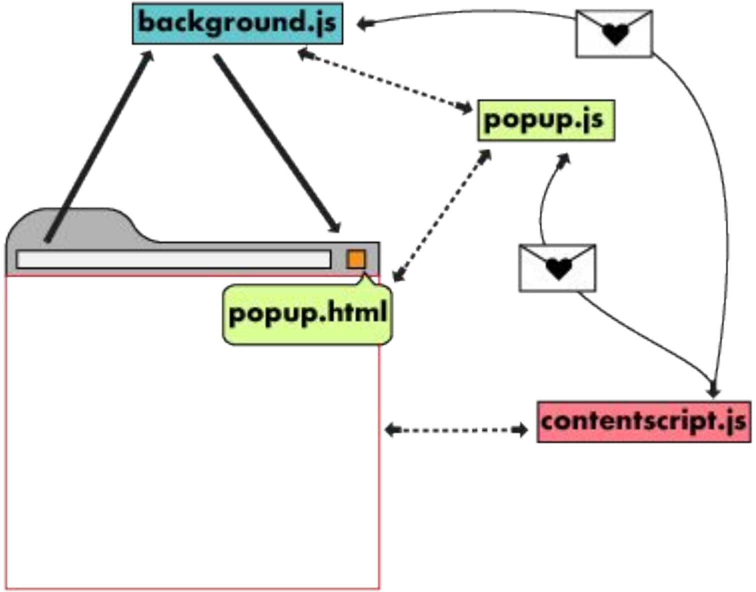
Trends and Lessons from Three Years Fighting Malicious Extensions

Nav Jagpal, Eric Dingle, Jean-Philippe Gravel, Panayiotis Mavrommatis, Niels Provos, Moheeb Abu Rajab, and Kurt Thomas, Google

Motivation

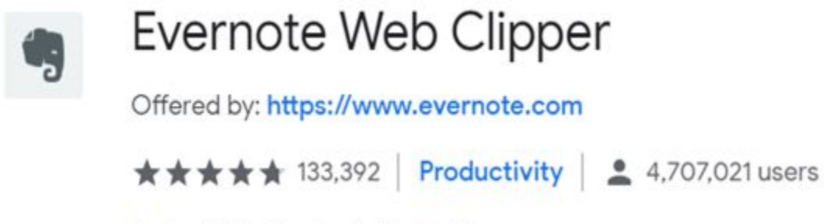
Chrome Extensions – What & Why?

- Small add-ons.
- Enhance browser experience.
- Chrome Extensions - Distributed by Chrome Web Store.



Source: https://developer.chrome.com/extensions/overview

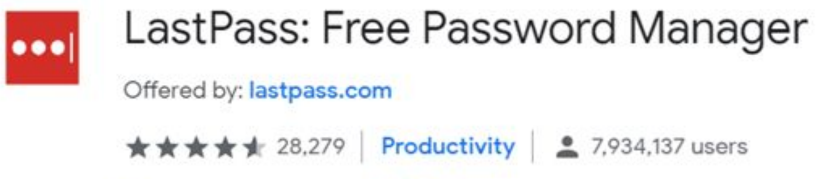
Extensions – Utility



Evernote Web Clipper

Offered by: https://www.evernote.com

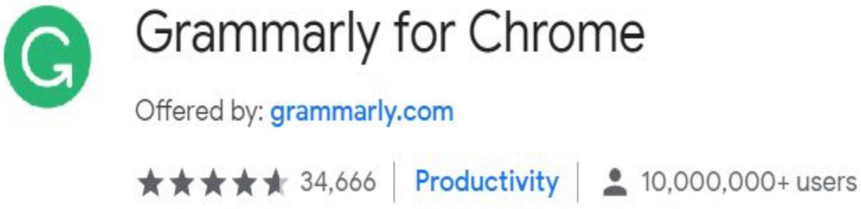
★★★★⯪ 133,392 | Productivity | 4,707,021 users



