Why I left Microsoft, and why I want to save the software monetization industry

Dennis Batchelder
AppEsteem Corporation
June 2016

A security weenie for 30 years…

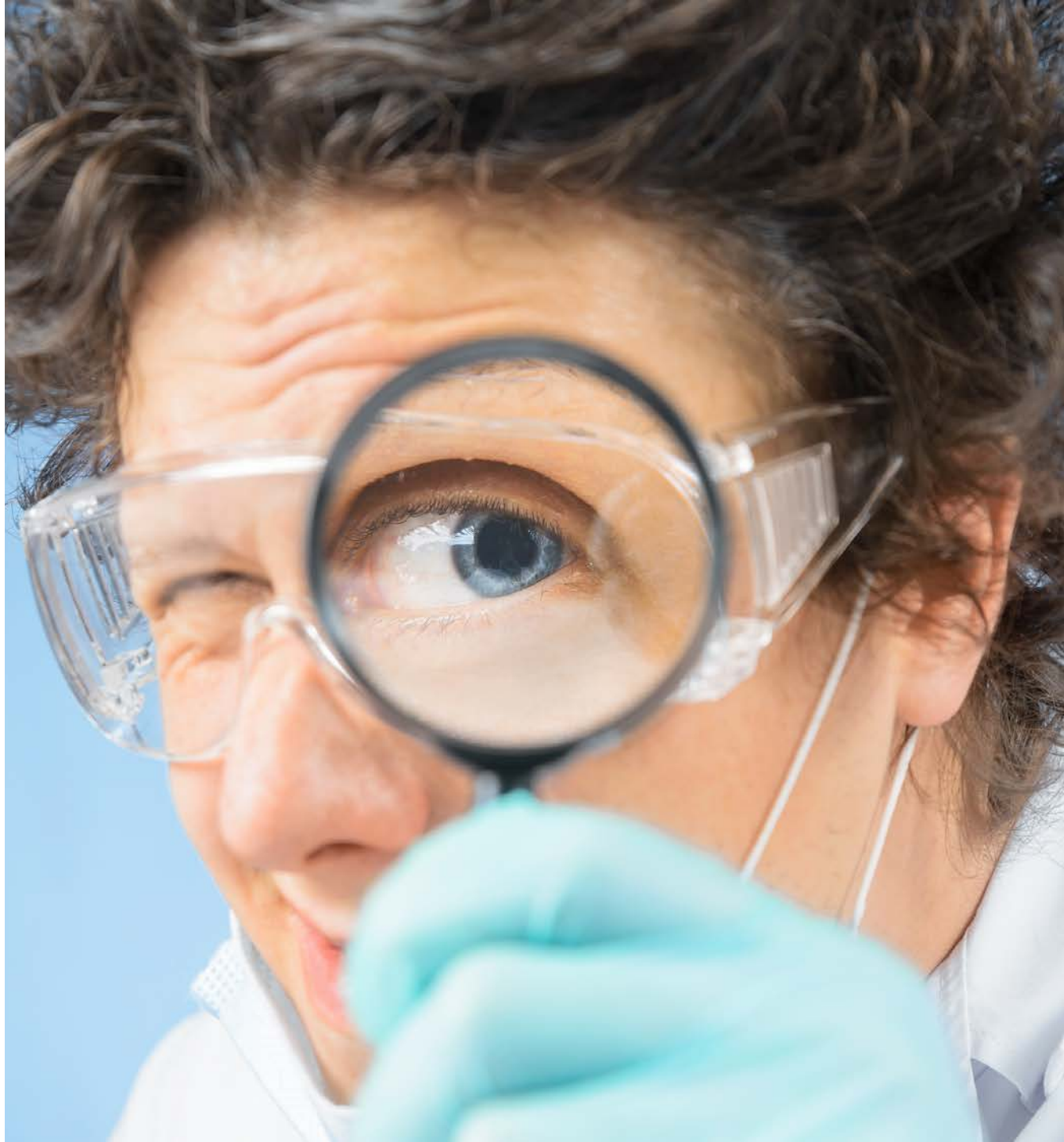
What gets me excited is fighting bad guys and protecting consumers

