Stopping Worms, Malicious Insiders, And Other Lower Life Forms in the Virtual Data Center

TAK3D0WNC0N: DS 4

Michael Berman, CISSP
CTO Catbird

Introduction

- Me: pen tester, kernel engineer, cybercrime investigator, virtual security SME
- You: understand virtualization, firewalls, intrusion detection, and incident response
- Keep it interactive

Is your current information security management system working?

Poll:

- Are you constantly being attacked from both the inside and the outside?
- Or, are you not being attacked?

catbird

Hypothesis: two kinds of attack

1. Largely automated, targeting system resources, or PII
   - Botnets, phishing, pharming, …
2. Mostly manual, targeting crown jewels
   - Old-school
   - Now called APT for some reason

Facts

- Each type of attack is on the rise
- Both can be very damaging
- Both can be described, detected, deterred

Do some homework

- What do I mean by “described?”
- What about unknown unknowns?

We can learn from outside our industry

- North American Air Safety
  - No single point of failure
  - Requires 6 or more mistakes to cause a crash
- Accidents in North American Climbing
  - No single point of failure
  - Requires two or more mistakes to be in jeopardy

Attack project plan

1. Reconnaissance
2. Exploit weakness
3. Infiltrate or Blitzkrieg
4. Gather the goods
5. Exfiltrate
6. (some times) Repeat 4-5

How are the botnet folks different?

Our track record: not so good

- Heartland Financial
  - SQL-injection
  - Single point of failure in external facing web application
- RSA, and Epsilon
  - Spear phishing
  - One unsafe click
- SIPRNet (wikileaks)
  - One bad user

But we already know the answer

- Don’t we?

Describe attack

- Understand attack methodologies
- Look for multiple points to disrupt attack
- Implement mitigation

Did anyone say…

DEFENSE IN DEPTH

But that’s

- Hard
- Expensive
- Useless

- Cue the world’s smallest violin playing the world’s saddest song

No. It’s really easy.

- And worth it
- Virtualization security to the rescue
- Let me explain
- Then it’s demo time

Virtualization security

- Accurate inventory
  - Reduces unknowns
- Security orchestration
  - Reduces gaps and avoids manual failures
- Elastic deployment
  - Places security bastions everywhere
- Lowers costs
  - Easier to deploy, manage, and sustain

Explanation

- Virtual security is integrated with hypervisor
  - Hypervisor protects bastion/bastion protects hypervisor
  - Integrity is reinforced
  - Controls are more accurate and harder to defeat
  - Hypervisor APIs allow for increased automation
  - Automation increases resilience

DEMO

Would you like to see my 1950?

- I’m going to show the attack elements
- Then demonstrate defense

Conclusion

Leverage

- You’re virtualizing anyway
- Virtual security provides better protection and defense in depth

Reap the benefits

- Reduce risk of successful attack
- Decrease cost of an incident
- Improve compliance
- Lower security TCO

catbird

Questions

- Thank you
- www.catbird.com