LastPass: Free Password Manager

Offered by: lastpass.com

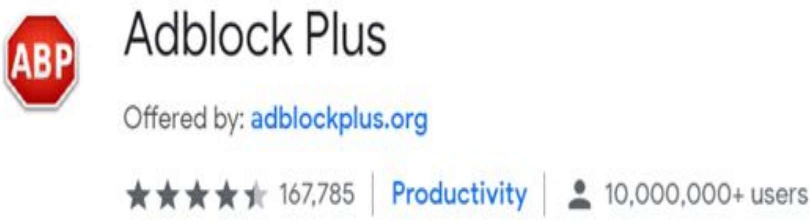
★★★★⯪ 28,279 | Productivity | 7,934,137 users



Grammarly for Chrome

Offered by: grammarly.com

★★★★⯪ 34,666 | Productivity | 10,000,000+ users

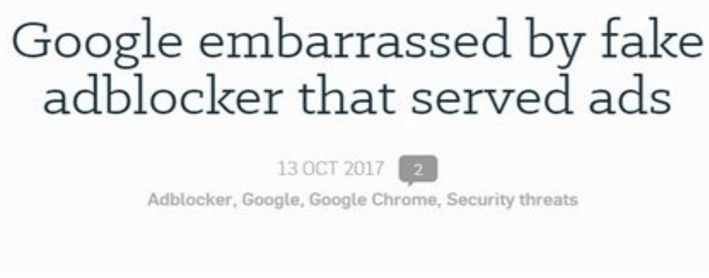


Adblock Plus

Offered by: adblockplus.org

★★★★⯪ 167,785 | Productivity | 10,000,000+ users

While at the same time…



Google embarrassed by fake adblocker that served ads

13 OCT 2017 2

Adblocker, Google, Google Chrome, Security threats

Source: https://nakedsecurity.sophos.com/2017/10/13/google-embarrassed-by-fake-adblocker-that-served-ads/

Goal

- ➢ Block newly submitted malicious extensions before publishing.
- ➢ Take down existing malicious extensions present in the store.

Topics Discussed in this Research Study

Study on roughly 100,000 extensions submitted to Chrome Web Store in between January, 2012 - 2015.

➢ Design & implementation of security framework - WebEval.

➢ Trends of malicious extension in the wild.

