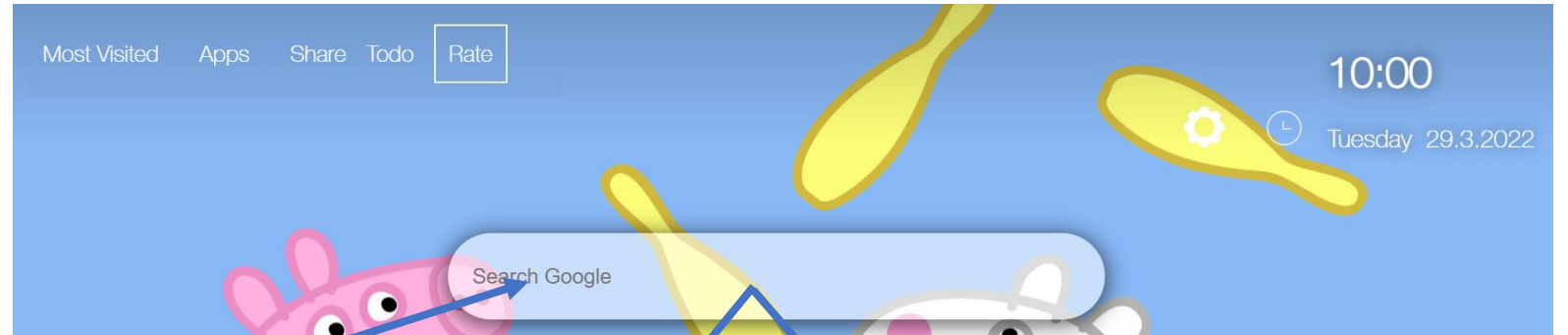


- 3,271 Extensions
- 135 Clusters
- 24 Per cluster
- Correlation between clusters and source code.

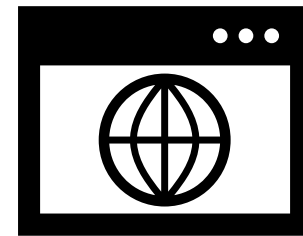
Security Analysis – Search Query Stealing



