Protecting the Protectors

How AppEsteem helps the security ecosystem succeed

Dennis Batchelder
5th China Cyber Security Conference
13 July 2017
Beijing, China

Background

- 25 years in cyber security
  - Snare, CA, Microsoft
- President of AppEsteem Corporation
- Security ecosystem champion

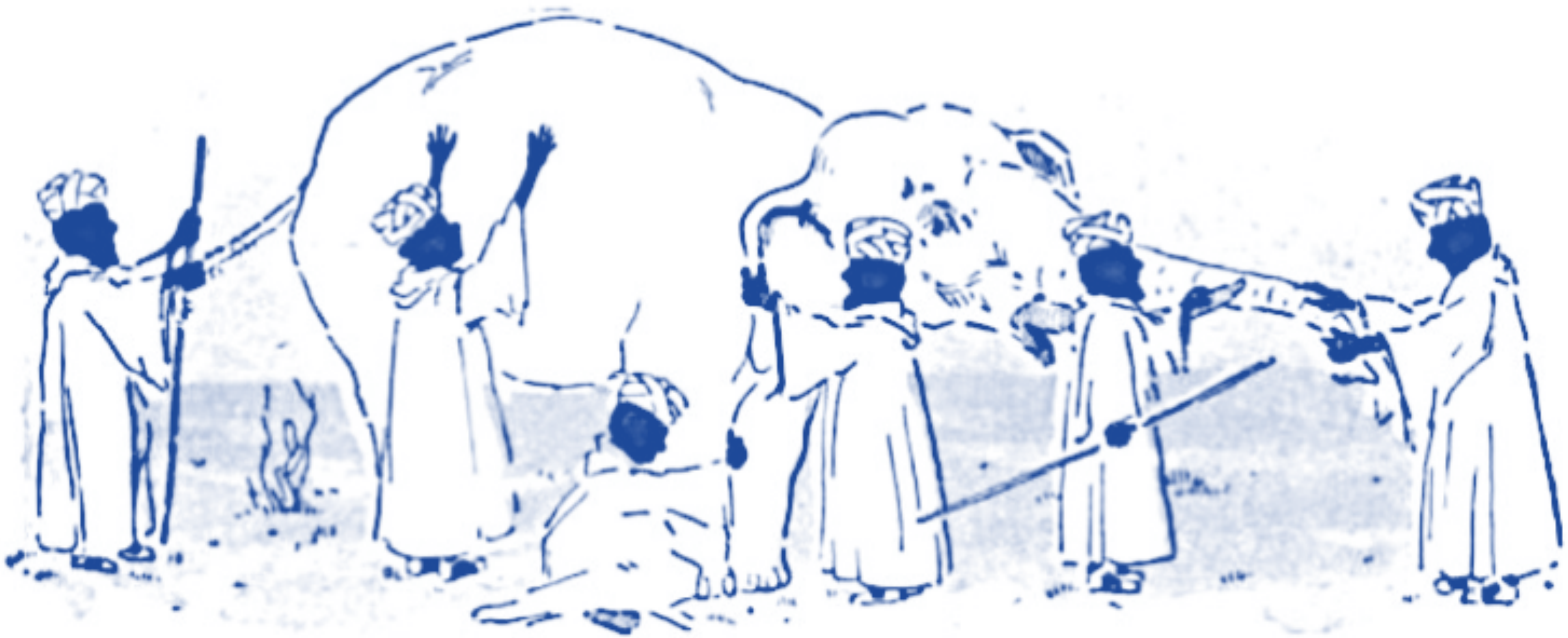
TRUSTED

AppEsteem™

MONITORED

Customers expect their security solutions to be efficient at detecting and stopping threats

Rope, wall, tree, fan, spear, or snake?



"The Blind Men and the Elephant" by John Godfrey Saxe
Illustration from Golden Treasury Readers, 1908