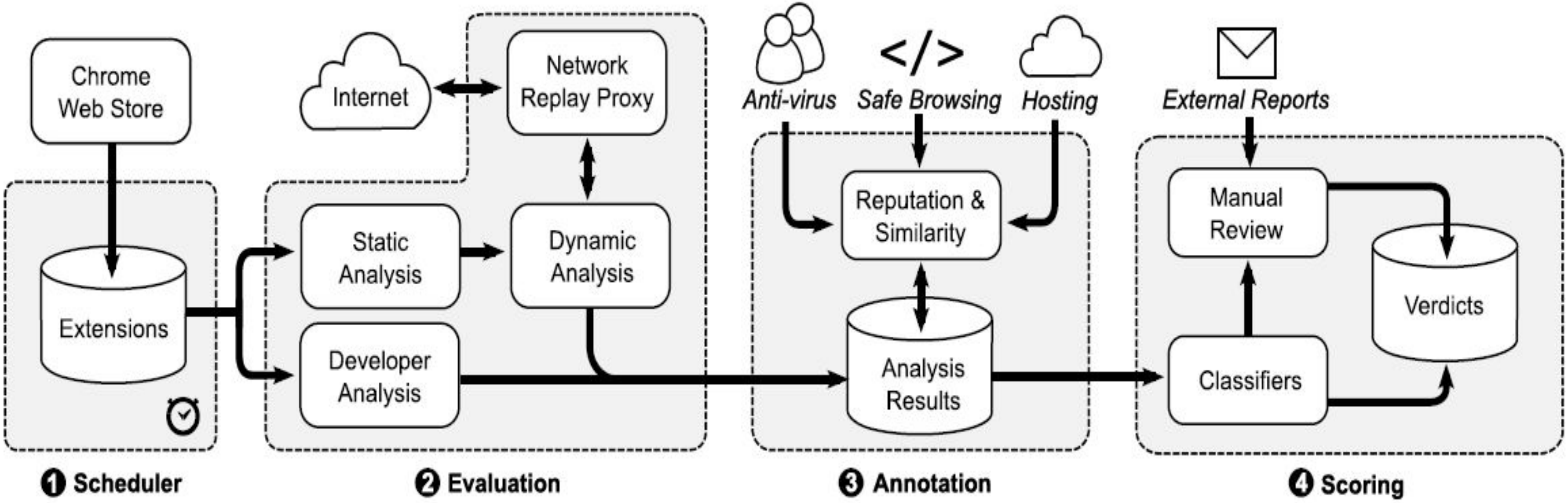
➢ Impact of undetected extensions

WebEval

Design Constraints

1. Minimum malware installs.
2. Simplified human verification.
3. Time – constrained.
4. Comprehensible, historical reports.
5. Tolerant to feature drift.

System Flow


Chrome Web Store
Extensions
Internet
Network Replay Proxy
Static Analysis
Dynamic Analysis
Developer Analysis
Anti-virus
Safe Browsing
Hosting
Reputation & Similarity
Analysis Results
External Reports
Manual Review
Verdicts
Classifiers
❶ Scheduler
❷ Evaluation
❸ Annotation
❹ Scoring

Evaluation - Extension Execution Framework

Static Analysis

- ➢ Permission & content script
- ➢ Code obfuscation
- ➢ Files & directory structure

Dynamic Analysis

- ➢ Behavioral Suites
- ➢ Network events
- ➢ Chrome & DOM API calls

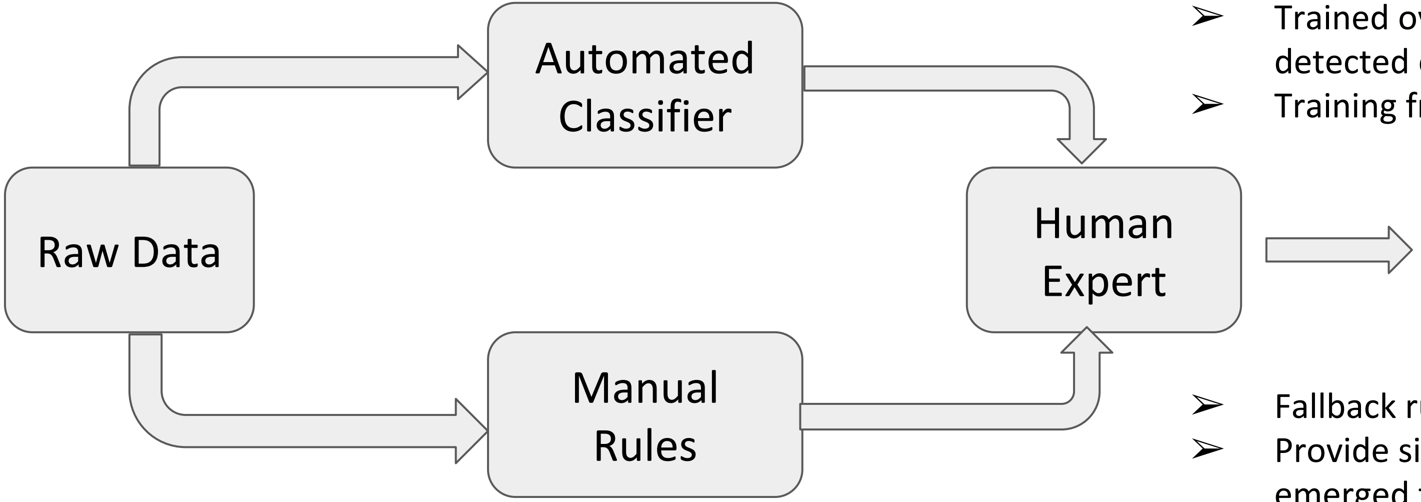
Developer Analysis

- ➢ Developer’s last login
- ➢ Developer’s registered email domain
- ➢ Developer’s age

