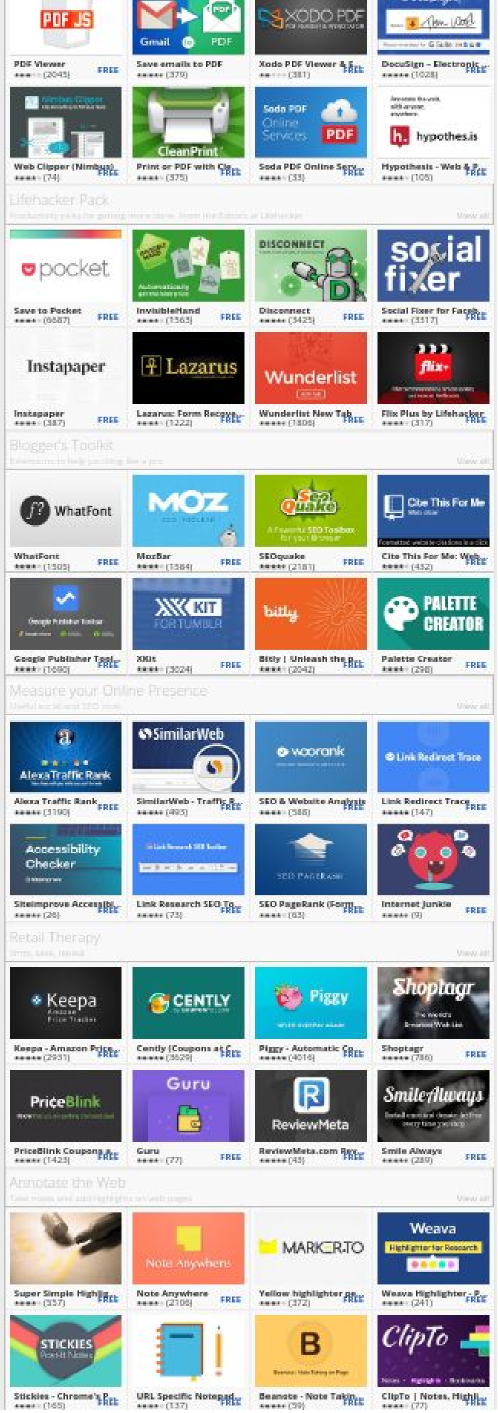
Ex-Ray: Detection of History-Leaking Browser Extensions

Michael Weissbacher, Enrico Mariconti, Guillermo Suarez-Tangil, Gianluca Stringhini, William Robertson, Engin Kirda

Northeastern University, University College London



PDF Viewer (2045) FREE
Save emails to PDF (379)
Xodo PDF Viewer & E... (381) FREE
DocuSign – Electronic... (1028) FREE
Web Clipper (Nimbus)... (74) FREE
Print or PDF with Cle... (375) FREE
Soda PDF Online Serv... (33) FREE
Hypothesis - Web & P... (105) FREE

Lifehacker Pack
Productivity picks for getting more done. From the Editors at Lifehacker
View all

Save to Pocket (6687) FREE
InvisibleHand (1563) FREE
Disconnect (3425) FREE
Social Fixer for Faceb... (3317) FREE
Instapaper (387) FREE
Lazarus: Form Recove... (1222) FREE
Wunderlist New Tab (1806) FREE
Flix Plus by Lifehacker (317) FREE

Blogger's Toolkit
Extensions to help you blog like a pro
View all

WhatFont (1505) FREE
MozBar (1584) FREE
SEOquake (2181) FREE
Cite This For Me: Web... (432) FREE
Google Publisher Tool... (1690) FREE
XKit (3024) FREE
Bitly | Unleash the p... (2042) FREE
Palette Creator (298) FREE

Measure your Online Presence
Useful social and SEO tools
View all

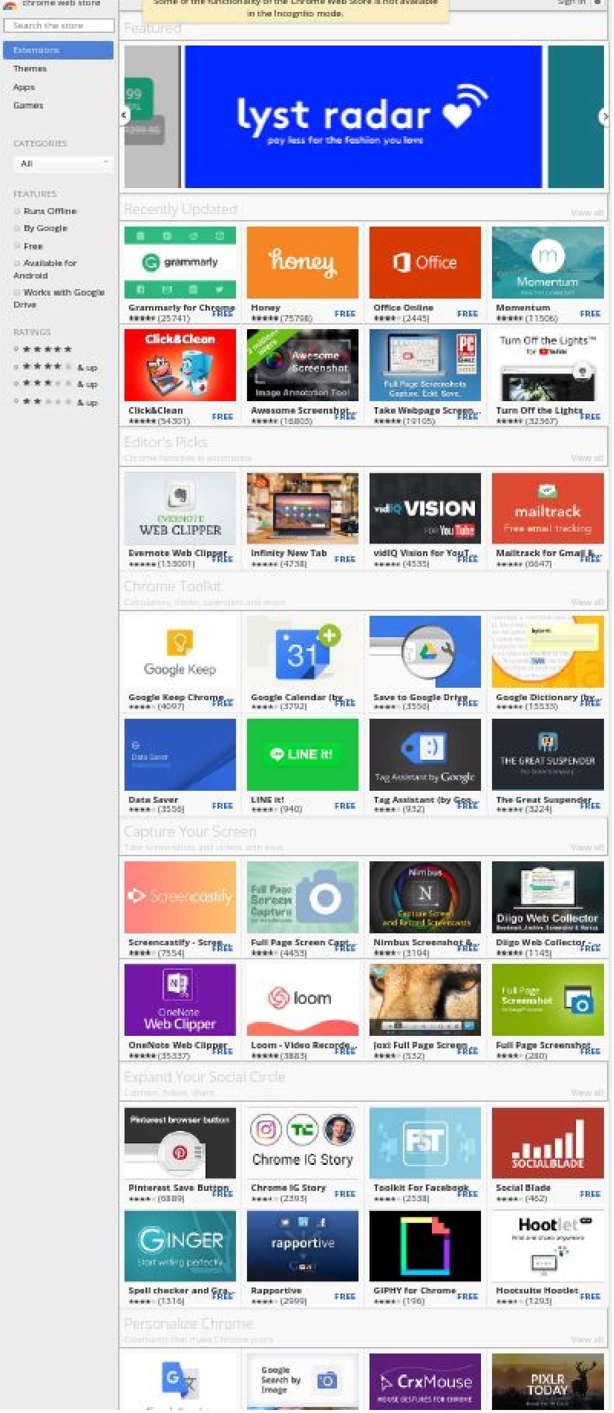
Alexa Traffic Rank (3190) FREE
SimilarWeb - Traffic R... (493) FREE
SEO & Website Analysis (588) FREE
Link Redirect Trace (147) FREE
Siteimprove Accessibi... (26) FREE
Link Research SEO To... (73) FREE
SEO PageRank (Form... (83) FREE
Internet Junkie (9) FREE

Retail Therapy
Shop, save, repeat
View all

Keepa - Amazon Price... (2931) FREE
Cently (Coupons at C... (3629) FREE
Piggy - Automatic Co... (4016) FREE
Shoptagr (786) FREE
PriceBlink Coupons a... (1423) FREE
Guru (77) FREE
ReviewMeta.com Rev... (43) FREE
Smile Always (289) FREE

Annotate the Web
Take notes and add highlights on web pages
View all

Super Simple Highlig... (337) FREE
Note Anywhere (2106) FREE
Yellow highlighter pe... (372) FREE
Weava Highlighter - P... (241) FREE
Stickies - Chrome's P... (165) FREE
URL Specific Notepad... (137) FREE
Beanote - Note Takin... (39) FREE
ClipTo | Notes, Highli... (77) FREE



chrome web store
Search the store
Sign in
Some of the functionality of the Chrome Web Store is not available in the Incognito mode.

