Destroying unwanted software together

How the antimalware ecosystem can help solve this for good

Dennis Batchelder
AppEsteem Corporation
May 2016

Making an app free can bring it great distribution

Customers love to install

1) Free games
2) Free utilities
3) Free movies

And they don't always pay attention…

Free apps may come with strings attached

Some strings are appreciated

- Value-based offers, like AV products ☺

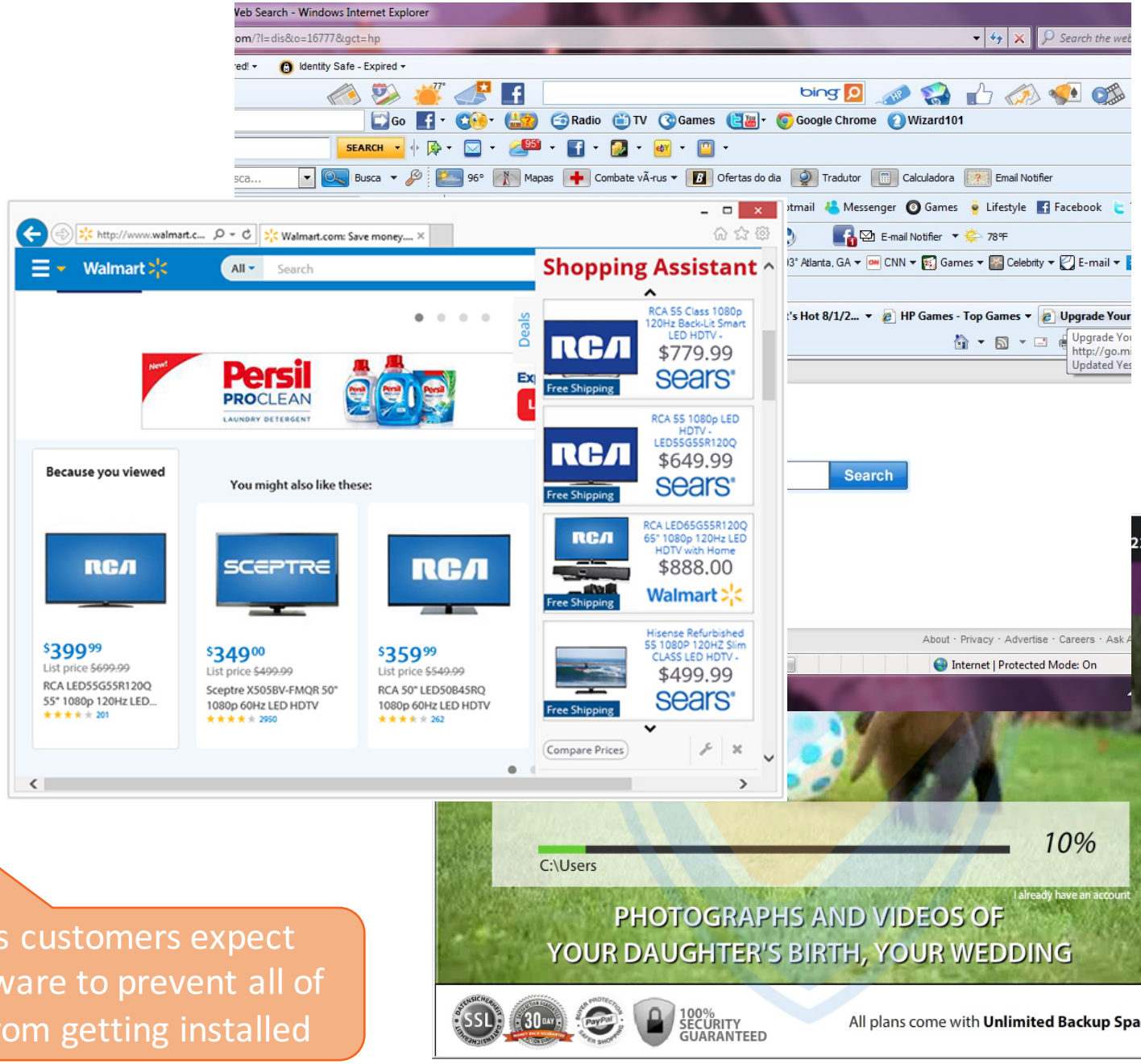
Some are under-appreciated

- Aggressive toolbars
- Unwelcome changes to search and home pages
- Popups
- Injected/replaced ads

