RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: EXP-R03

Advanced Persistent Security to Combat Advanced Persistent Threat

Ira Winkler, CISSP

President
Secure Mentem
@irawinkler

Araceli Treu Gomes

Subject Matter Expert –
Intelligence and Investigations
Dell SecureWorks
@sleepdeficit_

#RSAC

Why The Hype Matters to Us

- It destroys our focus
- It changes the story
- It asks questions that shouldn't be asked
- It deflects blame
  - Bad security vs unstoppable enemy
- "If the top organizations can be hit, there is no way anyone will expect us to stop the attacks"

The Question That Should Be Asked

Was it really a "sophisticated" attack, or just bad security?

The Proclaimed "Sophisticated Attacks"

- Hacking Team
- IRS
- Ashley Madison
- Anthem
- Premera
- You name it, it's sophisticated according to someone

Super Sophisticated

It Can Also Help You

- It gets people talking about security
- Use the narrative to help your cause
  - If management is concerned about the hype, use it
- Highlighting the common vulnerabilities exploited during attacks can get you funding to mitigate similar vulnerabilities
- Stating how your security would have stopped the attacks would give you kudos

Hacking Team

- Notable in that they supposedly support law enforcement and had zero day vulnerabilities
- Embarrassing data to customers
- Leak of vulnerabilities causing ripple effect

Sophisticated?

- Password was passw0rd
- Able to access and download data as engineer
- Sophisticated: HELL NO!
- Once inside there was apparently a flat network or easy data access

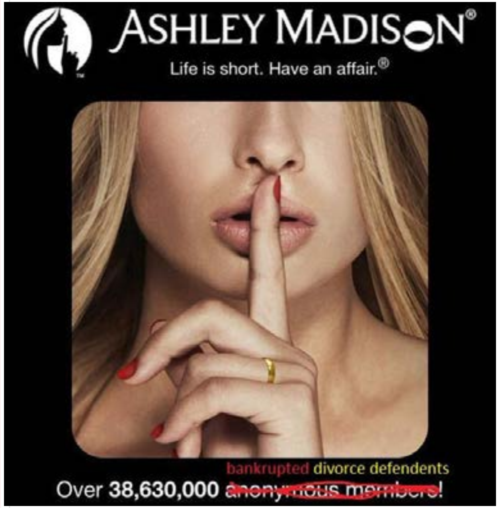
IRS Breach

- 330,000 records compromised through Get Transcript function
  - 400,000 attempted breaches
- Compromised authentication scheme
- Required “information on the taxpayer had”
  - Hmmmm….
- Criminal downloaded records, filed false tax returns
  - Stole $50 Million
- IRS Commissioner said it couldn’t be stopped citing
  - Smart criminals with lots of advanced computers, hiring smart people
  - OMG

Sophisticated?

- All the criminals needed were credit reports
- IRS used commercial system that asked questions with answers available through credit reports
- ***Went undetected for 400,000 relatively intensive attempts***

Ashley Madison


ASHLEY MADISON®
Life is short. Have an affair.®
bankrupted divorce defendents
Over 38,630,000 ~~anonymous members~~!

- Compromise of clients and client information
- Led to suicides
- Led to great embarrassment for others
- Demonstrated that they did not delete accounts as promised
- Released sensitive internal documents
- Revealed that there weren’t many real women on site

Sophisticated?

- SQL injection attacks likely
- Criminals claimed that network poorly segmented
- Pass1234 was root password on all servers
- Poor password encryption used
- Data not deleted
- Arrogance

Add a mask

Take advantage of our tools to add an extra level of discretion and character to your photos.

Anthem

- 80,000,000 health care records compromised
- Largest breach of his type

- This one was personal
- Potentially perpetrated by China
  - Seemed to have signature of Deep Panda, and pandas are from China
- A large number of people have government access

Sophisticated?

- Watering hole attack suspected
- Compromised administrator credentials
- Undetected for nine months
- Massive querying of data

Premera

- 11,000,000 accounts compromised
- Phishing attack suspected
- Operated for 9 months
- Deep Panda suspected again
- 277 data breaches in healthcare organizations in 2015

Commonalities

- Improperly segmented networks
- Detection Deficit Disorder
  - Ignoring or looking at incidents in wrong places
- Failure to white list
- Not monitoring critical systems
- Poor awareness
- No multi-factor authentication
- Phishing messages

Preventing the IRS Attack

- Frankly authentication might not be feasible to strengthen
- Better detection
- IP analysis
- Rapid increase in requests
- Focus on misuse detection