Extensions
Themes
Apps
Games

CATEGORIES
All

FEATURES
○ Runs Offline
○ By Google
○ Free
○ Available for Android
○ Works with Google Drive

RATINGS
○ ★★★★★
○ ★★★★☆ & up
○ ★★★☆☆ & up
○ ★★☆☆☆ & up

Featured

Recently Updated
View all

Grammarly for Chrome (25741) FREE
Honey (75798) FREE
Office Online (2445) FREE
Momentum (11506) FREE
Click&Clean (54301) FREE
Awesome Screenshot... (16805) FREE
Take Webpage Screen... (19105) FREE
Turn Off the Lights (32367) FREE

Editor's Picks
Chrome favorites in extensions
View all

Evernote Web Clipper (133001) FREE
Infinity New Tab (4738) FREE
vidIQ Vision for YouT... (4535) FREE
Mailtrack for Gmail &... (6647) FREE

Chrome Toolkit
Calculators, clocks, calendars and more
View all

Google Keep Chrome... (4097) FREE
Google Calendar (by... (3792) FREE
Save to Google Drive (3556) FREE
Google Dictionary (by... (13533) FREE
Data Saver (3556) FREE
LINE it! (940) FREE
Tag Assistant (by Goo... (932) FREE
The Great Suspender (3224) FREE

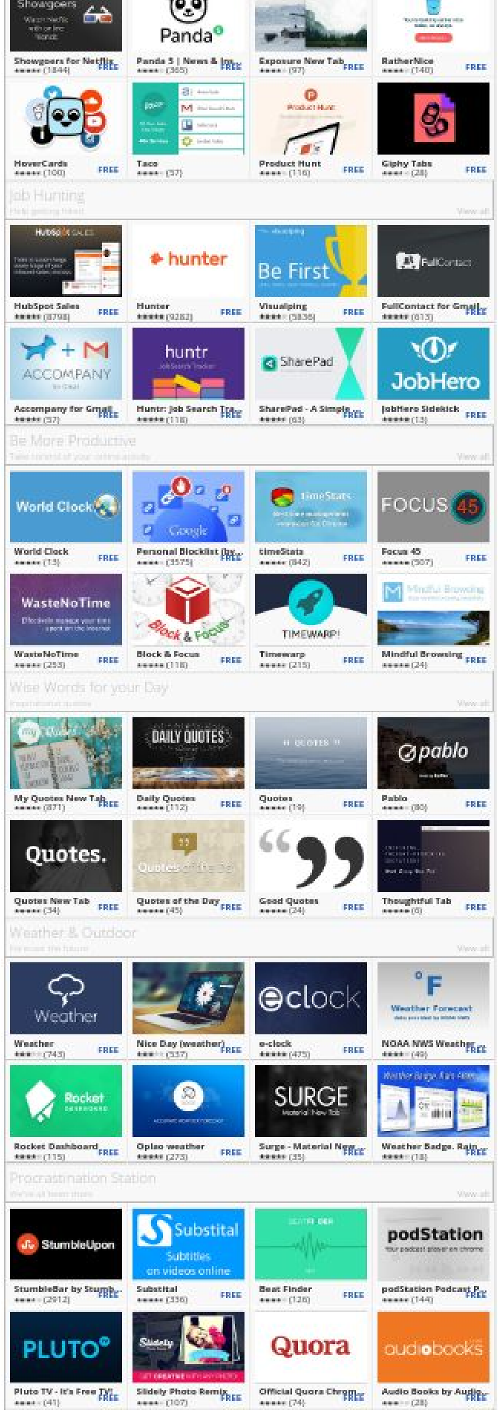
Capture Your Screen
Take screenshots and videos with ease
View all

Screencastify - Scree... (7554) FREE
Full Page Screen Capt... (4453) FREE
Nimbus Screenshot &... (3194) FREE
Diigo Web Collector -... (1145) FREE
OneNote Web Clipper (35337) FREE
Loom - Video Recorde... (3883) FREE
Joxi Full Page Screen... (532) FREE
Full Page Screenshot (280) FREE

Expand Your Social Circle
Connect, follow, share
View all

Pinterest Save Button (6889) FREE
Chrome IG Story (2393) FREE
Toolkit For Facebook (2538) FREE
Social Blade (462) FREE
Spell checker and Gra... (1316) FREE
Rapportive (2999) FREE
GIPHY for Chrome (196) FREE
Hootsuite Hootlet (1293) FREE

Personalize Chrome
Extensions that make Chrome yours
View all



Showgoers for Netflix (1844) FREE
Panda 5 | News & Ins... (365) FREE
Exposure New Tab (97) FREE
RatherNice (140) FREE
HoverCards (100) FREE
Taco (57)
Product Hunt (116) FREE
Giphy Tabs (28) FREE

Job Hunting
Help getting hired
View all

HubSpot Sales (8798) FREE
Hunter (9282) FREE
Visualping (5836) FREE
FullContact for Gmail... (613) FREE
Accompany for Gmail (57) FREE
Huntr: Job Search Tra... (118) FREE
SharePad - A Simple... (63) FREE
JobHero Sidekick (13) FREE

Be More Productive
Take control of your online activity
View all

World Clock (13) FREE
Personal Blocklist (by... (3575) FREE
timeStats (842) FREE
Focus 45 (507) FREE
WasteNoTime (253) FREE
Block & Focus (118) FREE
Timewarp (215) FREE
Mindful Browsing (24) FREE