Some are malware

- Malicious software
- Unwanted software

Today's customers expect antimalware to prevent all of these from getting installed



Classifying PUA is tough

High volume

- Most complaints

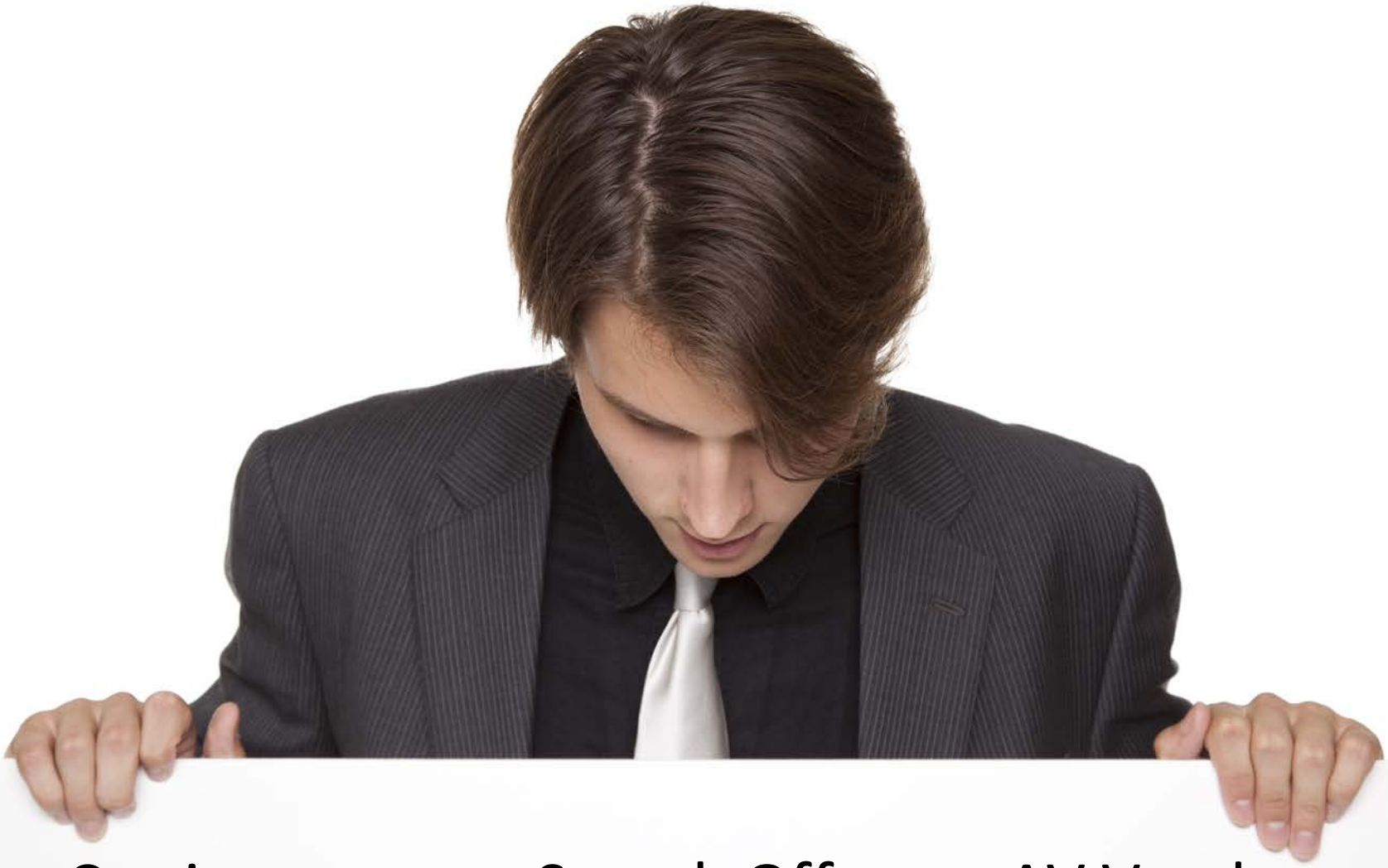
High risk

- FPs lead to lawsuits
- FNs lead to churn

High cost

- Breaks automation; requires manual verification
- Vendor disputes are time consuming
- Model doesn’t match traditional malware patterns