Security Analysis

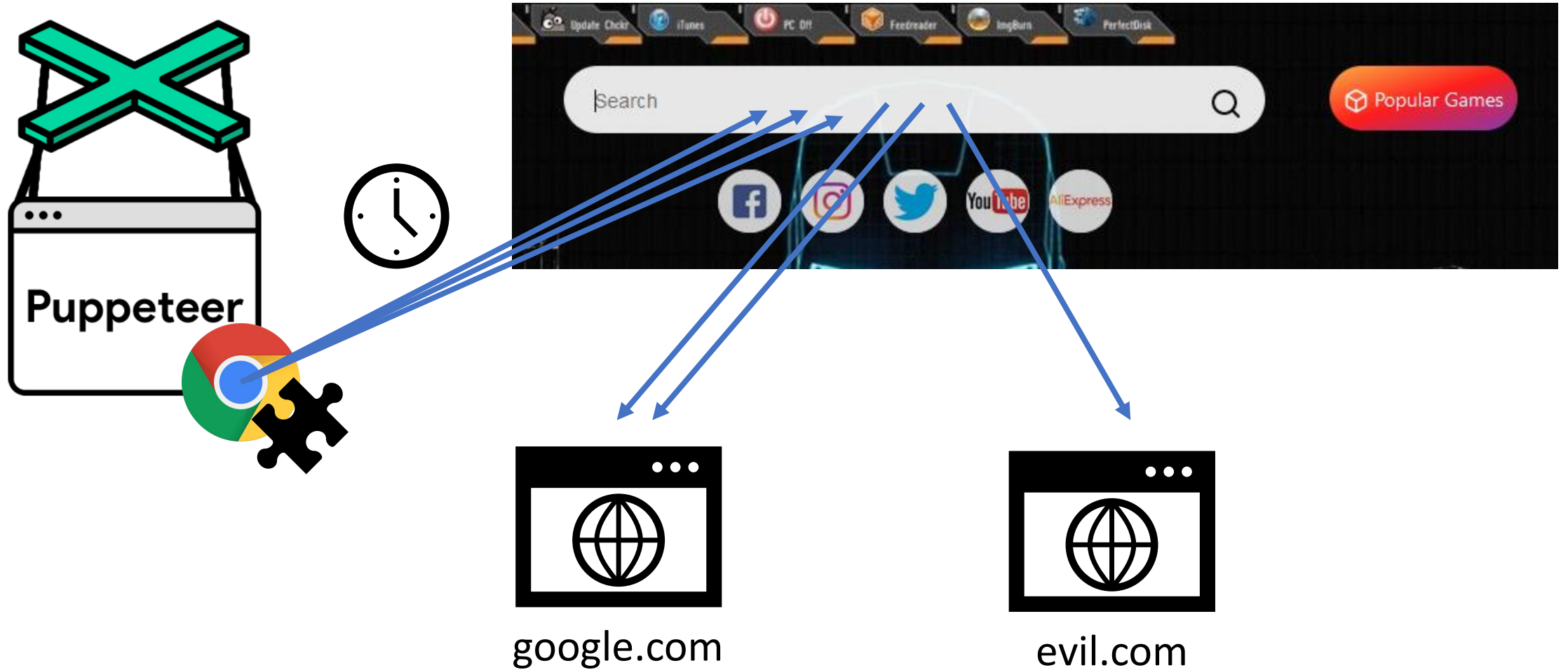


google.com



evil.com

Security Analysis – Long scan



Security Analysis – Results

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

<https://www.2-spyware.com> › [remove-cse-google-com](#) ⋮

[Remove Cse.google.com - Jan 2021 update](#)

Jan 2, 2021 — **Cse.google.com** is a so-called **virus** which can hijack your browser and deliver potentially dangerous ads. The collected data is used to initiate ...

[Windows](#) · [macOS](#) · [Edge](#) · [Firefox](#)

<https://virusguides.com> › [uninstall-cse-google-com-virus](#) ⋮

[Remove Cse.google.com “Virus” from Chrome/Firefox](#)

I wrote this article to help you remove **Cse.google.com**. This **Cse.google.com** removal guide is working for Chrome, Firefox and Internet Explorer.

<https://sensorstechforum.com> › [Browser redirect](#) ⋮

[Cse.google.com Redirect – How to Remove It](#)

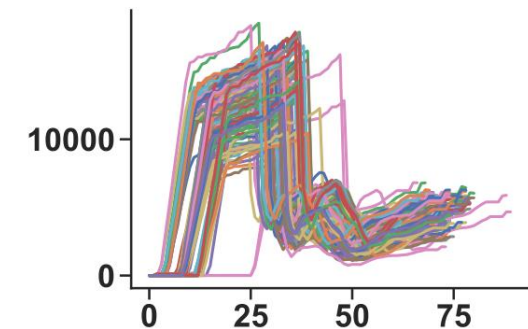
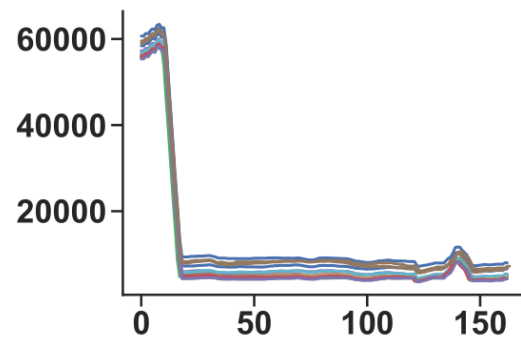
Jun 20, 2019 — From the drop menu select “Extensions”. Choose the suspected **malicious** extension you want to remove and then click on the gear icon. Remove the ...

