How to increase cybercrime:

Stop cooperating with each other

Dennis Batchelder
Hong Jia
AppEsteem

AVAR-2018, Goa India

We bring cooperative strategies to fighting consumer cybercrime

- First we align on UwS requirements
- Then we provide/publish Deceptor and Certified feeds
- Security partners enforce when they agree

This talk evaluates the effects of non-cooperation

Deceptor

TRUSTED
AppEsteem®
MONITORED

Software monetization is pervasive

- Consumers love free
- 90% of all installed apps are free
  - Free to try
  - Free with ads/offers
  - Freemium
- Most consumer AVs are software monetizers

Software monetizer funnel math

Example app costs with $6K advertising spend CPC

Step	Math	Counts	Calculated Cost	LTV Target to survive
Advertise	4% click through rate on search ads	600K see, 24K click	$0.25 CPC	
Install	50% accept, 50% install	12K accept 6K install	$1.00 CPI	$2.00
Convert	5% convert to paid	300 convert	$20 cost to convert	$40.00

What if a monetizer wants to make even more?

If software monetizers scare, trick, or cheat consumers, they're committing cybercrime

(We call their apps **Deceptors** and feed them to security partners)

Ways Deceptors commit cybercrime

Monetization Goal	Cybercrime
Traffic: Spend money to get consumers to see your "free" offer	Scary ads, false representation, malicious suppliers and affiliates
Distribute: Get installed, then stay as long as possible	Irresistible offers, fear at uninstall, stealth, hardening
Monetize: Search, ads, bundles, upsells, call centers, resource "borrowing"	False sense of urgency, PII and resource theft, price gouging, threats, install malware

Deceptors breed more Deceptors

- Deceptors earn more, so they out-bid competitors for even more traffic
- Competitors now face higher advertising costs, so they become Deceptors; a vicious, infectious cycle

AVs to the rescue?

Based on market coverage

Step	Counts / Cost	5%	20%	50% *	75%	90%
Advertise	24K click / $0.25 CPC					
Install	6K install / $1.00 CPI	**5,700 / $1.05**	**4,800 / $1.25**	3,000 / $2.00	1,500 / $4.00	600 / $10
Convert	300 convert / $20 cost to convert	**285 / $21**	**240 / $25**	150 / $40	75 / $80	30 / $200
Response		**Ignore**	**Evade**	Choose a path	Comply	Comply

* Until AV blocking coverage approaches 50%, Deceptors can afford to hurt consumers