An example of the software monetization ecosystem



- Carrier apps
- Installers
- Search Offers
- Advertisers
- AV Vendors
- Platforms

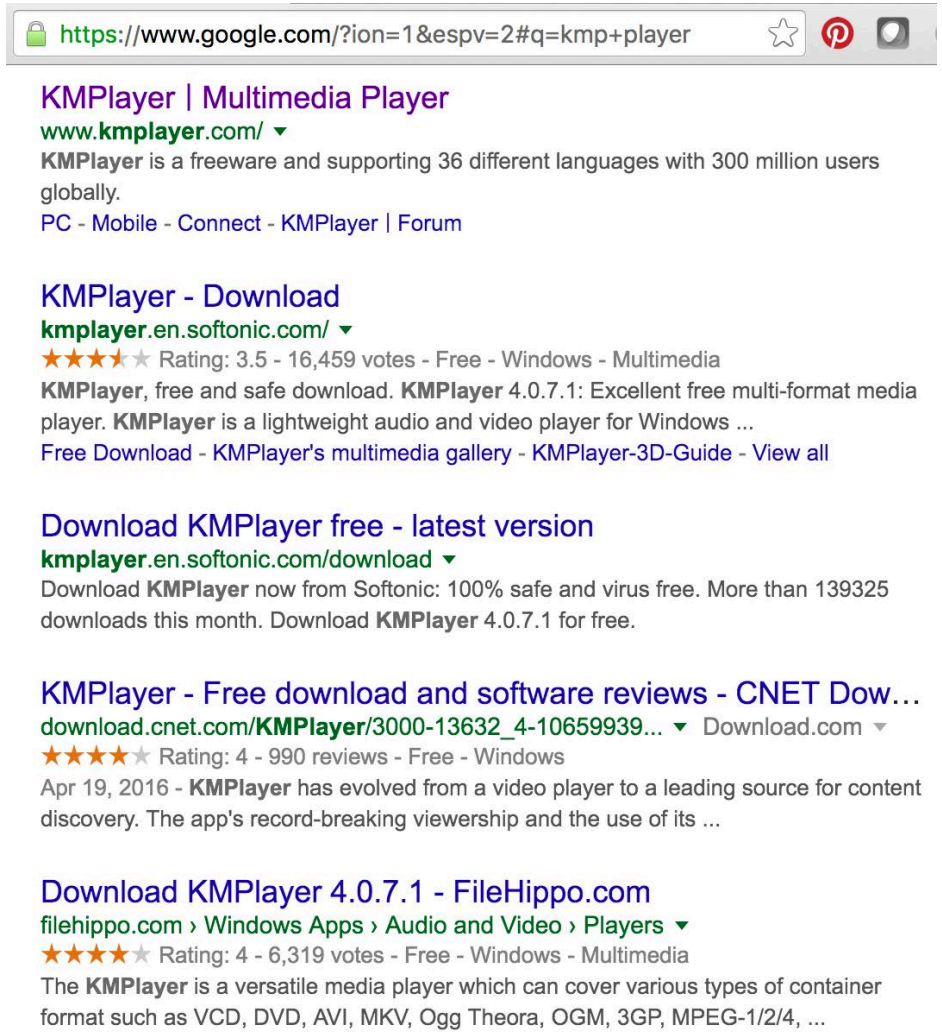
The Carrier App

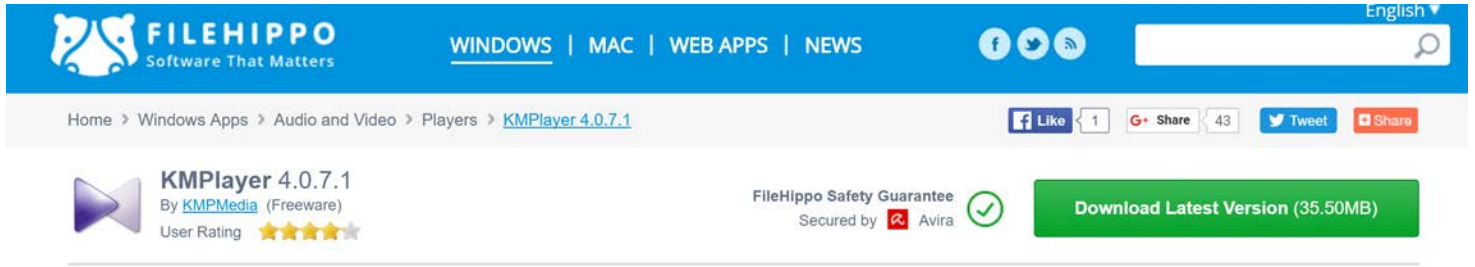
- The app everybody wants, but nobody wants to pay for
- This example: KMPlayer from KMP Media
- From official site