Wise Words for your Day
Inspirational quotes
View all

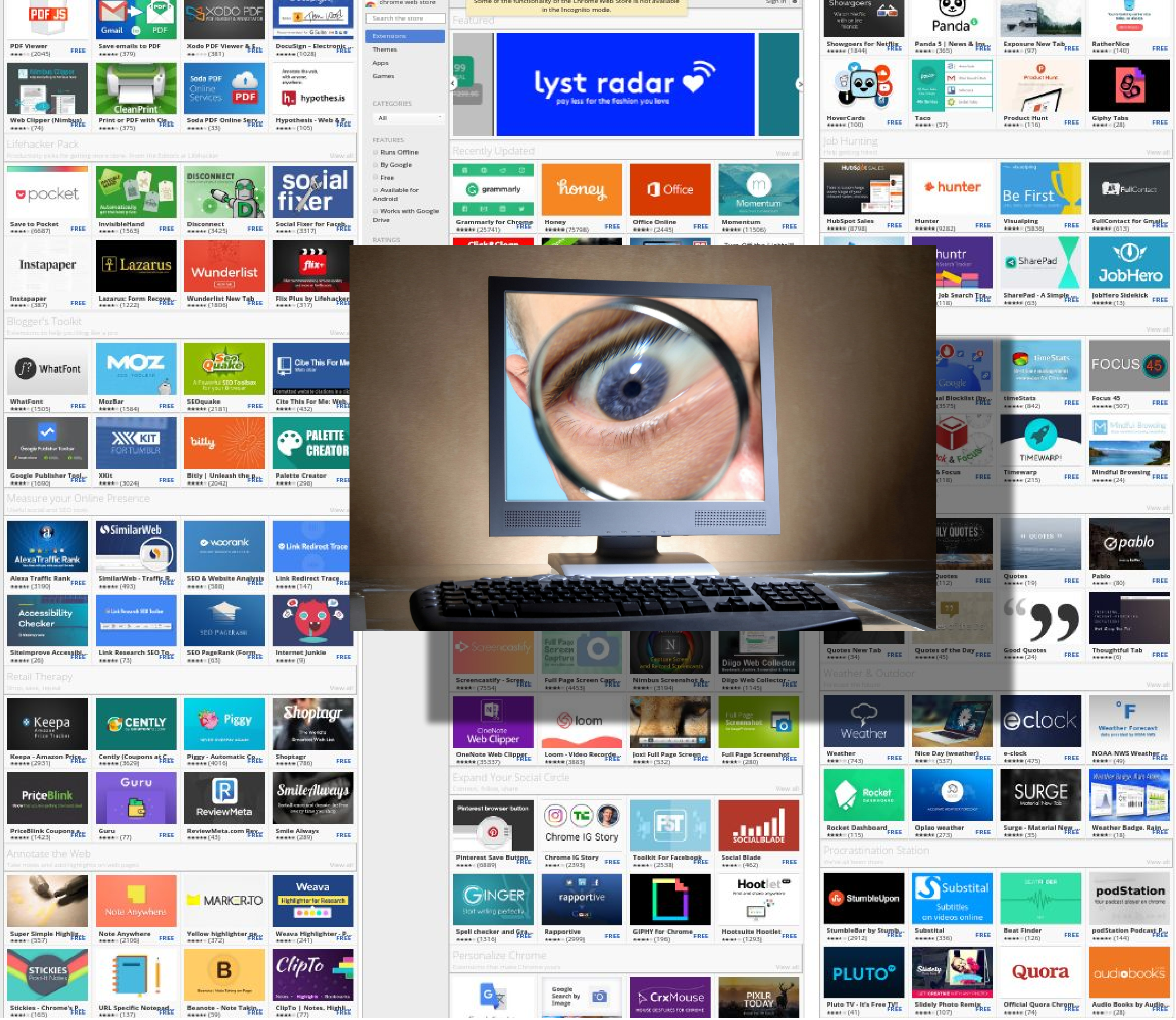
My Quotes New Tab (871) FREE
Daily Quotes (112) FREE
Quotes (19) FREE
Pablo (80) FREE
Quotes New Tab (34) FREE
Quotes of the Day (45) FREE
Good Quotes (24) FREE
Thoughtful Tab (6) FREE

Weather & Outdoor
Forecast the future
View all

Weather (743) FREE
Nice Day (weather) (537) FREE
e-clock (475) FREE
NOAA NWS Weather... (49) FREE
Rocket Dashboard (115) FREE
Oplao weather (273) FREE
Surge - Material New... (35) FREE
Weather Badge. Rain... (18) FREE

Procrastination Station
We've all been there
View all

StumbleBar by Stumb... (2912) FREE
Substital (336) FREE
Beat Finder (126) FREE
podStation Podcast P... (144) FREE
Pluto TV - It's Free TV! (41) FREE
Slidely Photo Remix (107) FREE
Official Quora Chrom... (74) FREE
Audio Books by Audio... (28) FREE


chrome web store
Featured
lyst radar
pay less for the fashion you love
Recently Updated
Lifehacker Pack
Blogger's Toolkit
Measure your Online Presence
Retail Therapy
Annotate the Web
Expand Your Social Circle
Personalize Chrome
Job Hunting
Weather & Outdoor
Procrastination Station
pocket
Instapaper
Lazarus
Wunderlist
social fixer
WhatFont
MOZ
SimilarWeb
Keepa
CENTLY
Piggy
Shoptagr
PriceBlink
Guru
ReviewMeta
grammarly
honey
Office
Momentum
loom
Chrome IG Story
SOCIALBLADE
GINGER
rapportive
Hootlet
CrxMouse
hunter
Be First
JobHero
FOCUS 45
TIMEWARP!
pablo
Weather
clock
SURGE
StumbleUpon
Substital
podStation
PLUTO
Quora
audiobooks
Panda
FREE

Overview

- Extension Basics
- Extension Privacy Risks
- HoneyPot Probe
- Detection Methodology
- System Design and Evaluation
- Conclusion and Discussion

How extensions work

- Additions to browser core functionality
- Powerful API based on permissions
    - Modification of active pages
    - Modification of requests / responses
    - Often access to all visited pages
    - Access to cookies
    - Access to previous history

Extension Privacy Risks

- Privacy leaks through
  - Modifications to the site: referrer
  - Request or response interception
  - Polling active tab
  - ...
- No unified way of detection
- Previews work:
  - Manual analysis
  - Leaking keywords, search traffic

Extension Privacy Mitigations

- Permissions can restrict access to sites
- Extensions often over-request access
- Only modest permissions required to leak history