The Irari Rules of Sophisticated Attacks

- Must not actualize because of a Phishing message
- Malware must have been undetectable
- Passwords were not easily guessed
- User awareness exploited with poor awareness program in place
- Known vulnerabilities cannot have been exploited
- Multifactor authentication in use on critical systems
- Passwords were not hardcoded into the systems (or on TV)
- Detection capability was in place and not ignored
- Proper network segmentation in place
- User accounts had minimum privileges

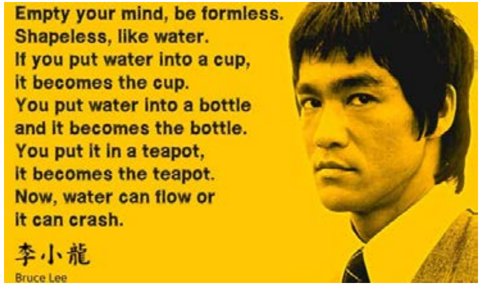
Advanced Persistent Threat or *ADAPTIVE* Persistent Threat?

- They are Persistent
- They are a Threat
- But they are more adaptive than they are advanced
- Advanced implies sophisticated
- Sophisticated implies unstoppable

APT Assumes Failure

- Actually, “successful” APT assumes failure
- They assume there will be countermeasures in place
- They assume there will be detection mechanisms
- They know they need to be adaptive
- They are proactive

“Be like water” – Bruce Lee



Empty your mind, be formless.
Shapeless, like water.
If you put water into a cup,
it becomes the cup.
You put water into a bottle
and it becomes the bottle.
You put it in a teapot,
it becomes the teapot.
Now, water can flow or
it can crash.

李小龍
Bruce Lee

“Persistence and focus will get you in”