KMP is a versatile multi media player which can cover a various different types of contained formats. Without any separate Codec, you are able to play any media files because KMP has its' own internal Codec. Supported Codec are separated by internal & external. For the sound Codec, KMPlayer supports MPEG1, 2, AAC, WMA 7, 8, OGG & etc. and it additionally supports matrix function/normalizer function when internal sound Codec is being used. Internal Codec gets processed inside of KMPlayer so it's faster & safer. Also KMPlayer supports all the Codec from ffdshow and it additionally supports MPEG1/2. If you're a user who finds it inconvenient to install Codec, who has a low CPU computer and/or a user who strives for an excellent multi-media playback player, you'll be able to modify your environment to a convenient multi-media format by using KMP.

The Installer

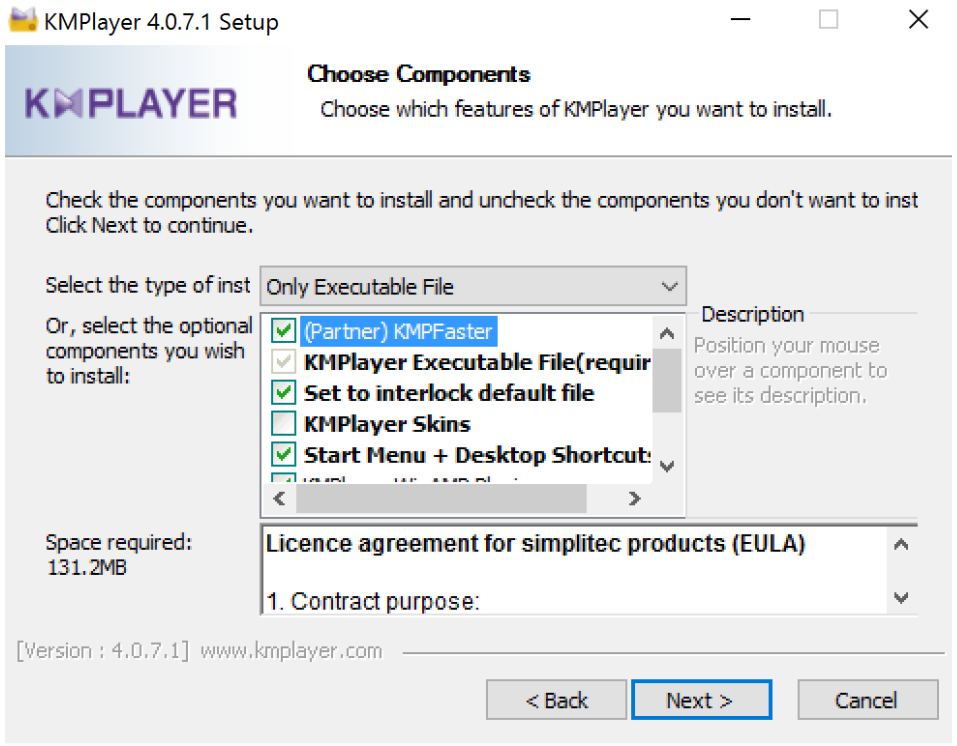
- Pays the carrier for the right to install in exchange for adding more offers
- May pay for marketing (or rely on advertisers)

