State of the Threat

Chaos, Insecurity & Crime "In the Cloud"

Brent Huston, Security Evangelist
@lbhuston
bhuston@microsolved.com

MICROSOLVED, INC.

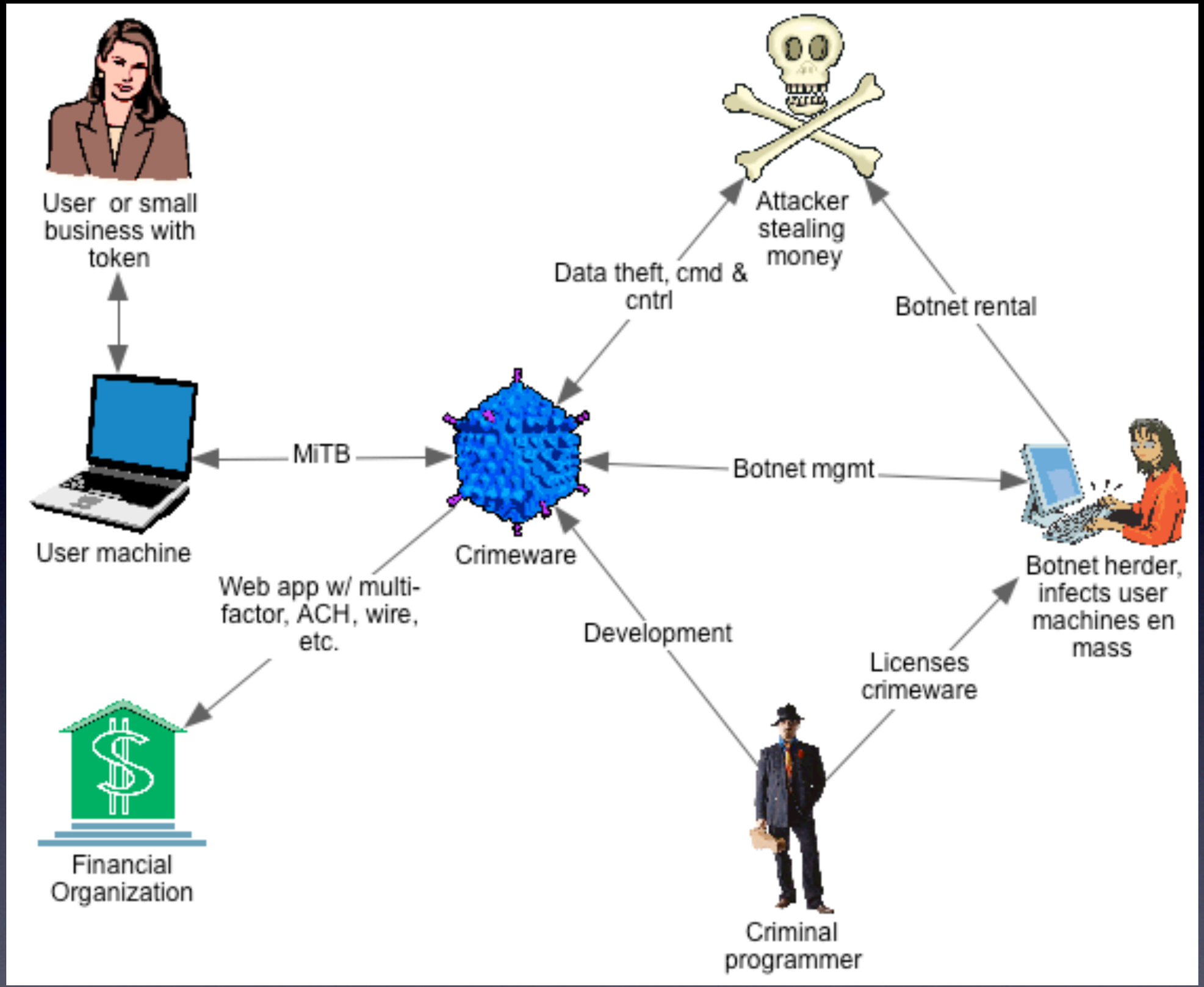
Pragmatic Problems

- 361 > 144 > 4
- Profit, loss & the data economy

- Health records are the new gold
- IP is the new platinum
- Crime is the new green