Extension Analysis

- ➢ Total no. of installs
- ➢ Total no. of users rating the extension
- ➢ Average rating of extension

Scoring Extensions



- ➢ 20 million features
- ➢ Trained over all previously detected extension
- ➢ Training frequency - daily

- ➢ Fallback rules
- ➢ Provide signals for newly emerged threats

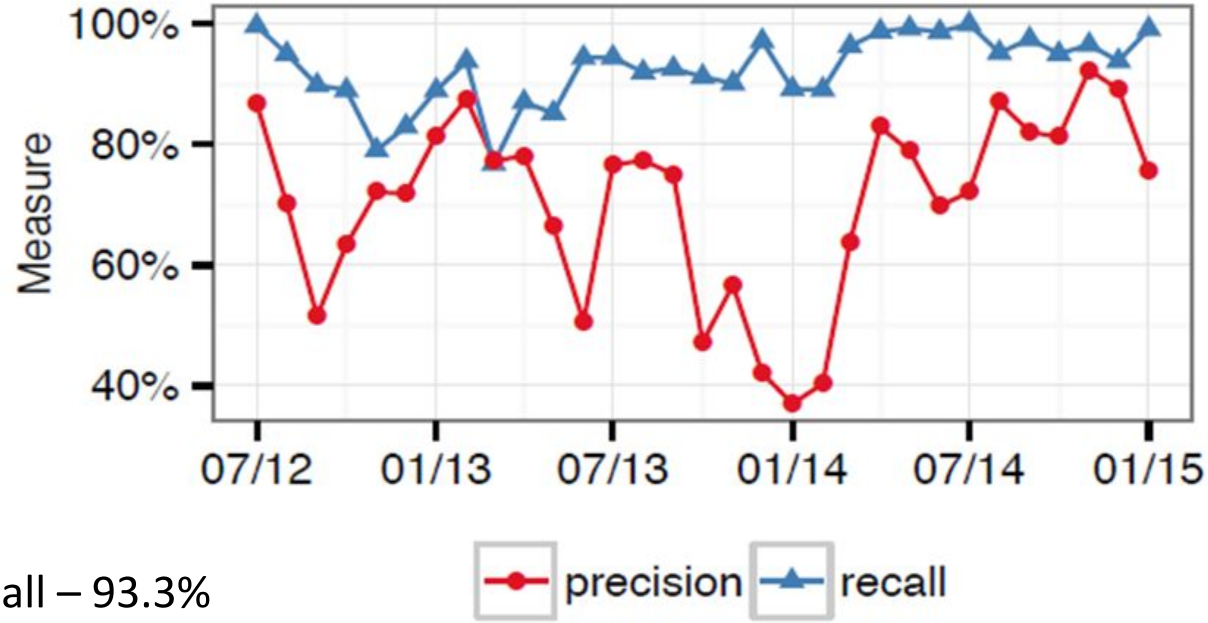
Decision = {Block, Take Down, Good to Go}

Evaluation Dataset

Evaluation Window	January, 2012 - 2015
Total Extensions Reviewed	99,818
Total Malicious Extension Found	9,523 (9.4% of all extensions)
Total Malicious Developers Found	2,339
Total Extensions Manually Reviewed	10,120
Extensions Scan Rate	19,000/day (Approx.)

Source:https://cdn.onlinewebfonts.com/svg/img_510380.png

Accuracy - Precision & Recall



Overall Recall – 93.3%

Overall Precision – 73.7%

Why Human Experts?