Ancient History

- 1985: First security job: the IRS.
- Various small bus/dev/management positions
- 1992: Founded Snare Networks: early VPN pioneer.
- 1999: Sold to Computer Associates

My road to anti-malware at CA

- Architect, SVP
- Watched budgets spent on threat
- Decided to “fix” the malware problem, and chose Microsoft in 2007 as the only company who wanted to/could do it



Microsoft made a difference

2007-2014: MMPC part of the enterprise/cloud business unit

- 2009: made MSE free to increase worldwide protection coverage
- 2011: embedded security into products as a feature
- 2012: defined our strategy to orchestrate the ecosystem and not compete
  - VIA: sharing with the ecosystem
  - CME: coordinated malware eradication to better fight and eliminate the bad guys
  - CSA: get the bad guys out of the downloader/ad-tech industries
- It worked ☺

2014-2016: MMPC "acquired" by Windows

- Team integrated into Windows
- Focus on competing/tests cost us our focus on protecting consumers
- I felt we were fighting the good guys ☹

Meanwhile, CSA suffered

CSA had great plans

- Re-taking the industry from its worst players
- We had some great meetings in Herzliyya, Canterbury, Las Vegas, New York, Prague

We felt early successes

- Better communications, clearer guidelines, faster dispute resolution
- Some of the worst players quit

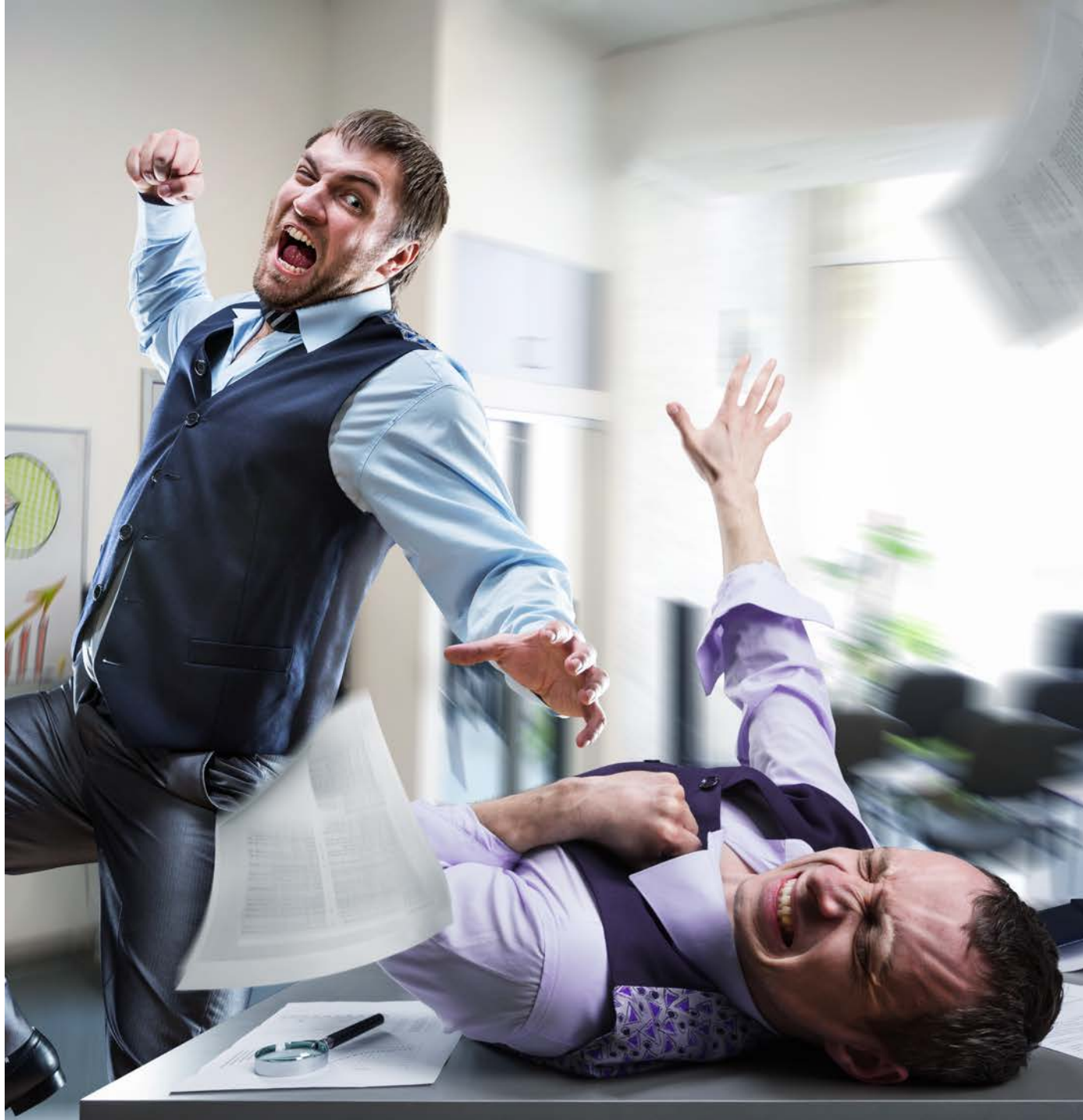
But it stalled before it operationalized