But it’s hard for a security company to have a **full perspective.**

AppEsteem addresses this full perspective problem with app intelligence

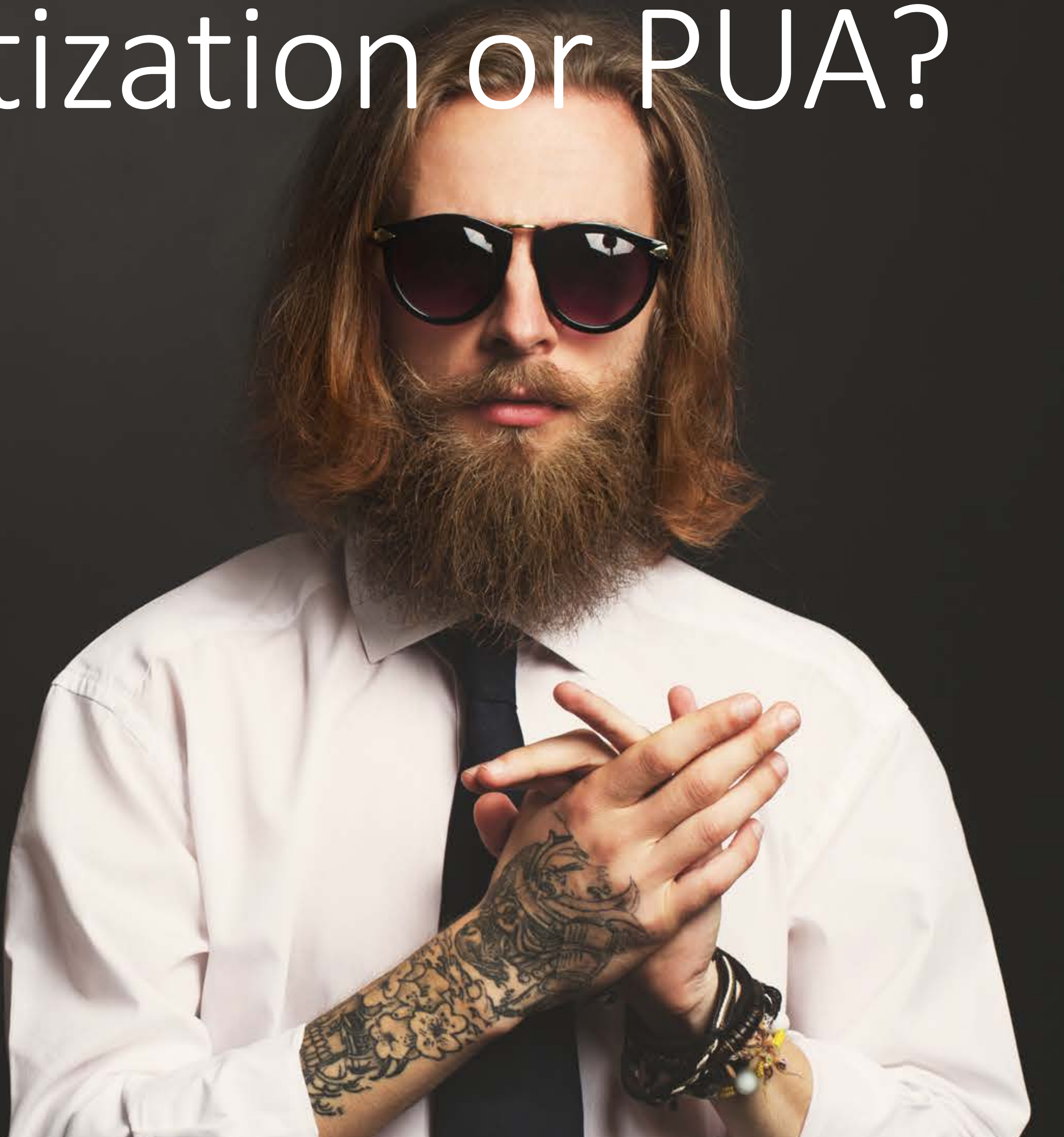
Helping AVs fight deceptive software monetizers (PUA)

TRUSTED AppEsteem™ MONITORED

Software monetization or PUA?

- Offer “free” apps
- Make millions in revenue
- Proud of their brand
- Spend big money on performance marketing

- BUT: compete ruthlessly, driving up marketing costs
- This leads to aggressive, deceptive, consumer-unfriendly behaviors (PUA)



Example deceptive monetizer behaviors

- Fake news affiliates
- Scary and lying ads
- Misleading landing pages
- Installing and changing settings without permission
- Exaggerating system health problems
- Aggressive ad/offer injection