Threat Intelligence

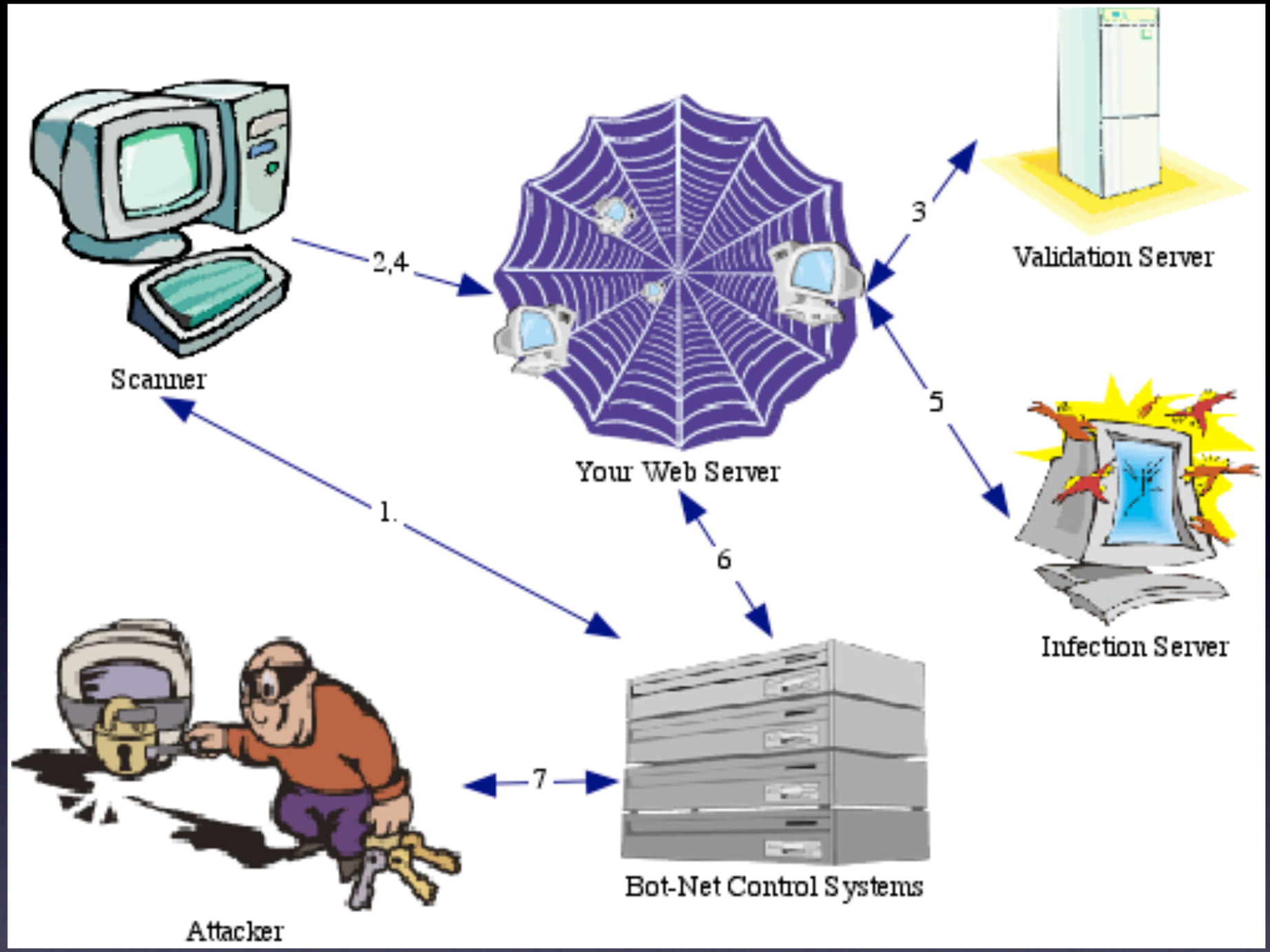
- Dedicated cyber-criminals
- No problem with historic security architectures & controls
- Prevention weakening, need increased containment, detection & response capabilities