Tracker Comparison

- On Websites:
  - Opt-in: Website owner
  - Opt-out: Ghostery

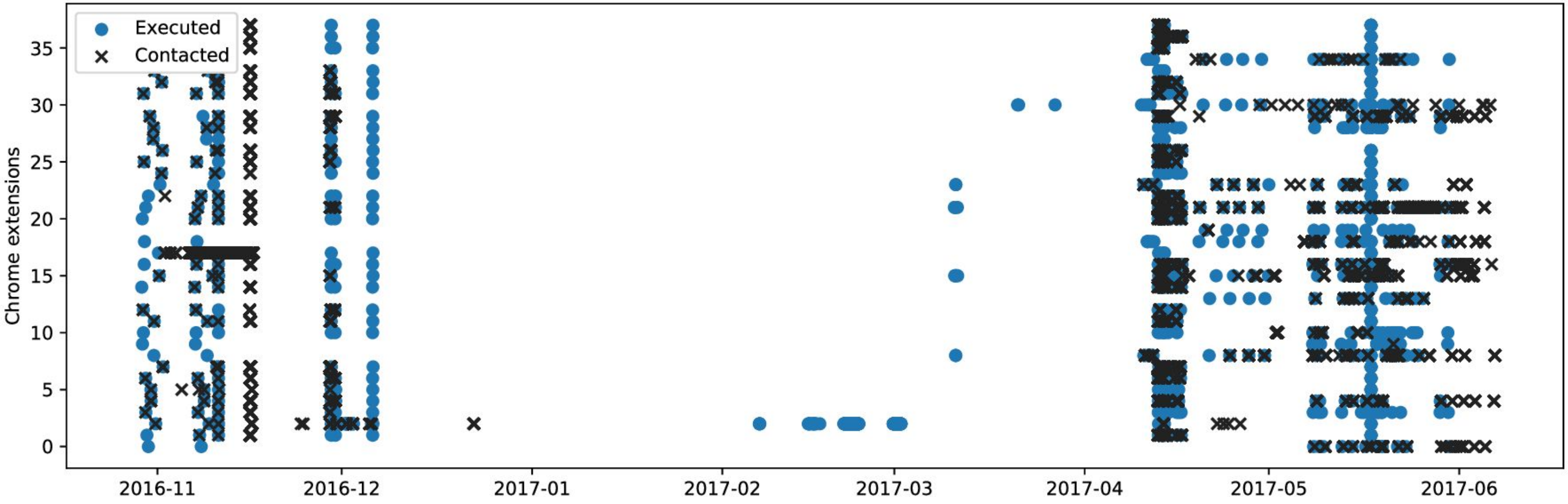
- In Extensions:
  - (typically) all websites
  - Implicit Opt-in through installation
  - No opt-out

“Is this an issue in practice?”

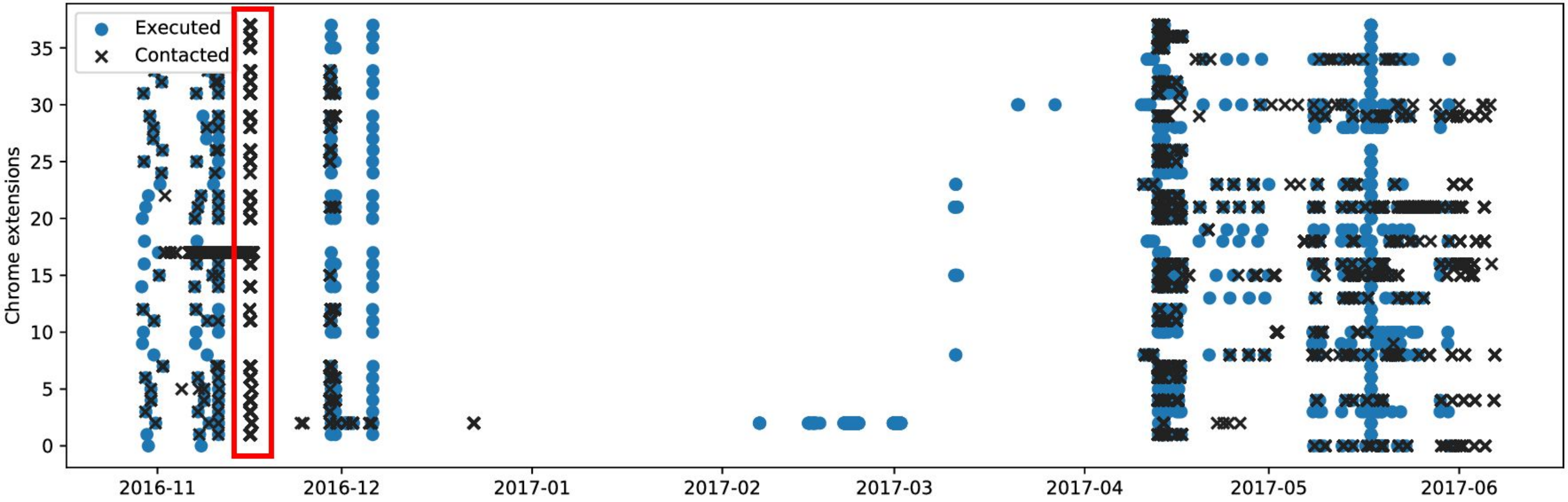
HoneyPot Probe

- Extensions run in a container
- Web and DNS local
- URLs unique to extension
- Public Internet only for other resources
- Browsing our website...
- ... which is also available on the public Internet