We watch AVs struggle to keep up with PUA

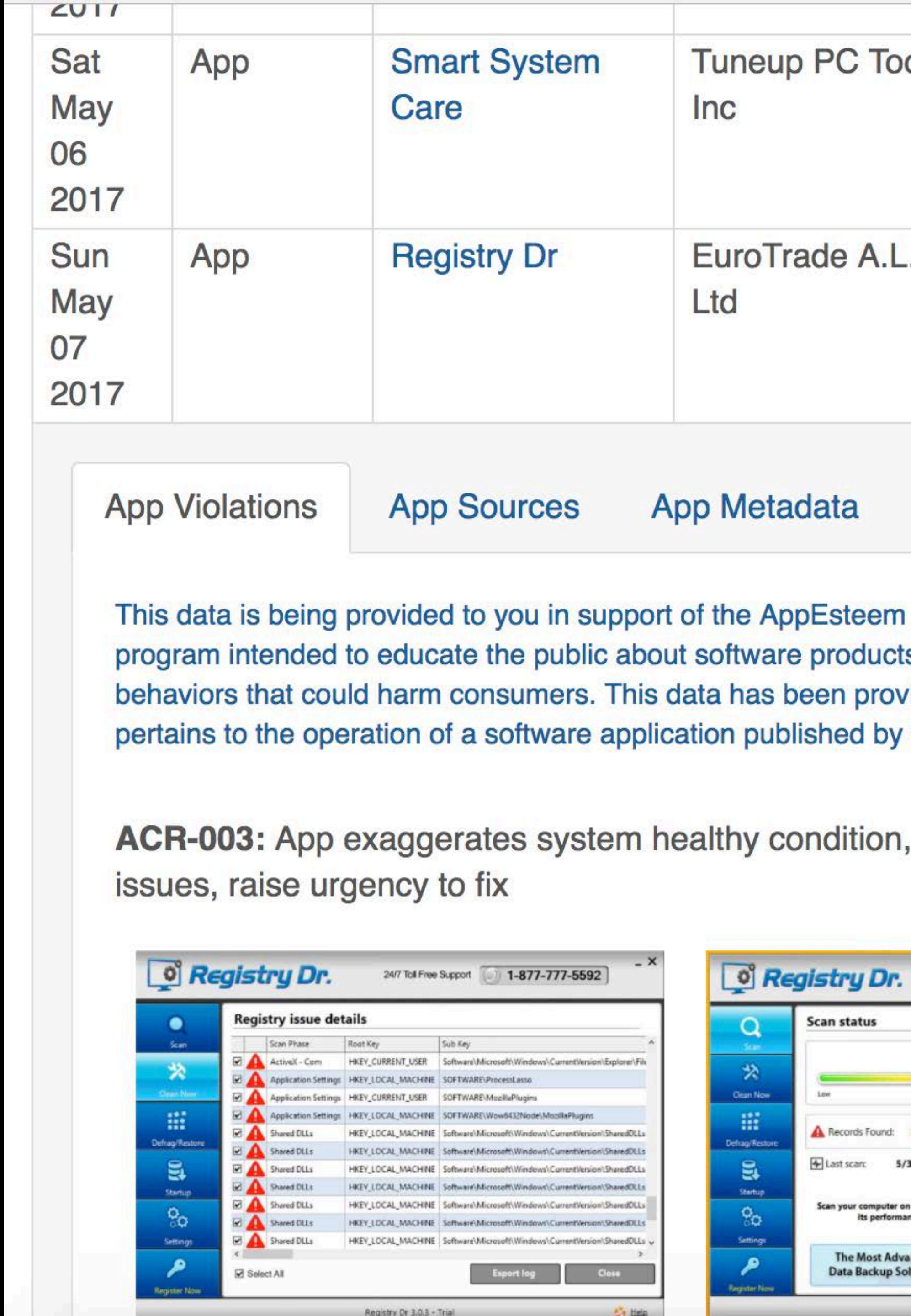
- Automation breaks
- Analysis is slow
- Monetizers fight with lawyers
- Researchers hate the work
- No standard requirements

Our goal is to help AVs by leading monetizers to choose sides

We use our requirements to do this

Monetizers can choose to be Deceptors…

- By violating any of the 29 deceptive behaviors agreed to by most of the largest AVs
  - https://customer.appesteem.com/Home/Deceptor
- We hunt for Deceptors, gather evidence, and publish
  - https://customer.appesteem.com/deceptors



2017			
Sat May 06 2017	App	Smart System Care	Tuneup PC Too Inc
Sun May 07 2017	App	Registry Dr	EuroTrade A.L. Ltd

This data is being provided to you in support of the AppEsteem program intended to educate the public about software products behaviors that could harm consumers. This data has been prov pertains to the operation of a software application published by

ACR-003: App exaggerates system healthy condition, issues, raise urgency to fix

Registry Dr.