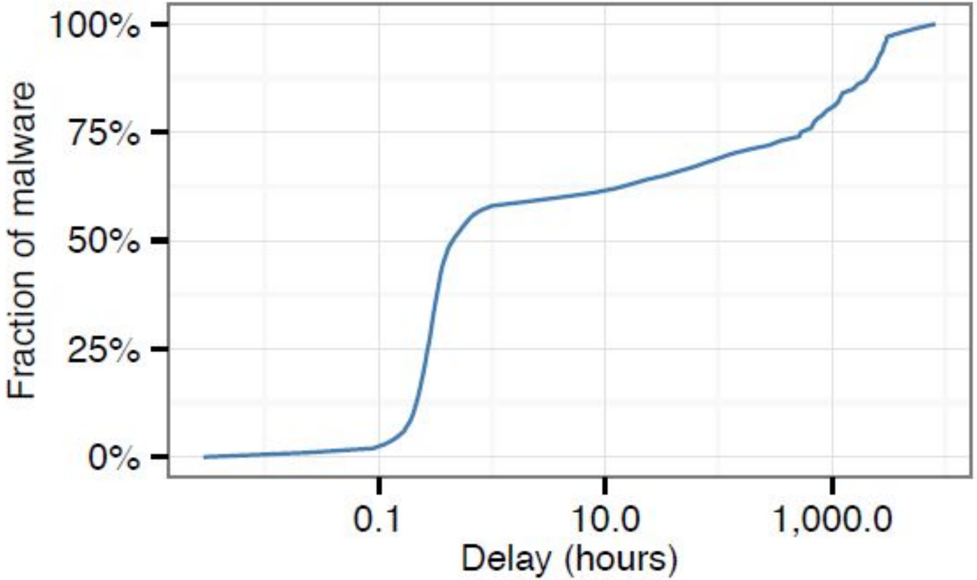
- ➢ Reduce false-positives & false negatives.
- ➢ Adaptation to new threats.
- ➢ Live deployment environment - requires additional check.
- ➢ Time taken to decide - 2.75 minutes per extension.

Key Indicators to Detect Malicious Extensions

- ➢ Modification of CSP headers.
- ➢ Uninstalling other extension.
- ➢ Preventing uninstall of extensions.
- ➢ Chrome & DOM API calls.

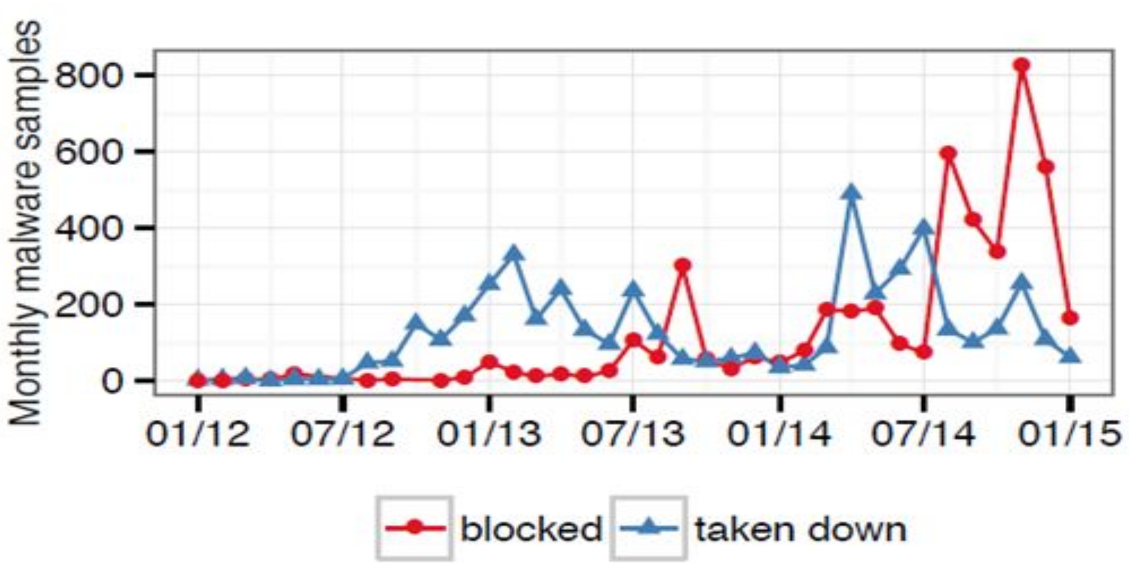
Permissions - not really.

