WildExtensions
Discovering and Analyzing Unlisted Chrome Extensions

Aidan Beggs - NC State
Alexandros Kapravelos - NC State
Browser Extensions

● HTML + Javascript
● “Small software programs that customize the browsing experience” [1]
● Access to a privileged API
  ○ Permissions granted by user upon installation
  ○ Clearly, everyone reads the permissions they’re granting...

AdBlock

Add "AdBlock"?

It can:
Read and change all your data on the websites you visit
Display notifications

- Pretty reasonable permissions?
Unlisted Extensions

- Work similarly to unlisted YouTube videos
- Unlisted extensions are still hosted officially by Google
  - Reviews and user install count are also still maintained by Google
- Cannot find extensions via a search of the web store
  - Used to support direct installation of extensions from websites: “inline installation”
  - Inline extension installations disabled due to security concerns
- Primary focus of paper
  - Finding and analyzing unlisted extensions in the wild
“ProMediaConverter Promotions”

ProMediaConverter Promotions
Offered by: https://www.promediaconverter.com
★★★★★ 0 | Productivity | 94,403 users

No results for "ProMediaConverter Promotions"
Make sure all words are spelled correctly, or try a different search.
“ProMediaConverter Promotions”

- Still pretty reasonable permissions?
Advertisement Scams
Extension Advertisement Scams
window.noMoneyLink = "https://easyfileconverter.net/go/base2.php?id=2";
window.noMoneyLink2 = "https://easyfileconverter.net/go/base2.php?id=2";
window.offers = [{"url": "https:\/\/easyfileconverter.net\/go\\/base2.php?id=5","id": "1hfibgclamffnddoicjmoopmgomknmb","type": "propel"},
{"url": "https:\/\/easyfileconverter.net\/go\\/base2.php?id=3","id": "afdckneponhndpfpjdmphnnhnnfopjlbe","type": "propel"},
{"url": "https:\/\/easyfileconverter.net\/go\\/base2.php?id=2","id": "AFW","type": "iac"}];
window.se_offer = "http://typ.navigateto.net/go/affredirectimplementation_id=aff555-ty-nf&offer_id=1029&aff_id=84&source=googlecancel&aff_sub5=converter_&sendToWebstore=true&retry=1";
window.is_mac = false;

ClassifiedsNearMe Promos
Offered by: https://www.classifiedsnearme.com

⭐⭐⭐⭐ 0 | Search Tools | ⚽ 14,955 users
Duplicate Extensions

- Multiple extensions that seem to be the same extension
Loved it
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

love it
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

Great
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

great
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

great
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

good
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

good
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

good
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

Just as for others here it changed the searches in google, got more adds than search results. Don't add this to your chrome!

Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

do the ads go away after the extension is uninstalled, or is it more akin to a virus?

Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

Thank you for the heads up!

Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

A Google User
Jan 3, 2019

good
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

No longer works on YouTube, so... kinda useless for me.

Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

https://ytmp3.co/ try that bro you can convert ur youtube videos or music

Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse

A Google User
Jan 3, 2019

good
Was this review helpful?  O  Yes  O  No  Reply | Mark as spam or abuse
• Still pretty reasonable permissions?
What can malicious extensions do?

- Steal user information
  - Emails
  - Passwords
  - Credit card information
  - Etc.

- Advertisement injection
  - Replace existing advertisements with advertisements hosted by extension
Challenges

- How to automate finding unlisted extensions?
  - In malicious extension maker’s best interest to make automation as hard as possible
- Unfortunately, extension links are often obfuscated
  - How to bypass this?
Automating the process

- Use a headless web browser that evaluates JavaScript (PhantomJS)
  - Let the web browser handle de-obfuscation
- Search static web archives for remnants of inline extension
  - &lt;link rel="chrome-webstore-item" href="https://chrome.google.com/webstore/detail/itemID"&gt;
- Navigate ads by hand
Extensions as a backdoor

- Not overtly malicious, still problematic
- Extension used as a logic bomb?
  - Benign now, but may be leveraged at any time by a malicious agent to induce malicious behaviour
- Universal XSS found in extensions
  - Recently, Evernote Web Clipper (4.6 million installs)
Results

- Found 1,097 unlisted extensions
  - Cumulative installs totalled over **127 million installations**
- Found 461 duplicated extensions
  - Cumulative installs totalled over **40 million installations**
Results

- Leveraged Mystique API to analyze privacy leakage of extensions
  - Taint analysis engine
  - Public interface
- Among unlisted extensions, flagged 3.33%
- Among duplicated extensions, flagged 6.73%
- Original Mystique paper found 2.13% of extensions flagged, representing a statistically significant increase among unlisted and duplicated extensions found [2]

Google’s Mitigations

- Removed inline installations
- Reworked extension model
  - Manifest V3
  - Unused permissions removed
- Attempts to better screen extensions
  - Banned code obfuscation
  - Code minification still allowed
Recommendations

- Give users more power to understand extension permissions
- Continue improving auditing for extensions
- Penalize misleading extension ads
Limitations

- Rotating adware
- More complex ad campaign obfuscation may have circumvented automated crawling
Thank you!

- Questions?

Contact:

awbeggs@ncsu.edu