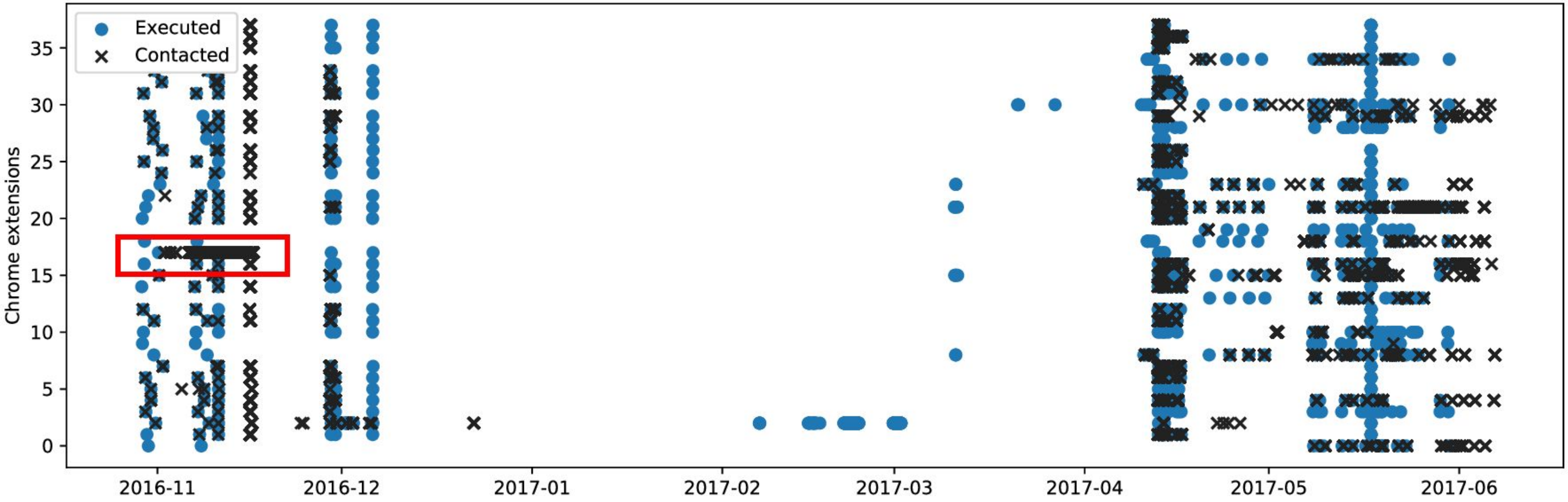
HoneyPot Probe



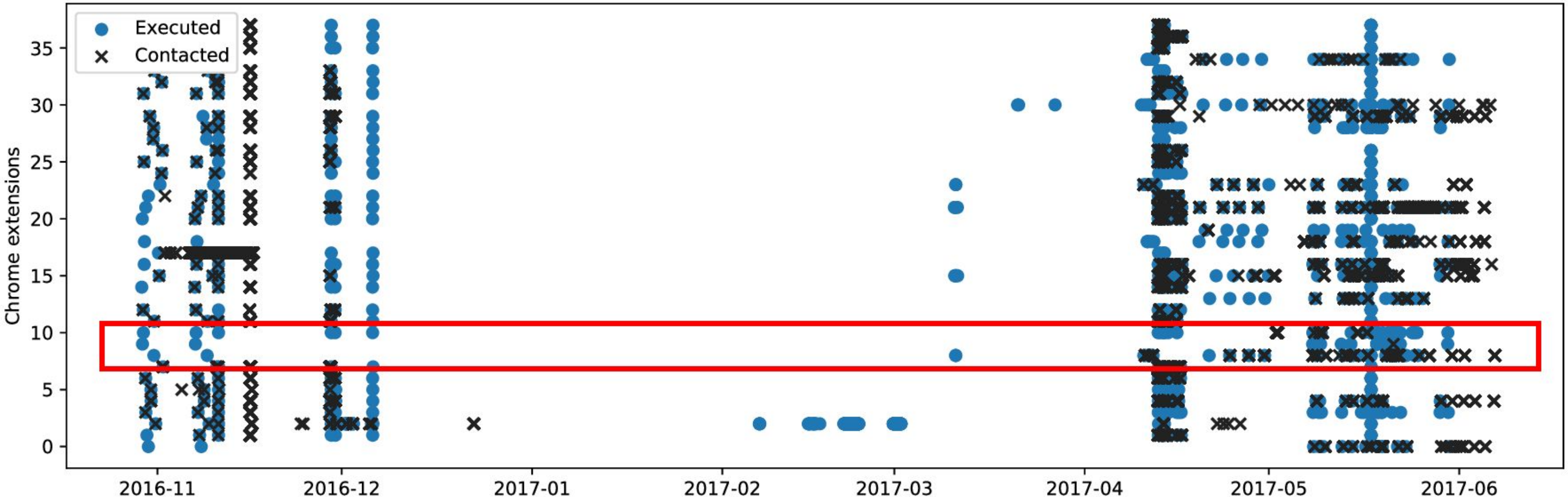
HoneyPot Probe



HoneyPot Probe



HoneyPot Probe



HoneyPot Incoming Connections

Extension Name	Installations	Connection Origin
Stylish - Custom themes	1,671,326	*.bb.netbynet.ru *.moscow.rt.ru *.spb.ertelecom.ru
Pop Up Blocker for Chrome	1,151,178	*.aws.kontera.com 176.15.177.229 *.bb.netbynet.ru
Desprotetor de Links	251,016	*.aws.kontera.com *.moscow.rt.ru *.bb.netbynet.ru

HoneyPot Probe

- Connections prove use of data
- Excluding VPN: 38 Extensions
- Connection often immediately after execution
- They leak immediately
- Indications for collaboration, no proof
- No malicious activity detected
- Motivation for automated detection system

Detection Methodology

Hypothesis: For tracking samples, sent data size should grow in relation to history provided to the extension.

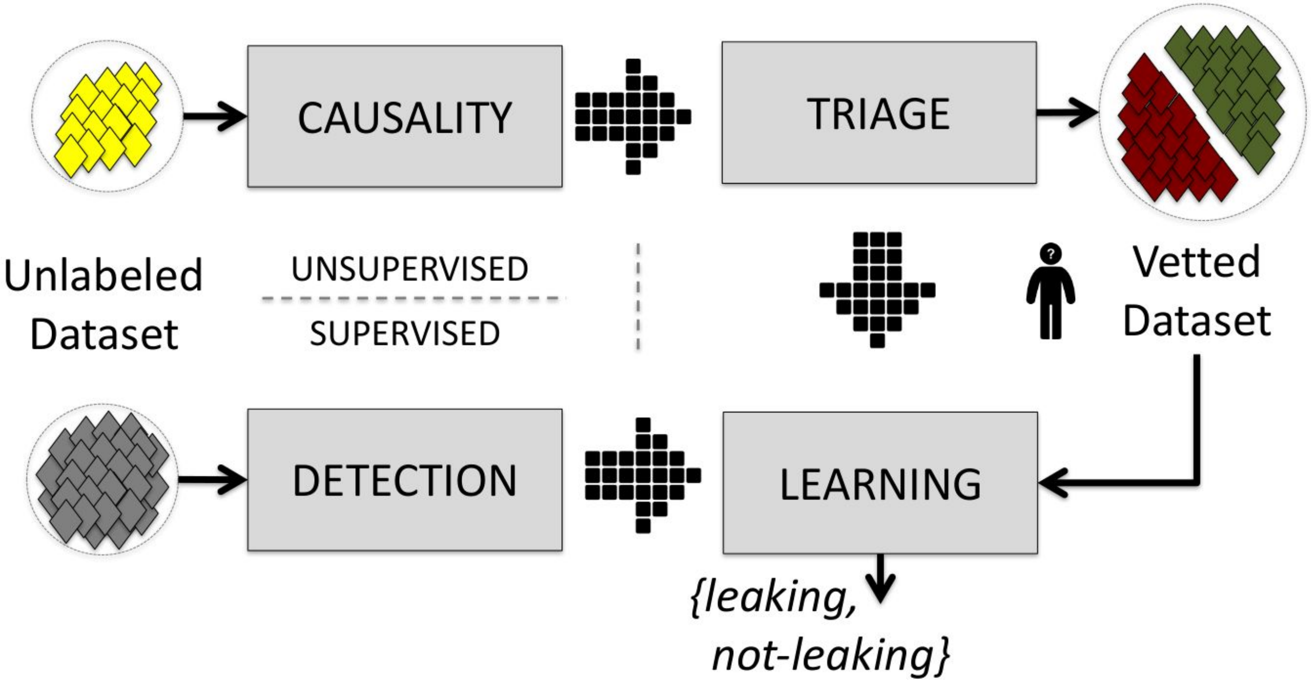
Ex-Ray Goals

- Robust Detection
  - Traffic obfuscation / encryption
  - Method of data collection / exfiltration
- Automated detection of leaks
- Large scale