Security Analysis – Results

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

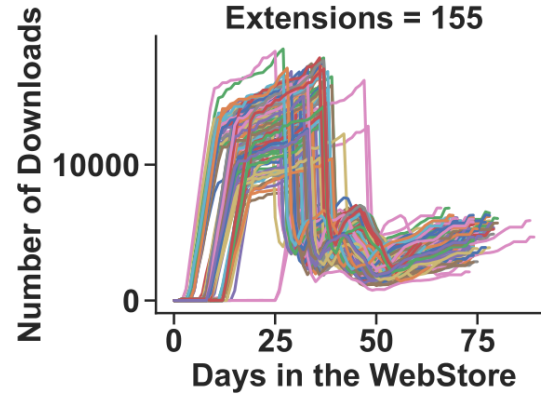
Security Analysis – Results

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

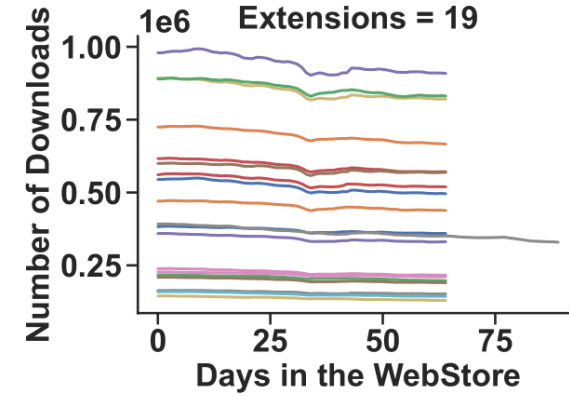


Classifier

Malicious

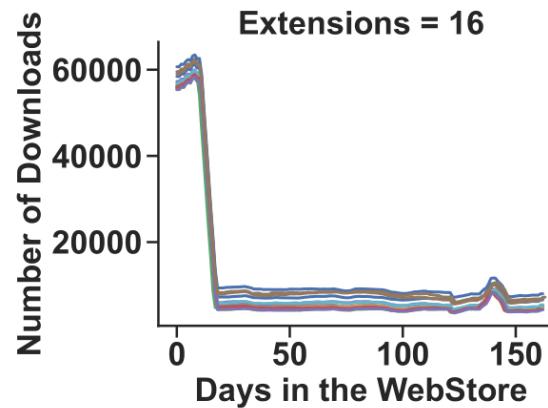


(a) TabHD extensions

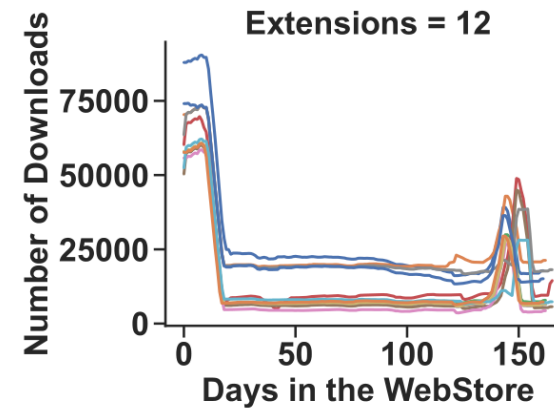


(b) MyWay extensions

Benign



(a) FreeAddon extensions



(b) FreeAddon extensions

Classifier - MiniRocket

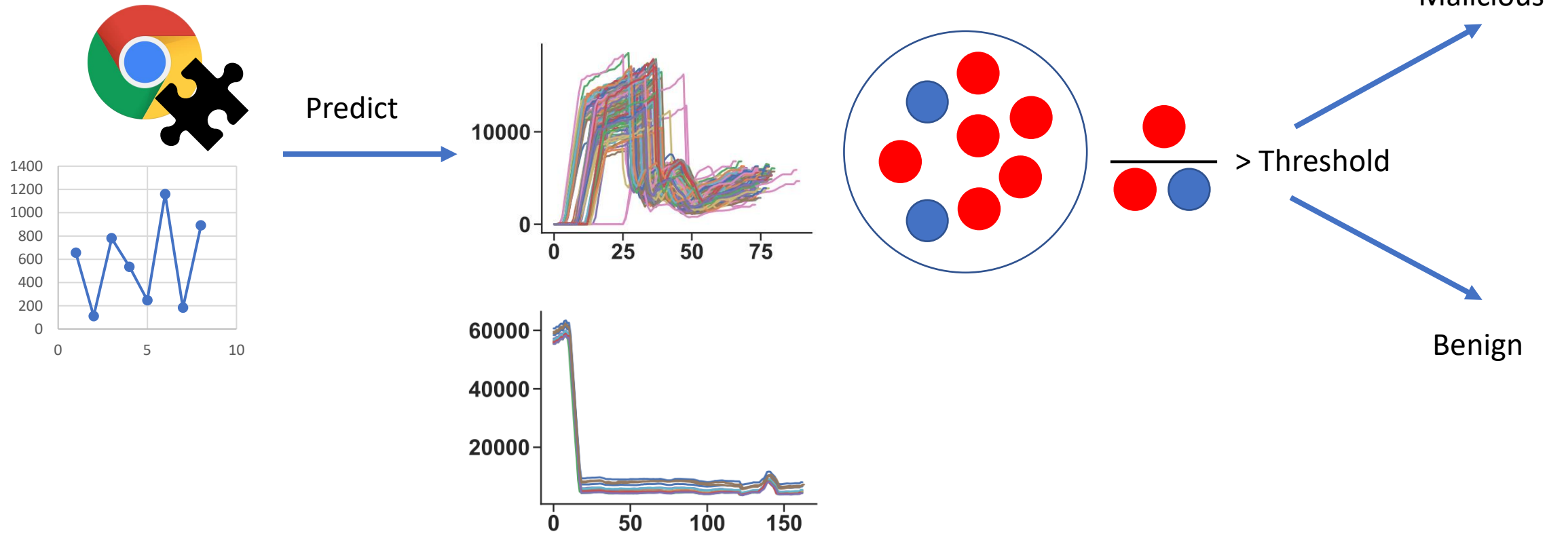


Use already removed extensions for training. (2,059)