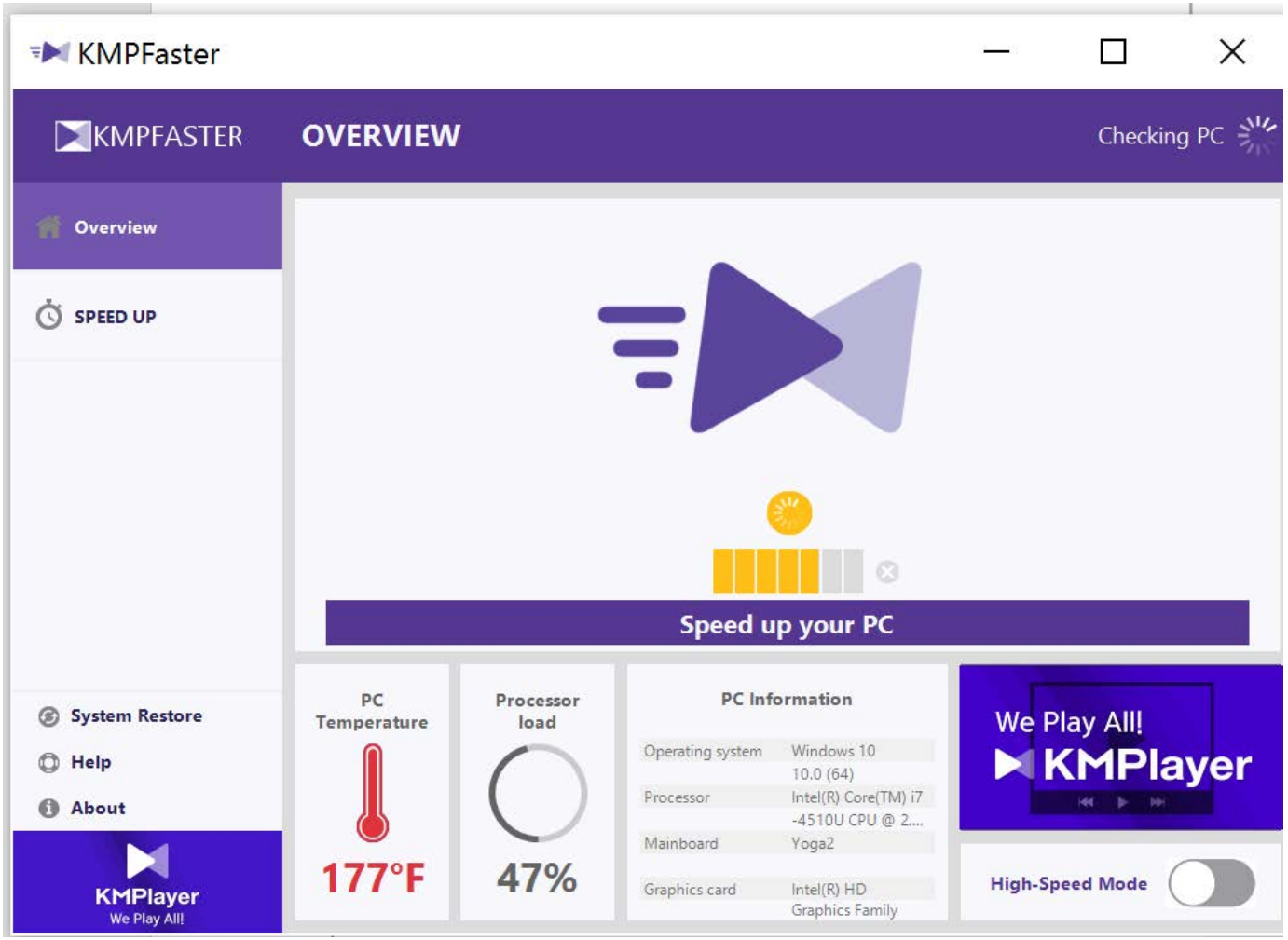


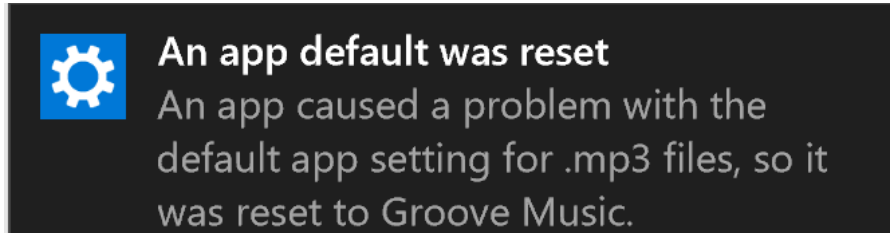


The Offers

- Can monetize, but need distribution
- Usually there's one search offer and one or more software offers
- Pay the installer, usually after an auction







It’s not easy getting detection right…

Probably clean:

- Carrier app
- Offering app

Probably unwanted behavior:

- The Installer’s offer approach

What do you detect?