Rob Joyce

Chief, NSA Tailored Access Office

Advanced Persistent Security

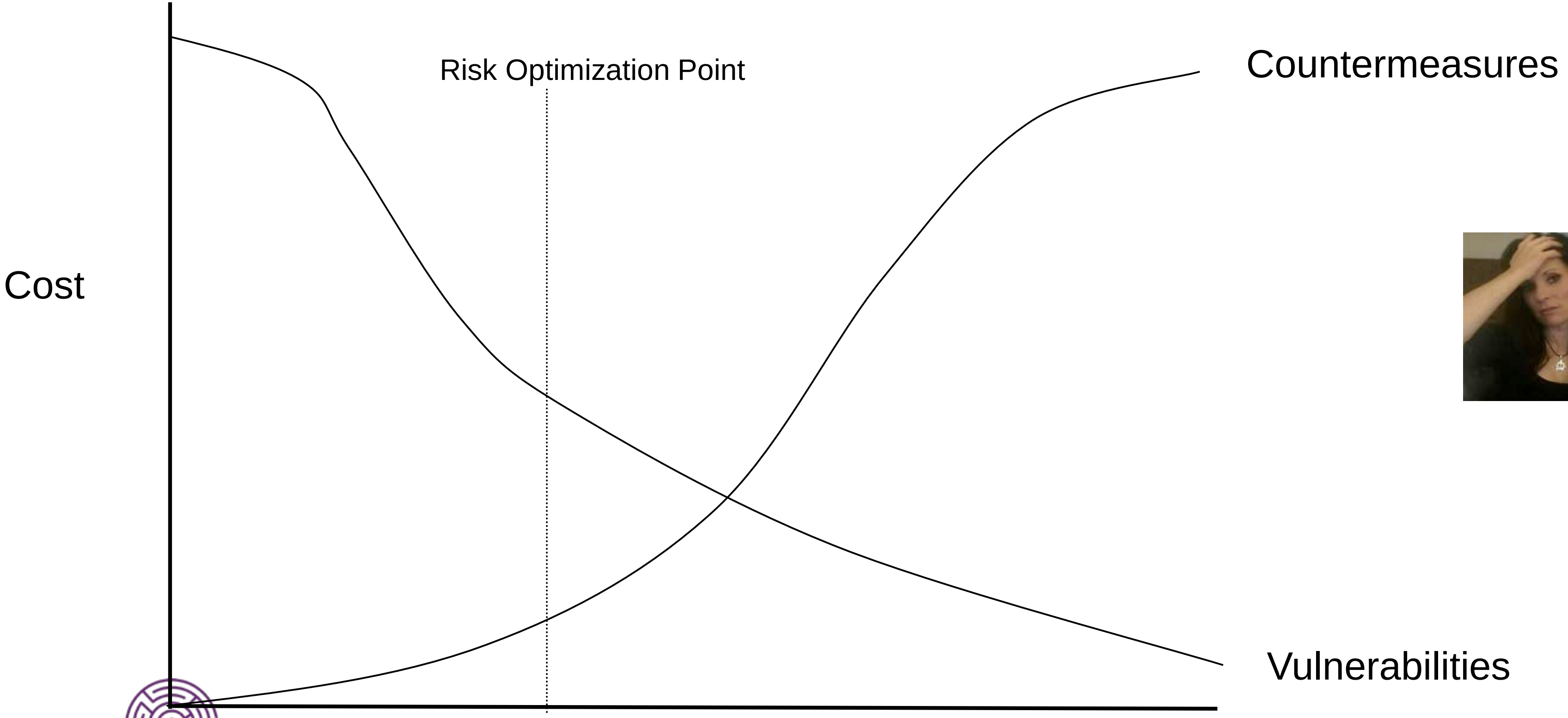
Advanced Persistent Security

- Fight APT with APS
- Adaptive Persistent Security, but Advanced Persistent Security is a better buzz term
- Security programs must be adaptive
- Security programs must assume failure
- Designed to presume failure
- Extrusion prevention > Intrusion prevention

Risk Management Implies Failure is Acceptable

- IRS hack demonstrates availability requires better detection, not prevention
  - It can be more cost effective
  - Better detection = Better protection
- Security is about Risk Management not perfect prevention
- Detection and reaction mitigate loss that cannot be prevented
- Adversary disruption is an acceptable “Security” strategy
  - Kill Chain Analysis
  - Goal is exit prevention

Optimizing Risk



Proaction

- Design program always looking for failures
- Determine where failure is likely to occur
- Perform threat intelligence to determine likely attackers and attack vectors
- Implement security countermeasures as appropriate
- Implement detection
- Build the ability to modify protection into your program

Defensive Information Warfare

Protection

Detection

Reaction

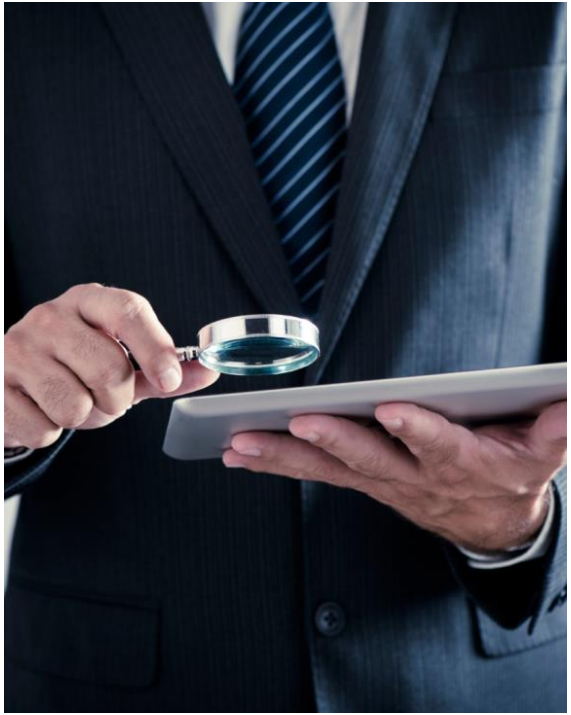
SECURE
MENTEM

Protection

- Understand what you Value
- Understand your Threats
  - What they target
  - What they value
  - Likely attack vectors
- Determine your vulnerabilities
- Prioritize countermeasures based on likely threats and vulnerabilities
- Address security culture

Detection

- Understand your Kill Chain
- Detection Deficit Disorder
  - Avoid it
- Human sensors
- Constantly examine the data
- Assume critical assets are being stolen
- Assume networks are compromised and look for indications



Reaction

- Reaction should be anticipated as being a common circumstance
- Reaction built into security program and architecture
- Determine who’s attacking you
  - What are their attack methods
- Look for additional attacks
  - Be a hunter
- Feedback into Protection
- Remember, your goal is exit prevention
  - Extrusion prevention is more manageable intrusion prevention

The Role of Security Culture/Awareness

- People have a role in Prevention, Detection, and Reactio
- A strong security culture prevents incidents
  - People should behave appropriately
- A strong security culture detects incidents in progress
  - Snowden’s coworkers should have noticed suspicious activi
  - Detecting incidents, phishing, etc.
- Reaction
  - Reporting
  - Taking actions to mitigate incidents before they get too damaging

Conclusions

- Attackers are successful not because they are advanced or sophisticated, but because they are adaptive and persistent
- Be adaptive and persistent in response
- Be proactive
- Failure is expected
- Failure can be good
- Implement Advanced Persistent Security

"Apply" Slide

- Next week you should:
  - Determine whether you have a "Security" program or a "Prevention" program
- Within 3 months you should:
  - Reevaluate your awareness program
  - Determine the protection of your critical data
  - Analyze your likely threats
  - Determine if you have Detection Deficit Disorder
- Within 6 months you should:
  - Reevaluate the structure of your overall security program

ficit