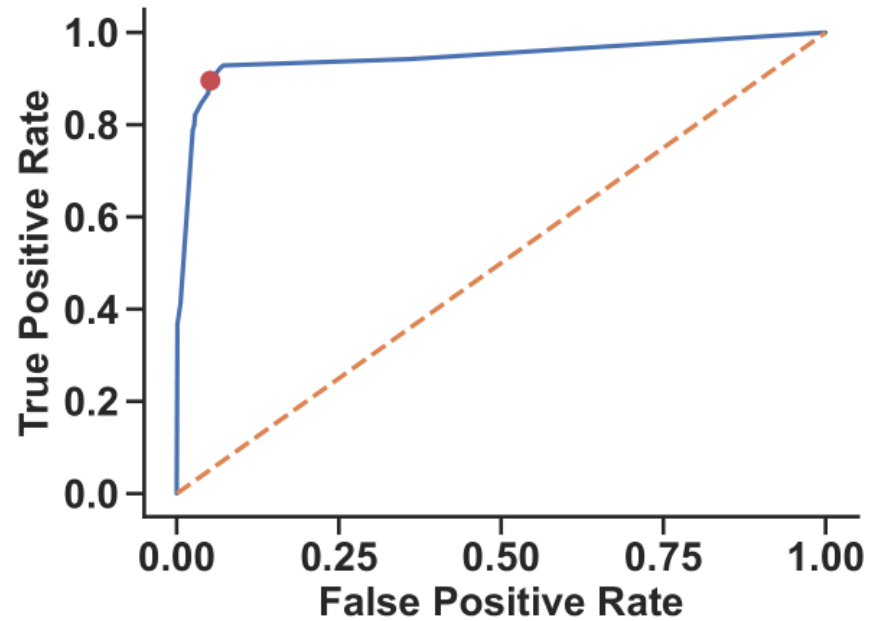


Use active extensions for testing (1,212)

Classifier

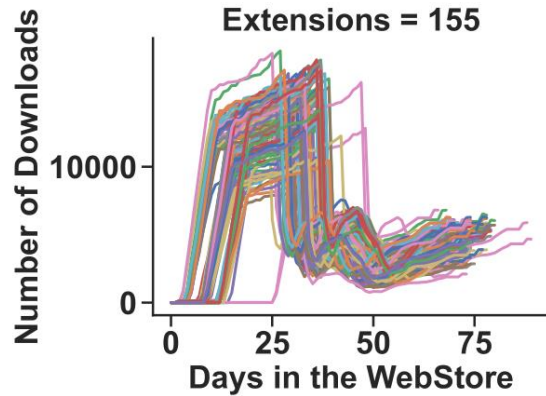


Classifier - Results

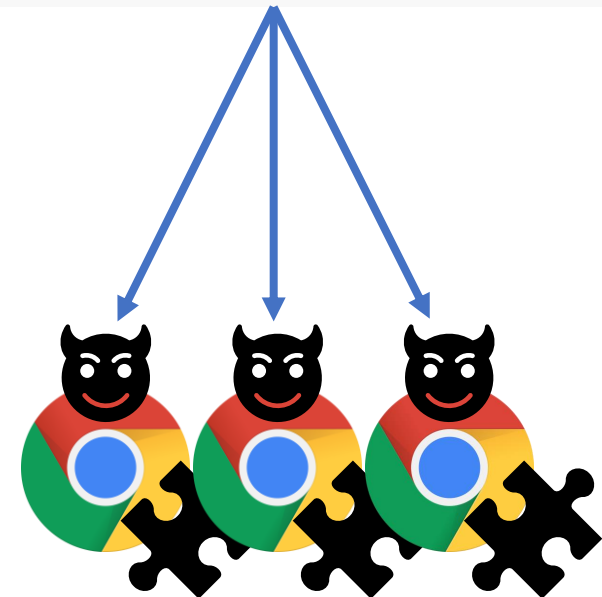


- Find 326 out of 364 malicious extensions
- F-score of 0.89
- Maliciousness threshold of 0.26