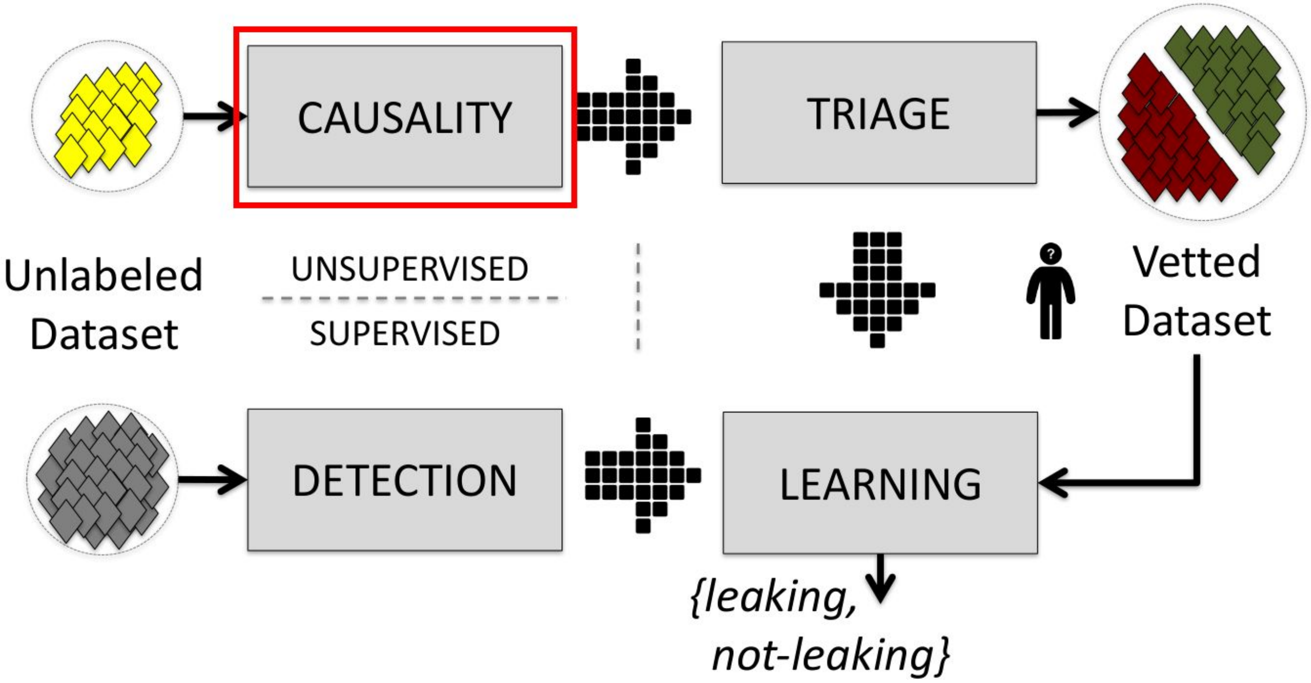
Detection Methodology

- Controlled environment
- Execution in multiple stages
- Vary size of browsing history
- Supervised and unsupervised methods

Detection Methodology



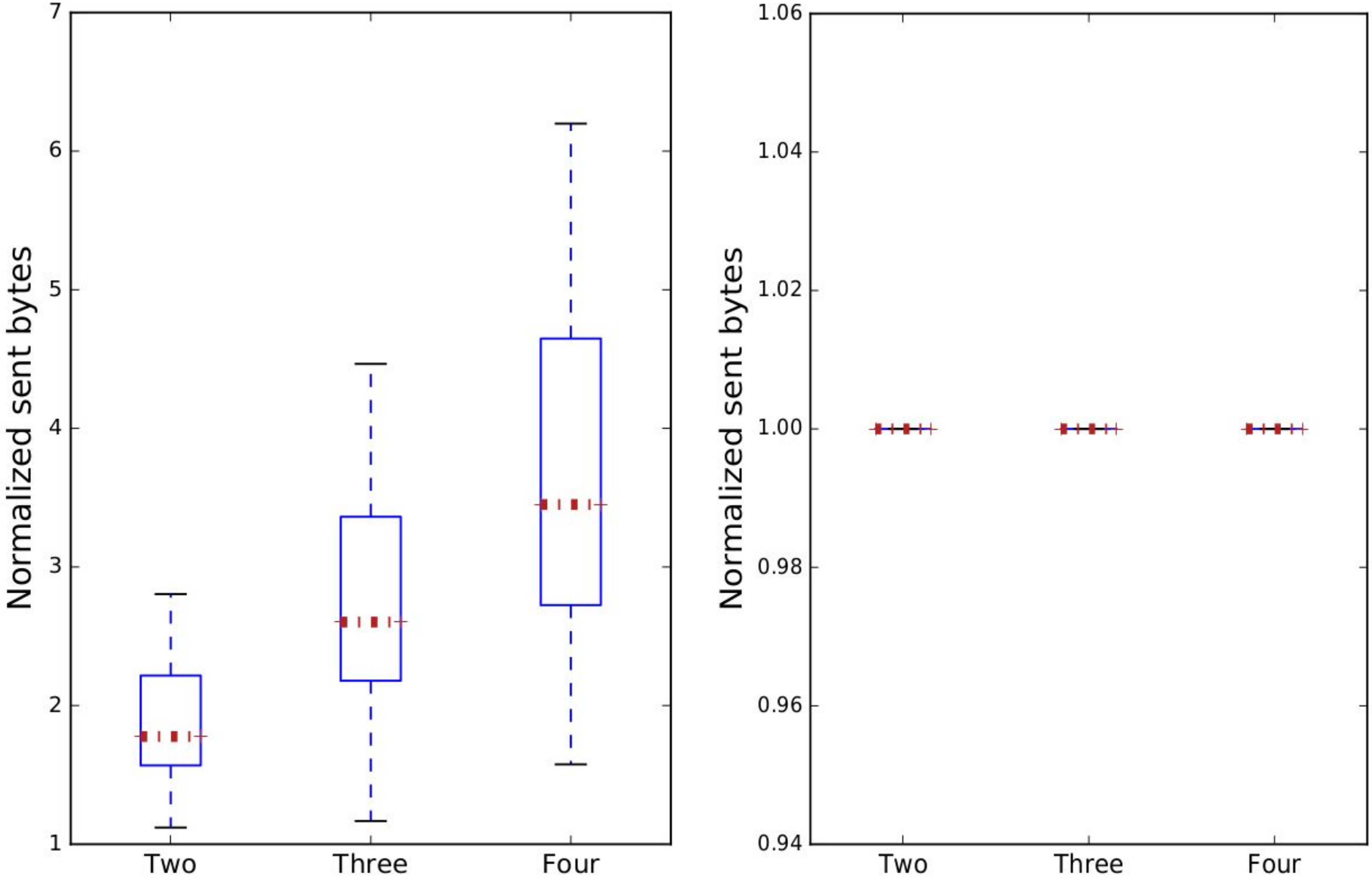
Detection Methodology



Causality

- Varying history as variable over stages
  - Stage 0: `example.com/example/index.html`
  - Stage 1: `example.com/example/<500characters>/index.html`
  - ...