Modern Crimeware Model

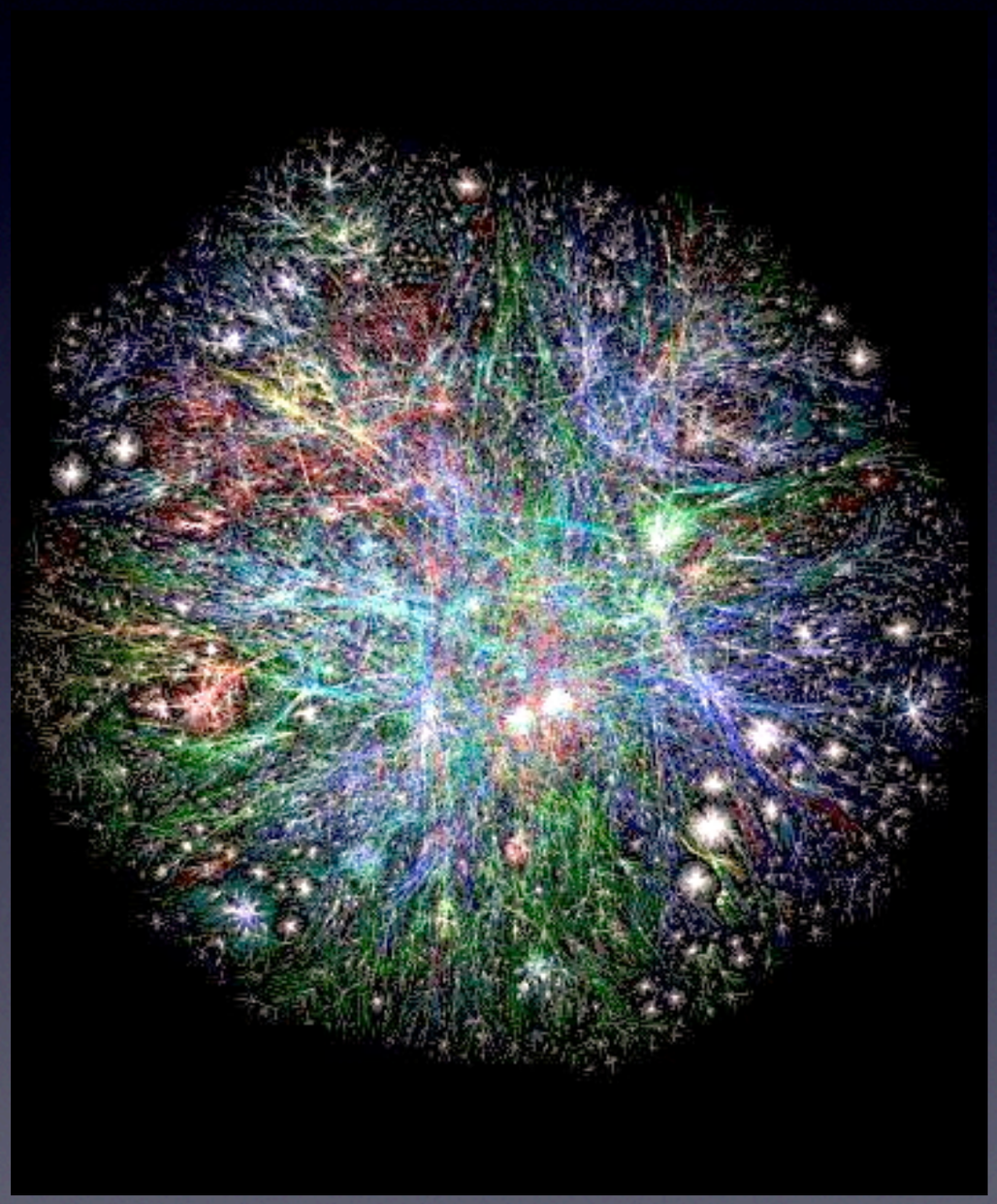
PHP/ASP Malware

- Most common #HITME probes
- Custom scanners developed daily
- New vulns hourly
- Open source improvement
- Start & end of crimes



PHP/ASP Malware Infrastructure

The Data Density Question



- Will crime follow the data to the cloud?