Combining with static analysis

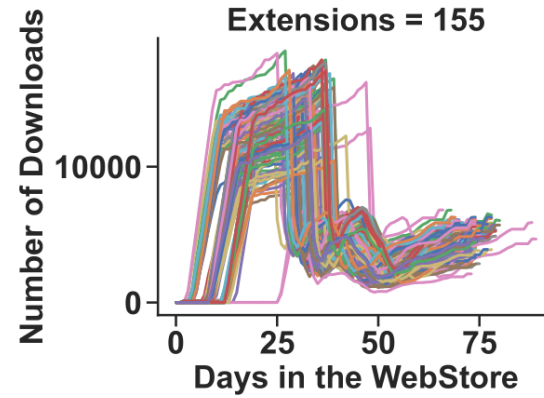
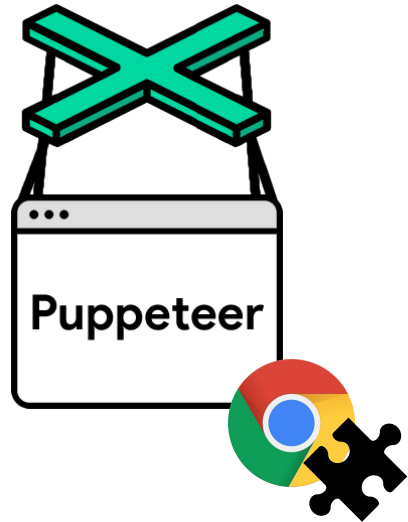


```
window.app= {  
  domain: 'https://mytab.me',  
  name: 'anime1-6'  
}  
  
(() => {  
  location.href = `${app.domain}/${app.name}/`;  
})();
```

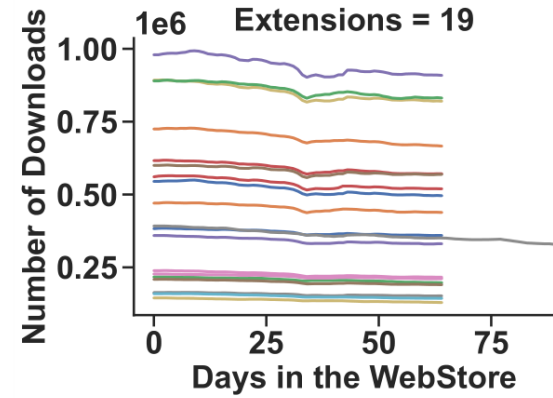


- We found 6,579 additional extensions
- 4,858 have been removed so far

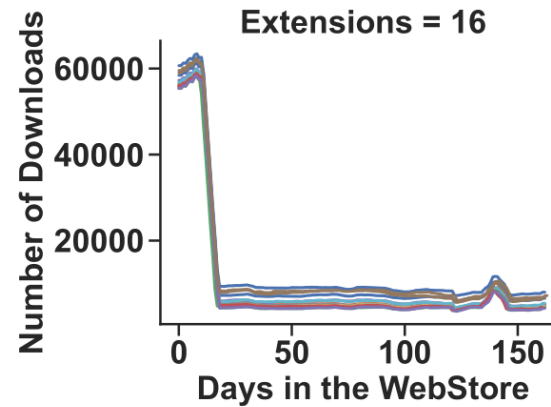
Conclusion



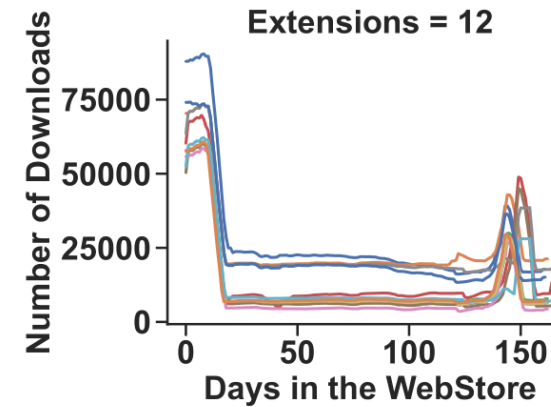
(a) TabHD extensions



(b) MyWay extensions



(a) FreeAddon extensions



(b) FreeAddon extensions

Malicious

Benign