- Expectations
  - Benign: no change
  - Otherwise: ?



(a) Tracking extension.

(b) Benign extensions.

Causality

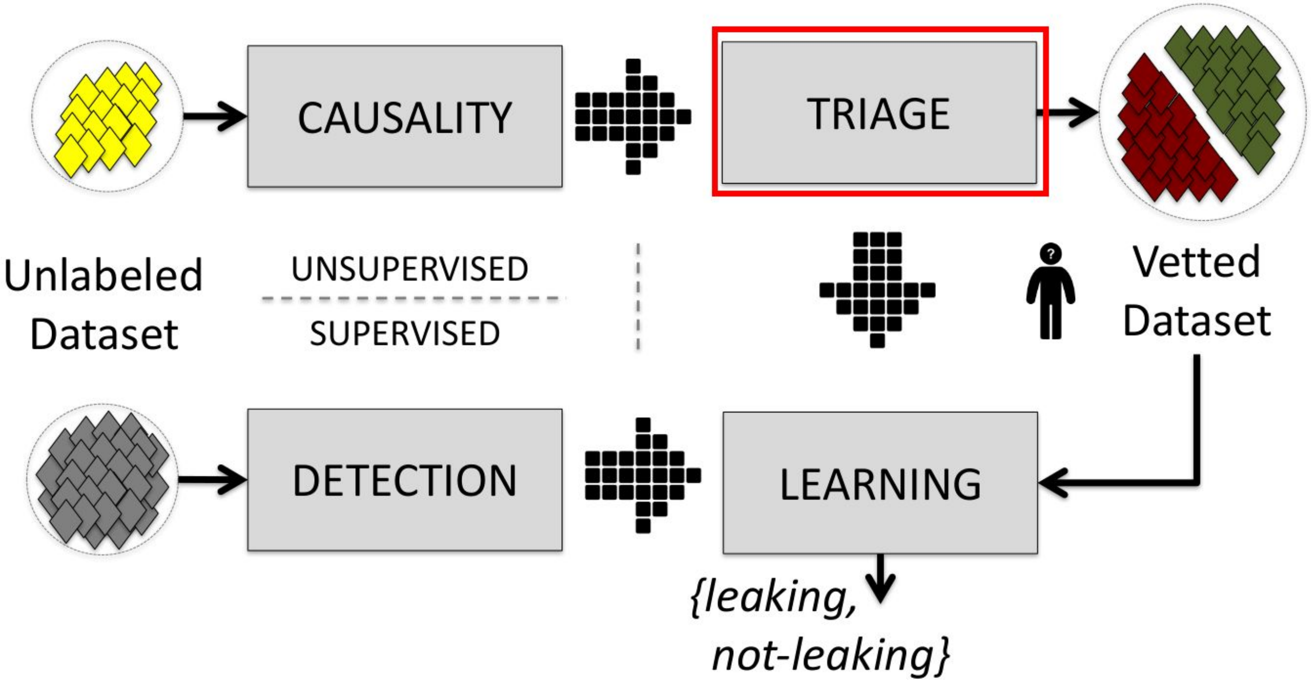
- Counterfactual analysis
- Input variable: size of history
- Output variable: <data sent, destination> tuples
- Invariants of trackers
- Goal: find deterministic tracking
- Supervised method: trained on benign and leaking datasets

Causality

Three steps

1. Minimum intercept: threshold
2. Minimum slope: increase
3. Level of confidence: proximity to model

Detection Methodology



Triage

- Quantify leakage
- Prioritize extensions
- Supports human analyst in prioritizing extensions

Triage

- L: number of leaked URLs between experiments
- |*si*|, |*sj*|: number of bytes sent to domain
- τ: expected threshold for increase

$$\mathrm{L}(s_i, s_j) = \frac{|s_j| - |s_i|}{\tau}$$

Triage

- Score: Likelihood of a leak
- s: transition between stages (i=>j)

$$\mathrm{score}(x) = \prod_{s} e^{\mathsf{L}(s)}$$

Triage

$$\text{leak}(x) = \begin{cases} \texttt{not-leaking} & \text{if } score(x) \leq 1 \\ \texttt{possibly-leaking} & \text{if } 1 < score(x) \leq 100 \\ \texttt{likely-leaking} & \text{otherwise.} \end{cases}$$

- Result: indicators for manual analysis

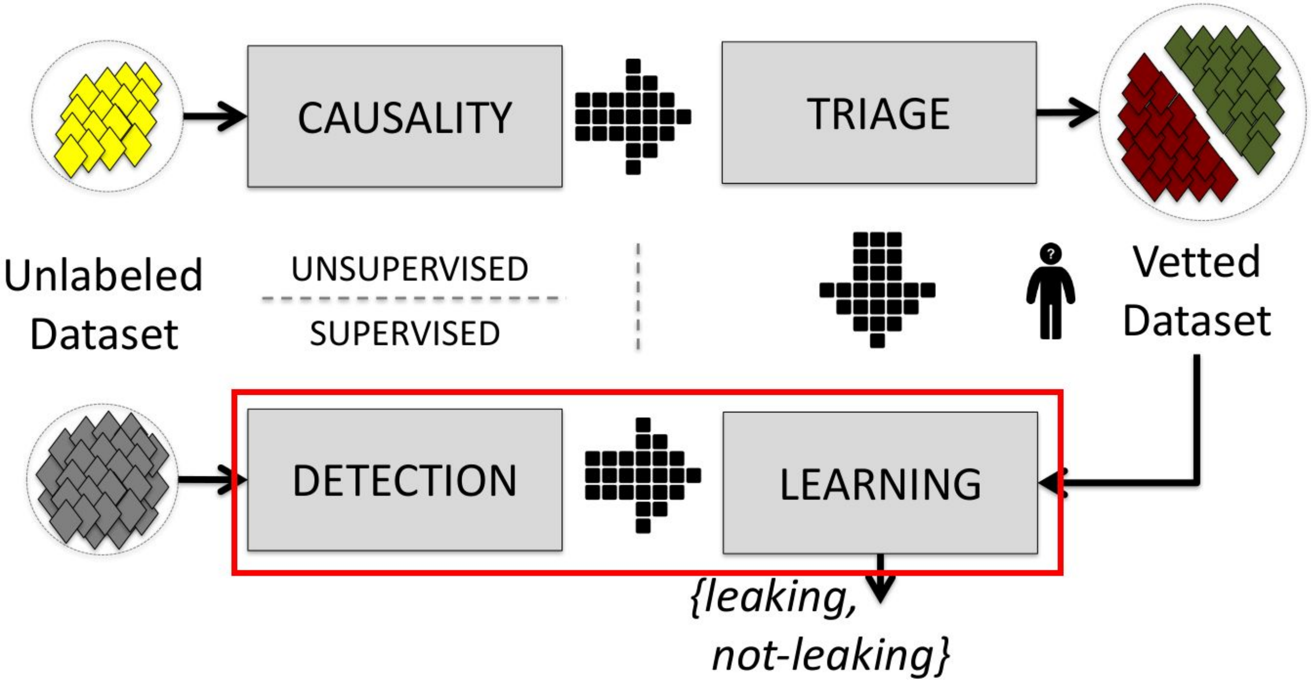
Triage Samples: Leak

```
QR Code Generator
    4e+18  connectionstrenth.com
   394.88  a.pnamic.com
    28.22  eluxer.net
     4.48  rules.similardeals.net
     1.16  code.jquery.com
```