Detection Latency



Median of Detection Frame: 25 Minutes

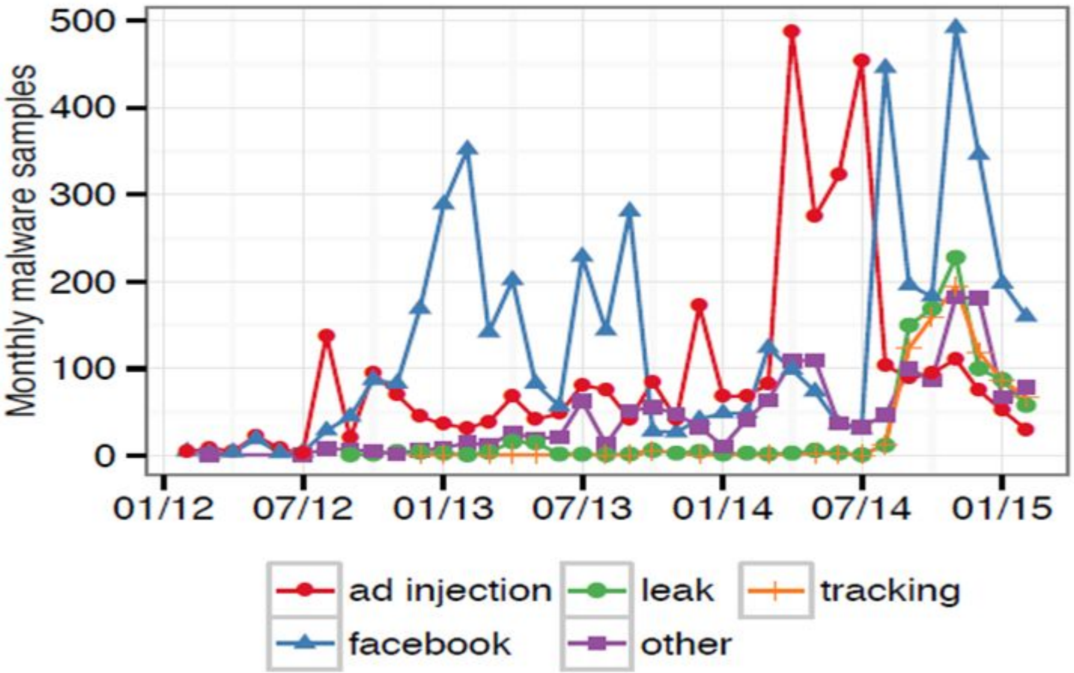
Moving Towards Proactive Approach



Overall Blocked/Taken Down Extensions

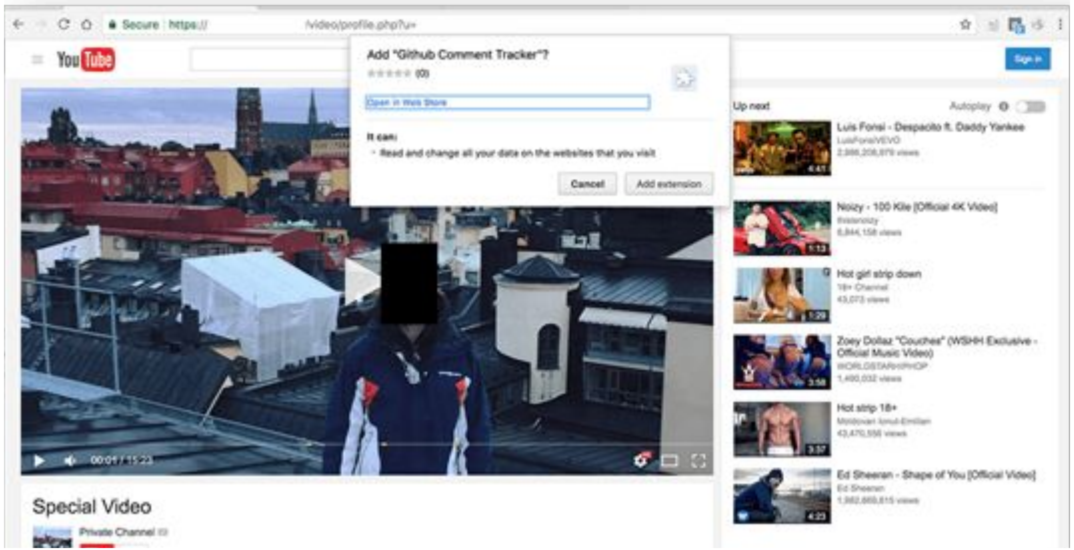
Trends of Extension Abuse

Different Malicious Extensions Detected in the Wild