24/7 Toll Free Support 1-877-777-5592

Registry issue details

		Scan Phase	Root Key	Sub Key
☑	⚠	ActiveX - Com	HKEY_CURRENT_USER	Software\Microsoft\Windows\CurrentVersion\Explorer\Fil
☑	⚠	Application Settings	HKEY_LOCAL_MACHINE	SOFTWARE\ProcessLasso
☑	⚠	Application Settings	HKEY_CURRENT_USER	SOFTWARE\MozillaPlugins
☑	⚠	Application Settings	HKEY_LOCAL_MACHINE	SOFTWARE\Wow6432Node\MozillaPlugins
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs
☑	⚠	Shared DLLs	HKEY_LOCAL_MACHINE	Software\Microsoft\Windows\CurrentVersion\SharedDLLs

☑ Select All

Registry Dr 3.0.3 - Trial

Registry Dr.

Scan status

⚠ Records Found:

Last scan: 5/3

Scan your computer on its performan

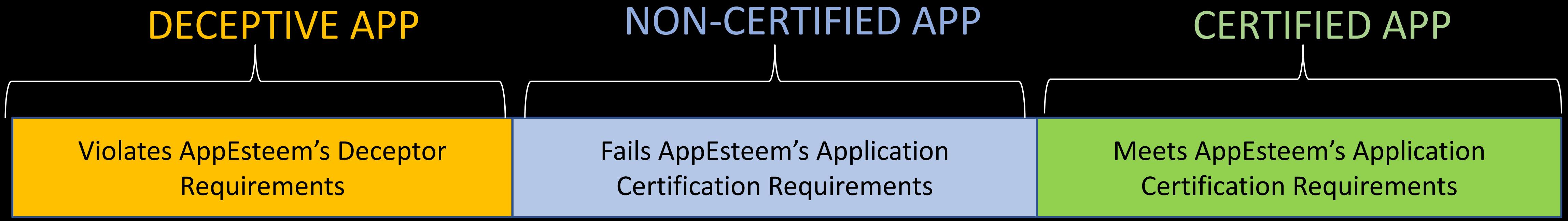
The Most Adva Data Backup Sol

Monetizers (hopefully) will choose to be clean

- They must pass all of our 130 requirements (software, ads, landing pages, call centers)
  - https://customer.appesteem.com/Home/AppCertReqs
  - This process usually takes 1-3 months
- We seal certified apps and publish
  - https://customer.appesteem.com/certified

We supply our app intelligence to the AVs

1) Apps violating our Deceptor requirements are DECEPTIVE
2) Apps we seal are CERTIFIED
3) We encourage NON-CERTIFIED apps to get certified
4) We provide both Deceptor and Certified feeds at no cost