Triage Samples: Benign

```
Bible Quote of the Day
     1.00   www.gstatic.com
     1.00   chromium-i18n.appspot.com
     1.00   ssl.gstatic.com
     1.00   localhost
     0.67   www.google.com
```

Detection Methodology



Behavioral Detection

- Based on previously flagged extensions
- Clang Libtooling instrumentation
  - C++ source code rewriting
  - 11,132 function trace points
- API call analysis
- Input: n-grams of API calls

Evaluation: Causality

- Crawled store for extensions > 1,000 installations
- 10,691 Extensions total
- 212 flagged: 1.9%
- 184 manually verified as leaking
- 28 wrongly identified
- False Detection Rate: 0.27%
    - Flagged due to ads
    - Possible improvement: increase # stages

Evaluation: Behavioral

- Best parameters:
  - n-gram: 2
  - F1 score: 96.43%
- Distinguishing calls:
  - URL manipulation
  - JavaScript manipulation
- Most distinguishing sequence:
  - extensions.browser.extension_prefs.GetExtensionPref()
  - chrome.browser.extensions.shared_user_script_master .GetScriptsMetadata()

Noteworthy Samples: Causality

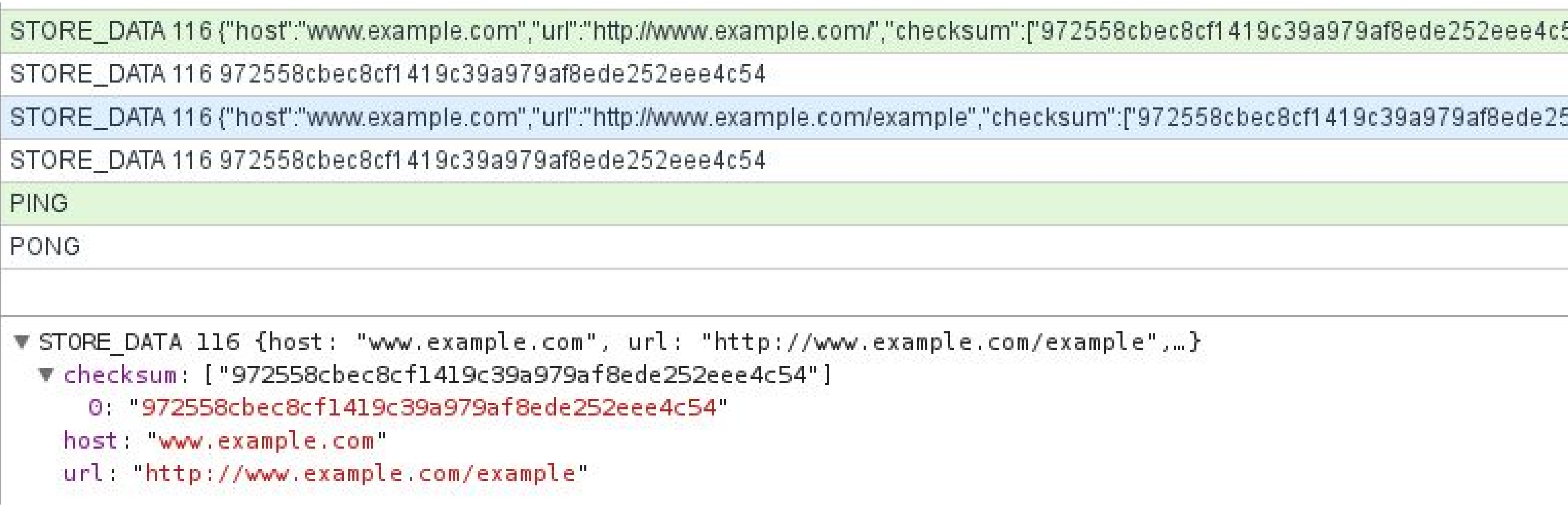
- Not detectable by state-of-the-art leakage detection systems
- Previously unknown leakage channels
    - Strong Encryption
    - Unsupported Protocol

Web of Trust (WOT)

- Provides crowd-sourced "trust" ranking
- 1.2M installations
- Extension received media coverage for selling user data
- RC4 encryption (See `crypto.js` file)
- Can be implemented similarly to Google Safe Browsing (offline)

CouponMate

- WebSockets: Protocol not supported by previous systems
- Protocol growing in popularity: 0.96%



```
STORE_DATA 116 {"host":"www.example.com","url":"http://www.example.com/","checksum":["972558cbec8cf1419c39a979af8ede252eee4c5
STORE_DATA 116 972558cbec8cf1419c39a979af8ede252eee4c54
STORE_DATA 116 {"host":"www.example.com","url":"http://www.example.com/example","checksum":["972558cbec8cf1419c39a979af8ede25
STORE_DATA 116 972558cbec8cf1419c39a979af8ede252eee4c54
PING
PONG

▼ STORE_DATA 116 {host: "www.example.com", url: "http://www.example.com/example",…}
  ▼ checksum: ["972558cbec8cf1419c39a979af8ede252eee4c54"]
      0: "972558cbec8cf1419c39a979af8ede252eee4c54"
    host: "www.example.com"
    url: "http://www.example.com/example"
```

Possible remediations

- Stores should analyze extensions to warn users
- Implement API to inspect background traffic
- Invasive tracking as single purpose rule violation

Conclusions

- Robust detection method for privacy leaks
- Prototype: Ex-Ray
- Supervised and Unsupervised methods
- 10,691 extensions analyzed
- 212 flagged
- Found two novel leaking channels in use

Thank you for your attention

Questions?

Paper and Data:

https://goo.gl/nezKGp