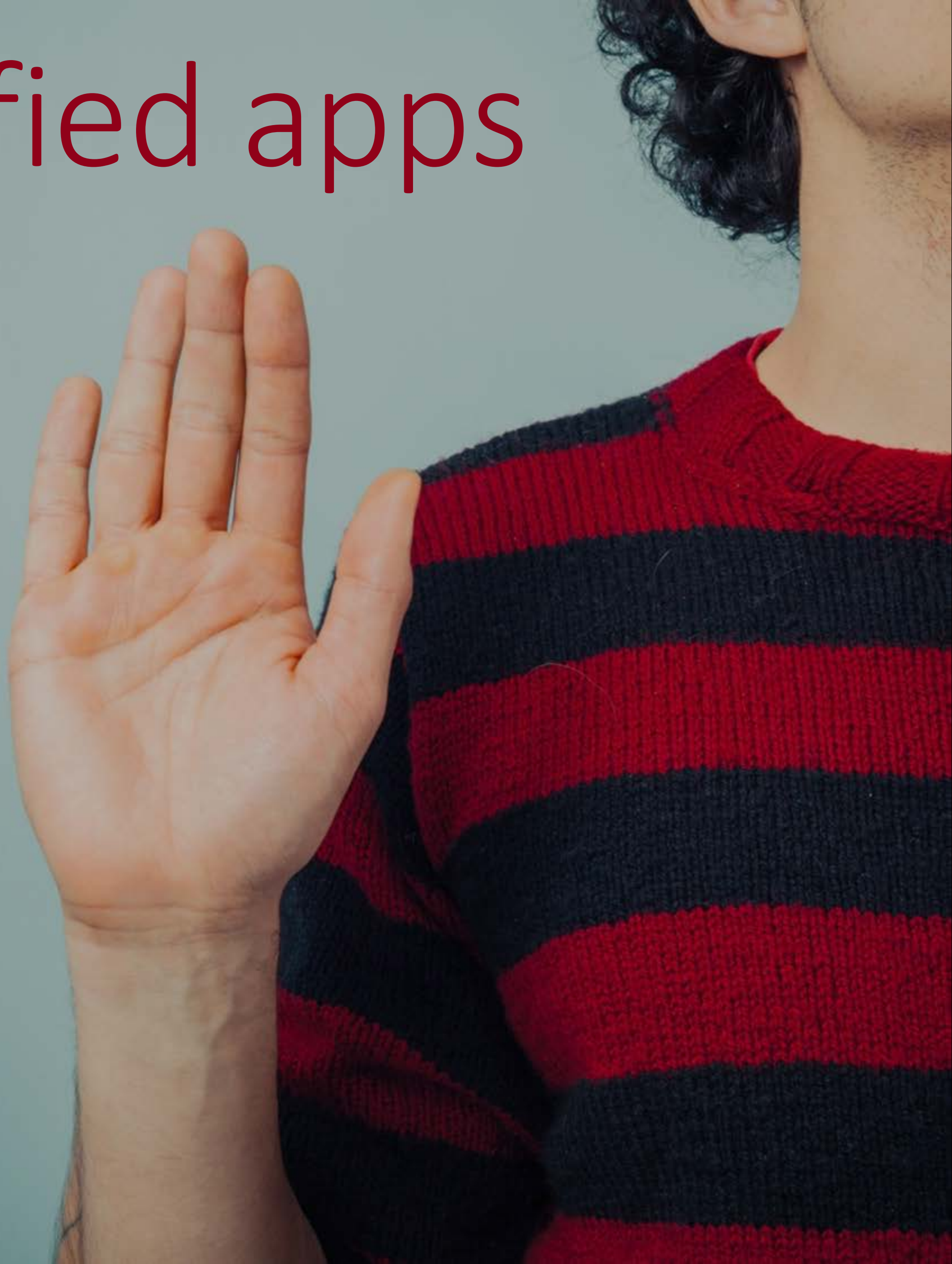
Analyzing Deceptor persistence

	Told app, didn't list n=48	**Listed as Deceptor** n=170
App Fixes/Dies	58%	95%
App Remains Active	42%	5%

- We measured what would happen if we didn't help coordinate
- All active Deceptors had <30% AV blocking

A better world: certified apps

- Certified apps promise to not violate any UwS or PUA requirements
- This puts a 33% hit on their business (they trade it for sustainability)
- We want AVs to encourage certification by
  - Providing actionable reasons if they're still detecting them
  - Creating a level playing field so they can thrive (detect Deceptors)



Certified app blocking encourages deception

Step	Counts / Cost	Clean cost of certification	5% detect	20% detect*
Advertise	24K click / $0.25 CPC	$0.25	$0.25	$0.25
Install	6K install / $1.00 CPI	4,000 / $1.50	3,800 / $1.58	3,200 / $1.88
Convert	300 convert / $20 cost to convert	200 / $30	190 / $32	160 / $38
Response		Hope	Worry	Panic, quit

* When AV blocking coverage approached 20%, half of the Certified apps reverted to Deceptors, increasing cybercrime

We’re enlisting more Dynamic Security Ecosystem partners

Block point	Deceptor Blocking Partner
Installs	AVs **(key player)**
Ads, offers, downloads	Browser safety, firewalls
Listings	Download sites, app stores
Money	Payment gateways, call centers, bundlers, affiliates

The more blocking partners involved, the better chance we have to stop cybercrime and encourage good software monetizer behavior

Reasons we’ve heard against cooperating

Reason	Our Response
We refuse to tell apps why we detect them	The prevalence of UwS proves this strategy fails. Why not give Certified apps a chance to fix?
Certified apps have no redeeming value, so I will keep detecting them as PUA	Can you make this claim without being hypocritical?
We will never trust a Certified app; they’re just finding other ways to cheat	If we find Certified apps hurting consumers, we’ll revoke their certification
We don’t think your requirements are strict enough	Please help us fix what we’re missing.
We can’t detect our business partners	Find new business partners, or encourage yours to start behaving

Rewarding cooperation

- We’ll explain to consumers why they’re safer with participating AVs. (PR and tests)
- We’ll support certified apps we find are unreasonably targeted by AVs (invalid, non-actionable, or non-shared reasons)

A call to cooperate

- You may think you can protect your customers by working alone
- But we’ve shown that working alone increases consumer cybercrime
- The best way to protect your customers is to work together
  - Block Deceptors as fast as possible
  - Encourage proper behavior of Certified apps
  - Help monitor for misbehavior
  - Help advance UwS requirements