- I felt this pain especially during ASW, meeting with the publishers

The monetization industry is worse off than before

- Google and Microsoft are outflanking CSA
- The cleanest guys are abandoning the space
- Bad behaviors run rampant
- Industry talks as if CSA is dead

And consumers are still getting screwed



Time to go…

2015: I resigned, but was asked to stay to drive strategy/ecosystem

- When Microsoft calls…
- But priorities changed
  - Policies centered around competitors, not bad guys
  - Eradication became a joke
  - CSA seemed de-prioritized

2016: I quit again, and this time it was welcome ☺

- I felt good about the eight years
  - Learned a lot about multi-stakeholder negotiations
  - Achieved 95% protection rate
  - Serious decline in malicious software
- But bad about two things
  - The increase of ransomware
  - Knowing how to fix this industry, but not getting it done

Launching AppEsteem

Finish what I started: make the CSA operational

- A unique opportunity to do this: trust from the AVs, platforms, and downloaders
- Replaced taggants with a seal and monitoring library
- Assembled a team
- Socialized a business plan
- Obtained (informal) AV and platform commitments
- Recruited for a July beta

This has to get done

- An almost-formed CSA only meets the needs of the platforms and the AVs
- Early supports wear targets on their backs
- Consumers still get screwed; the bad guys still profit

But we're running out of time

Moving quickly plans

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, supply chain

What apps will 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 monitoring data

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, 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 (e.g., 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

My assertions/food for thought

Business has trumped security in this industry

- We can no longer trust Microsoft and Google with this
- Many AVs are also compromised in this space
- Consumers will end up with less choice

We need the CSA for two things:

- Regulations: unless we're happy with non-consumer-focused guidelines
- Unity: It's too easy to beat each company individually

You have to be serious about cleaning up

- AVs and platforms only willing because they can get tougher on those who don't seal
- It means we have to monitor ourselves

If you do, it can be profitable and stable

- There's latent demand from high-quality carriers and offers
- With no race to the bottom, prices won't be insane with crazy fluctuations

But it's going to take courage

- It's hard to change, especially when you're asked to be first

And it will still be a bumpy ride

- Until the whole supply chain is sealed
- Until we reach critical mass

AppEsteem™

Certifying apps for a better world

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