Prominent Extension Abuses

Facebook session hijacking



[redacted]

Add "Github Comment Tracker"?

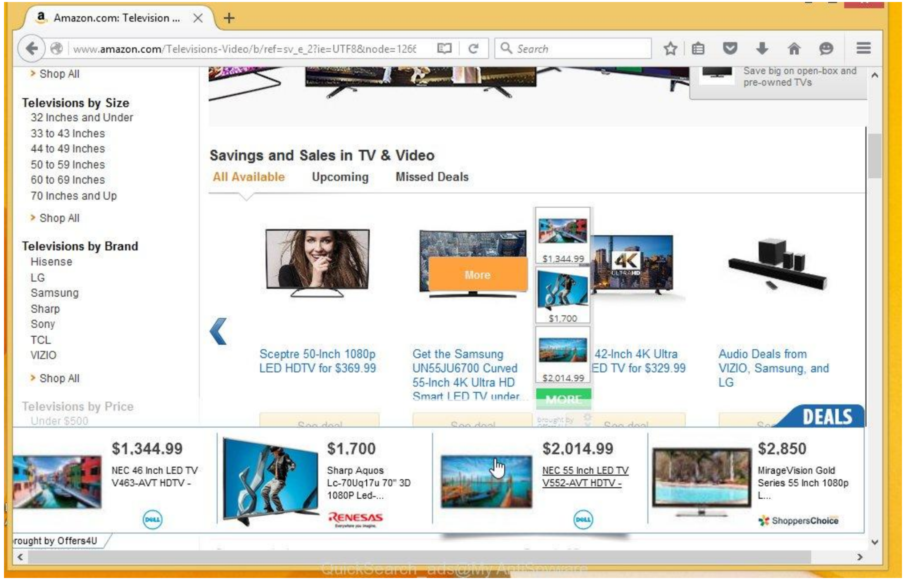
It can:

- Read and change all your data on the websites that you visit

Source:https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07171223/170831-facebook-malware-3.png