Getting this right is…

- Tough and time-consuming
- Hard to genericize
- Hard to keep your researchers interested

CSA tries to help

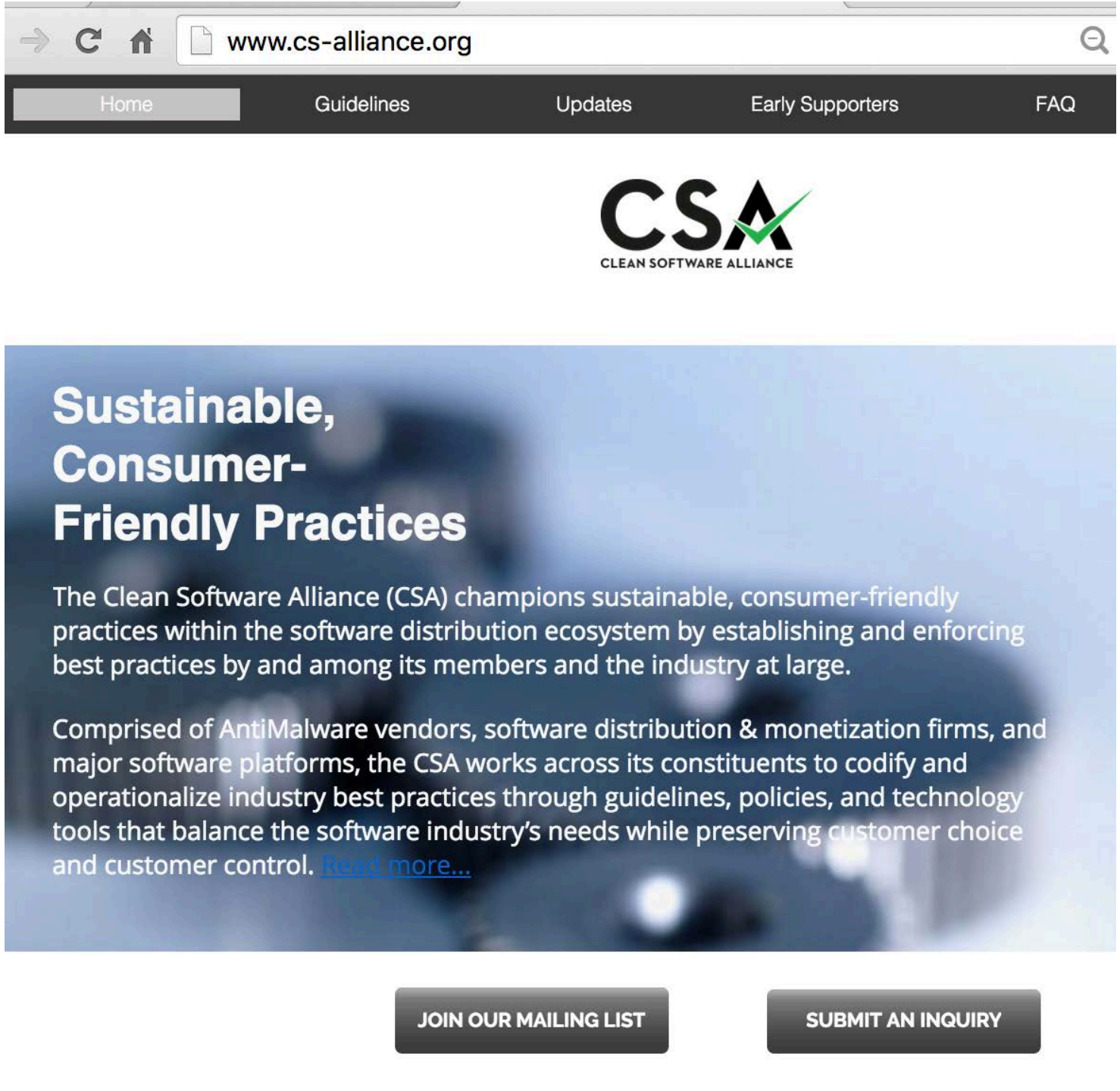
2014: Microsoft, AVs, Google, and installers founded the Clean Software Alliance