DECEPTIVE APP

Violates AppEsteem's Deceptor Requirements

NON-CERTIFIED APP

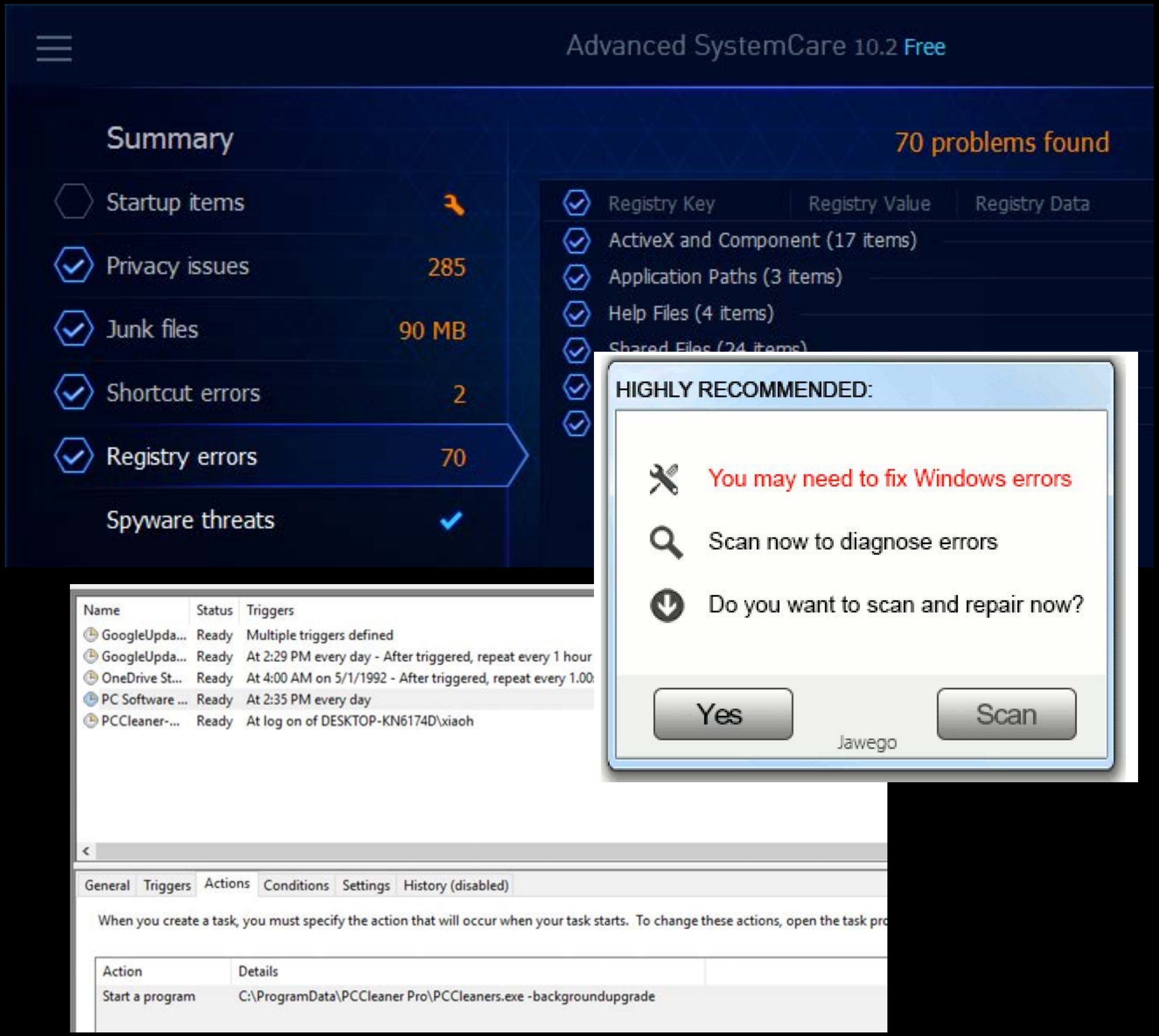
Fails AppEsteem's Application Certification Requirements

CERTIFIED APP

Meets AppEsteem's Application Certification Requirements

The Deceptor Program works!

- Many examples of monetizers changing their behavior
- Submissions by AVs, platforms, consumers
- Interest by law enforcement
- These are examples where AVs have been struggling to drive change for YEARS



Advanced SystemCare 10.2 Free

Summary

70 problems found

Startup items	
✓ Privacy issues	285
✓ Junk files	90 MB
✓ Shortcut errors	2
✓ Registry errors	70
Spyware threats	✓

✓ Registry Key | Registry Value | Registry Data

✓ ActiveX and Component (17 items)

✓ Application Paths (3 items)

✓ Help Files (4 items)

✓ Shared Files (24 items)

HIGHLY RECOMMENDED:

You may need to fix Windows errors

Scan now to diagnose errors

Do you want to scan and repair now?

Yes

Jawego

Scan

Name	Status	Triggers
GoogleUpda...	Ready	Multiple triggers defined
GoogleUpda...	Ready	At 2:29 PM every day - After triggered, repeat every 1 hour
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00
PC Software ...	Ready	At 2:35 PM every day
PCCleaner-...	Ready	At log on of DESKTOP-KN6174D\xiaoh

General | Triggers | Actions | Conditions | Settings | History (disabled)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task pro

Action	Details
Start a program	C:\ProgramData\PCCleaner Pro\PCCleaners.exe -backgroundupgrade

We try to certify apps from monetizers who are ready

Ready to be clean	Desperate to be clean
• Tracking consumer sentiment • Killing apps with no intrinsic value • Shifting to a long-term payment relationship with consumers • Seeking to understand the intentions behind the requirements	• Too-fast, unquestioning submission of contracts, attestations • Looking for ways to get around monitoring and certification • Withdrawing/substituting apps • Offering to pay extra to make the problem go away

AppEsteem offer to China's monetizers

- We've seen China-based monetizers distributing their apps world-wide
- These apps also need to choose a path: Deceptor or clean
- We've called out some of them as Deceptors
- We want to help China-based monetizers get it right
  - We will translate our requirements (Deceptor and Certification) to Chinese
  - We will certify any interested AV products for free

Thank you

Security companies help keep their customers safe, but who helps the security companies?

Dennis Batchelder is the President of AppEsteem, a company that helps security companies fight deceptive apps.

Dennis will show how security companies benefit from AppEsteem, and make a call to action for China-based security companies and software vendors to join in the fight against deceptive apps.

TRUSTED AppEsteem™ MONITORED

https://appesteem.com