- More density = lower cost for crime, lower risk for criminals

- The cloud is not living up to control ideals, so far...

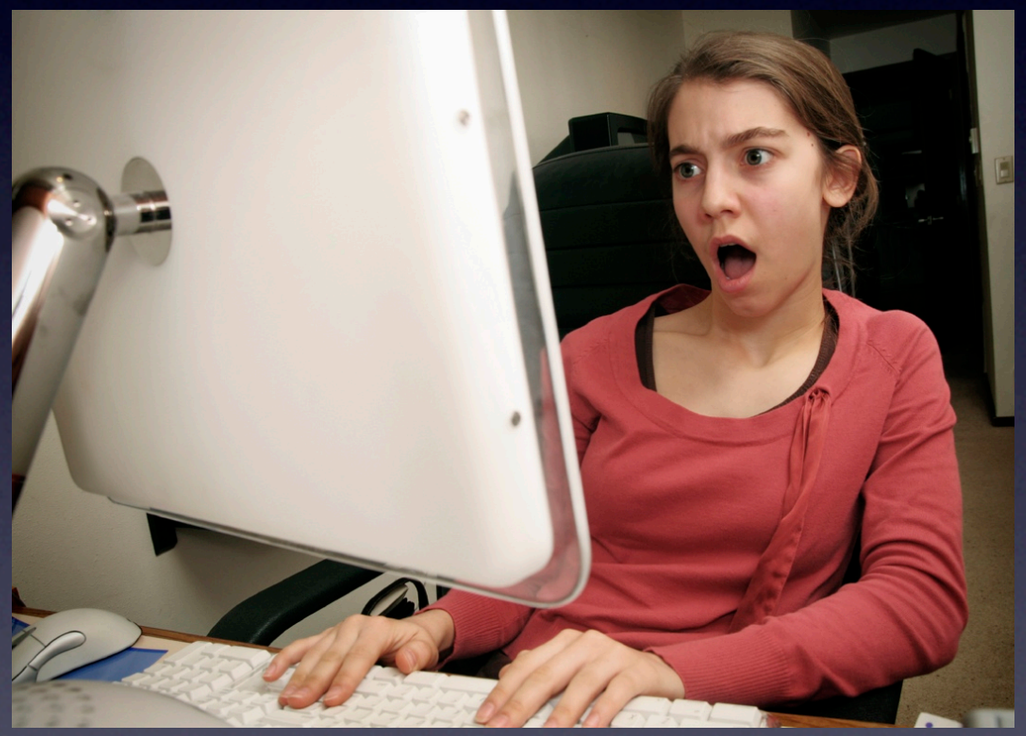
CIA, (Really, A!)

- Consumers don't understand your silos.
- What is CIA & why you should care…
- A has shown some major #FAILS
- Attackers use force multiplication to tamper with intended use cases

What We Are Seeing...

- Increased focus on end-points, mobile & embedded systems
- Malware with incredible complexity & diversity
- Slow, low & uniquely coded attacks
- Knowledgable attackers - understand tech, code & architecture ***better than you***
- Time to discovery & mitigation is growing, not shrinking...

What We Aren't Seeing...



- Jumping the hypervisor in real life, yet...
- Focused social media campaigns, that we know of…
- Malware that leverages exploits beyond privilege escalation
- ***Identified*** attacks against ***some*** critical verticals - Luck vs Ignorance?

Thoughts on Controls

- Spend time understanding what data they have, where it lives, how it moves and what trust is involved.
- Less focus on prevention, more on detection & response.
- Understand RATIONAL security - use threat metrics to scope controls
- Learn to see with "***FAIL Vision***"

Thanks & More Info

- @lbhuston
- bhuston@microsolved.com
- stateofsecurity.com
- microsolved.com
- By now, you should be thinking differently about information security!