Basic idea: self-regulate

- Create a safe haven for “clean” software vendors to operate
- Agree on a set of clean behavior guidelines
- Monetization players agree to follow guidelines
- AVs agree to not detect “clean” software vendors

But it’s struggled to form

- Almost agreed on guidelines
- But it hasn’t figured out how to enforce
- Nothing operationalized yet: no membership, no governance



The state of the industry

The market has matured and companies are incented to clean up

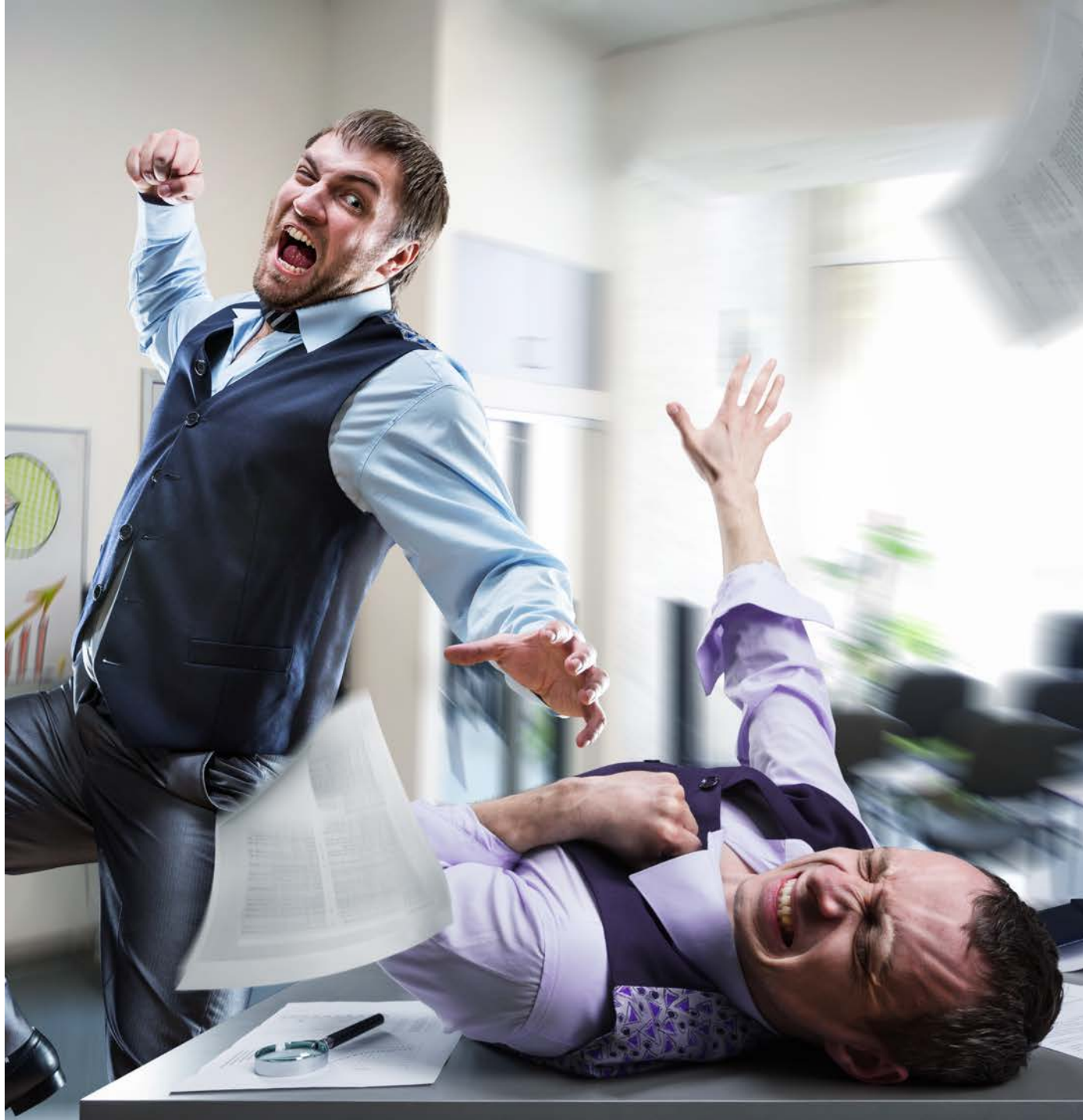
We have better communications between vendors, AVs, and platforms