Prominent Extension Abuses

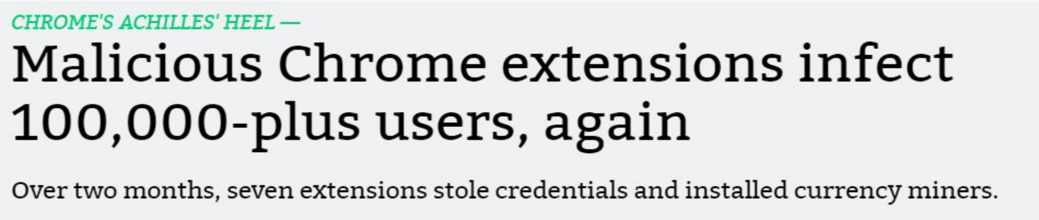
Ad injecting extensions


Amazon.com: Television ...
www.amazon.com/Televisions-Video/b/ref=sv_e_2?ie=UTF8&node=126
Search
Shop All
Save big on open-box and pre-owned TVs
Televisions by Size
32 Inches and Under
33 to 43 Inches
44 to 49 Inches
50 to 59 Inches
60 to 69 Inches
70 Inches and Up
Shop All
Televisions by Brand
Hisense
LG
Samsung
Sharp
Sony
TCL
VIZIO
Shop All
Televisions by Price
Under $500
Savings and Sales in TV & Video
All Available
Upcoming
Missed Deals
Sceptre 50-Inch 1080p LED HDTV for $369.99
More
Get the Samsung UN55JU6700 Curved 55-Inch 4K Ultra HD Smart LED TV under...
$1,344.99
$1,700
$2,014.99
MORE
42-Inch 4K Ultra ED TV for $329.99
Audio Deals from VIZIO, Samsung, and LG
DEALS
$1,344.99
NEC 46 Inch LED TV V463-AVT HDTV -
$1,700
Sharp Aquos Lc-70Uq17u 70" 3D 1080P Led-...
RENESAS
$2,014.99
NEC 55 Inch LED TV V552-AVT HDTV -
$2,850
MirageVision Gold Series 55 Inch 1080p L...
ShoppersChoice
rought by Offers4U
QuickSearch_ads@MyAntiSpyware

Source:http://www.myantispyware.com/wp-content/uploads/2016/02/QuickSearch_ads.jpg

Other Pertinent Threats

- Cryptocurrency miner.
- Banking thefts.
- Search leakage.
- User tracking.



CHROME'S ACHILLES' HEEL —

Malicious Chrome extensions infect 100,000-plus users, again

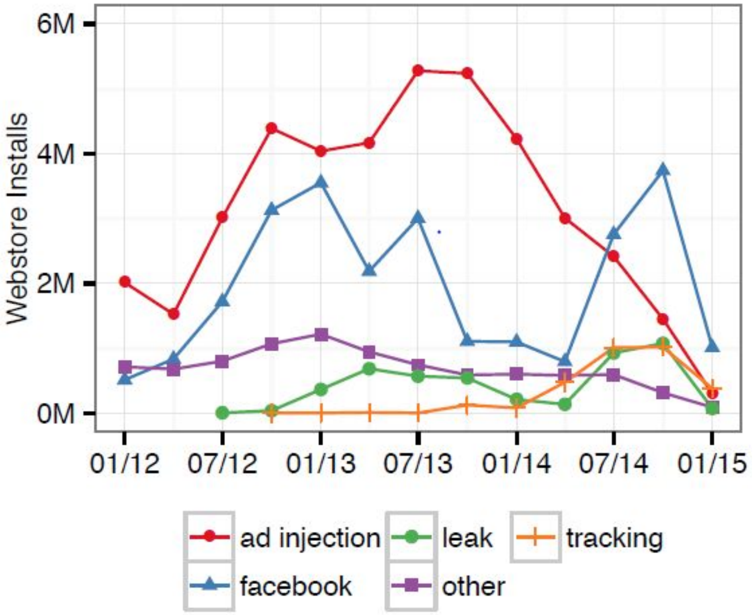
Over two months, seven extensions stole credentials and installed currency miners.

Source:
https://arstechnica.com/information-technology/2018/05/malicious-chrome-extensions-infect-more-than-100000-users-again/

Impact of Malicious Extensions

False - Negatives

- ➢ Approx. 100 extensions - affected 50 million users.
- ➢ Suggestion: Proactive approach.



Lessons Learned

- ➢ Extensive abuse different from malicious binaries.
- ➢ Monetization - driving force.
- ➢ Tools required to handle new, unforeseen threats.

Limitations

- ➢ Testing Extensions in Sandboxed Environment - not favorable.
- ➢ Chrome Lockdown Policy - way to bypass policy exists.
- ➢ Human resources - issue in scaling such systems.

Conclusion

- Identified & reported 96.5% – between January 2012 – 2015.
- 50% extensions – reported within 25 minutes.
- Human experts – integral to framework.
- False-negatives can have drastic impact.
- Evolutionary trends of extension abuse.
- Key challenges while detecting in live deployment environment.

Image Source:
http://www.iconarchive.com/download/i98233/dakirby309/simply-styled/Chrome-Web-Store.ico

Questions?