- "Compliance officer" ecosystem is developing to support the industry
  - Example: Entero has done this well

The worst players have left, but…

- Many detections (vendors feel targeted)
- Vendors still invest in AV evasion
- Platforms still tighten guidelines
- The downward spiral continues

Industry is ripe for self-regulation



Making it real: a trusted seal

AppEsteem is a security startup that certifies and monitors clean apps so they can be trusted.

The dream: support the good guys so AVs/ Platforms can deal harshly with the bad guys

Certify and "seal" apps that meet guidelines

- Clean Software Alliance Guidelines
- Microsoft Objective Criteria
- Google Quality Guidelines
- Others as applicable

Monitor and eliminate apps that go dirty

- Suspend/remove as necessary

Provide attribution, behavior, and distribution data to AVs and platforms

What apps need to do

Build your app

- ✓ Register your company and your product at AppEsteem
- ✓ Link your app with SRCL (pronounced “circle”), AppEsteem’s self-regulating client library
- ✓ Use our portal to see free telemetry and analysis

Seal your app

- ✓ Get your company validated that you’re using best practices to stay clean
- ✓ Submit your app for certification, and provide your distribution rules
- ✓ Your sealed app can be distributed by you and only the installers that you authorize
- ✓ Registered security companies and platforms can monitor any sealed app’s behavior

SRCL: built-in self-regulation

Pre-seal: report mode (data only to vendors)

- App behavior
- Detections/blocks observed
- Distributions observed
- Vendor can grant access to compliance officer

Post-seal: enforce mode (data also to AVs and platforms)

- Validates seal
- Enforces distribution rights (sites, parents, children)
- Obeys killbit/uninstall commands from AppEsteem
- Share of aggregated data, probably no specific numbers

Inside the seal

1. Identification
   - Unique IDs and names
   - Dates
2. Distribution rights
   - Permitted and prohibited sites/parents/children
3. Certifications
   - Which guidelines the app meets (CSA, Microsoft, Google)
4. Vendor attestations
   - Statements by vendor on the app's value and how it monetizes
5. Signature
   - File/Seal fast/full hashes, AppEsteem cert

1) Vendor signs app, submits
2) AppEsteem certifies and builds seal
3) Vendor packages seal, re-signs app
4) AppEsteem registers app

Identification	Seal ID Grant/Expire Dates App Name, ID, Version Vendor Name, Id Signing Certificate Thumbprint
Distribution Rights	W3C's ORDL-JSON format
Certifications	Guidelines/version numbers (URL)
Attestations	Value statement Monetization statement
Signature	Digital signatures in XML-DigSig/XAdES format with timestamping for fast and full validation

Partner AV/Platform benefits

If you partner with AppEsteem:

- State the certifications you trust
- Validate seals and enforce distribution
- Let AppEsteem handle issue resolution
- Get credit when you uncover issues

We will provide online app intelligence

- Vendor relationships
- App history, related seals
- Observed behavior graphs
- Distribution sumaries
- AV detection history

You can make online status checks

You can use our cache downloads

- Trusted Vendor and App Ids
- Seal revocations
- App and vendor suspensions

Our plans to get this operational

April - June: get industry interested

- AV disclosure: China, CARO
- Platform disclosure: Google, Microsoft
- Software Vendors: select calls and visits
- Compliance teams: Entero, others
- Land MOU with CSA
- Hire team, first cut at technology

July - September: run beta

- Goal: 2-3 installers, 2 download sites
- Land AV and platform commitments

October - December: rollout full capabilities

- Windows apps and Chrome extensions

2017: expand to Android, advertising, beer

Please help make this successful ☺

We need your support to get it right

- Join a bi-weekly call to land the design
- Tell us the data that would help you (vendor information, behavior)
- Help devise a workable issue resolution system
- Help us get the right data back to you

And if it makes sense (it should!)…

- Participate in our beta
- Seal your own offers
- Commit to trust AppEsteem seals

AppEsteem™

Certifying apps for a better world

http://appesteem.com
info@appesteem.com
@appesteem