PHISHLABS

Advanced Persistent Threat
vs
Advanced Persistent Security

Ira Winkler, CISSP
@irawinkler
ira@securementem.com

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?

PHISHLABS

The Proclaimed “Sophisticated Attacks”

- Sony
- IRS
- Ashley Madison
- ISIS hacks
- Healthcare companies
- Retailers
- You name it, it’s sophisticated according to someone

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?

- There was a Zero-day to get in
- Password was passw0rd
- Able to access and download data as engineer
- Sophisticated: HELL NO!
- Once inside there was apparently a flat network, easy data access, and no detection

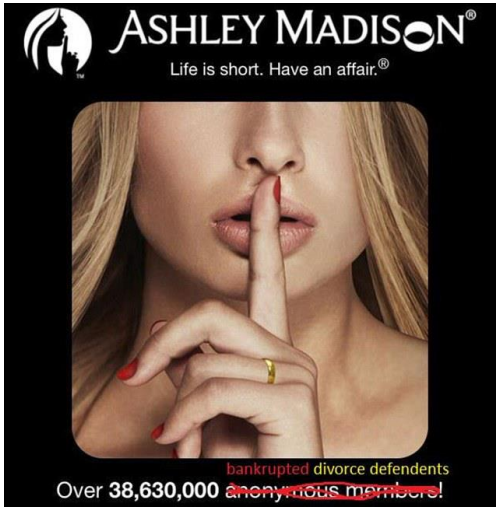
IRS Breach

- 700,000 records compromised through Get Transcript function
  - X Million attempted breaches
- Compromised authentication scheme
- Required “information on the taxpayer had”
- 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

Sophisticated?

- All the criminals needed were credit reports
- IRS used commercial system that asked questions with answers available through credit reports
- ***Went undetected for 700,000 relatively intensive attempts***

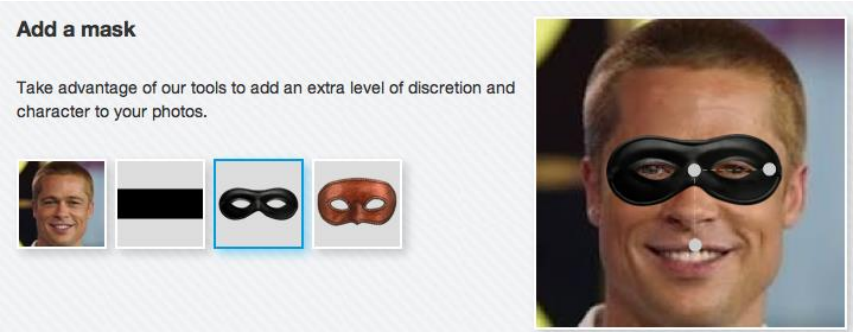
Ashley Madison



- 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?

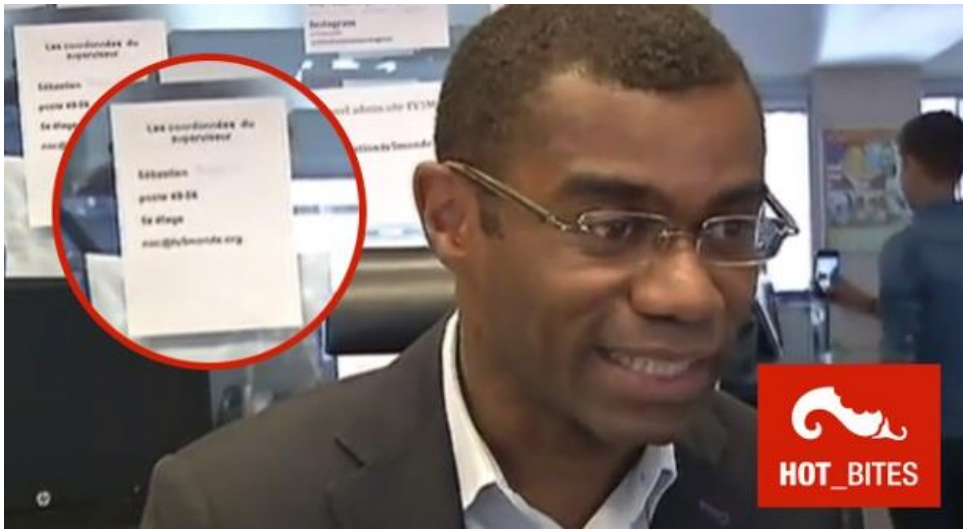
- SQL injection attacks likely
- Criminals claimed that network poorly segmented
- Pass1234 was root password on all servers
- Poor password encryption used
- Data not deleted
- Arrogance



PHISHLABS

CENTCOM/TV5Monde

- The world was talking about how advanced ISIS was
- The media questioned the security of US Government systems and classified data
- Politicians were horrified and wanted answers
- It was their Twitter feed
- It was their YouTube feed
- French politicians called it an attack against free speech



PHISHLABS

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

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

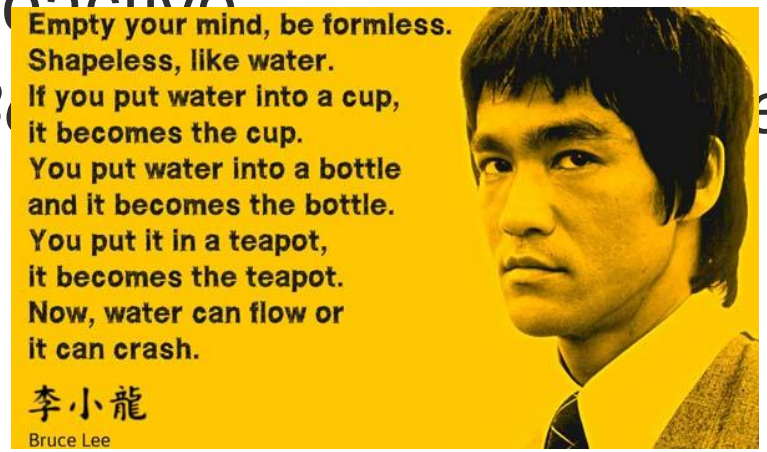
Advanced Persistent Threat or ADAPTIVE Persistent Threat?

- 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 pr

“B *ee*



PHISHLABS

“Persistence and focus will get you in”

Rob Joyce

Chief, NSA Tailored Access Office

Advanced Persistent Security

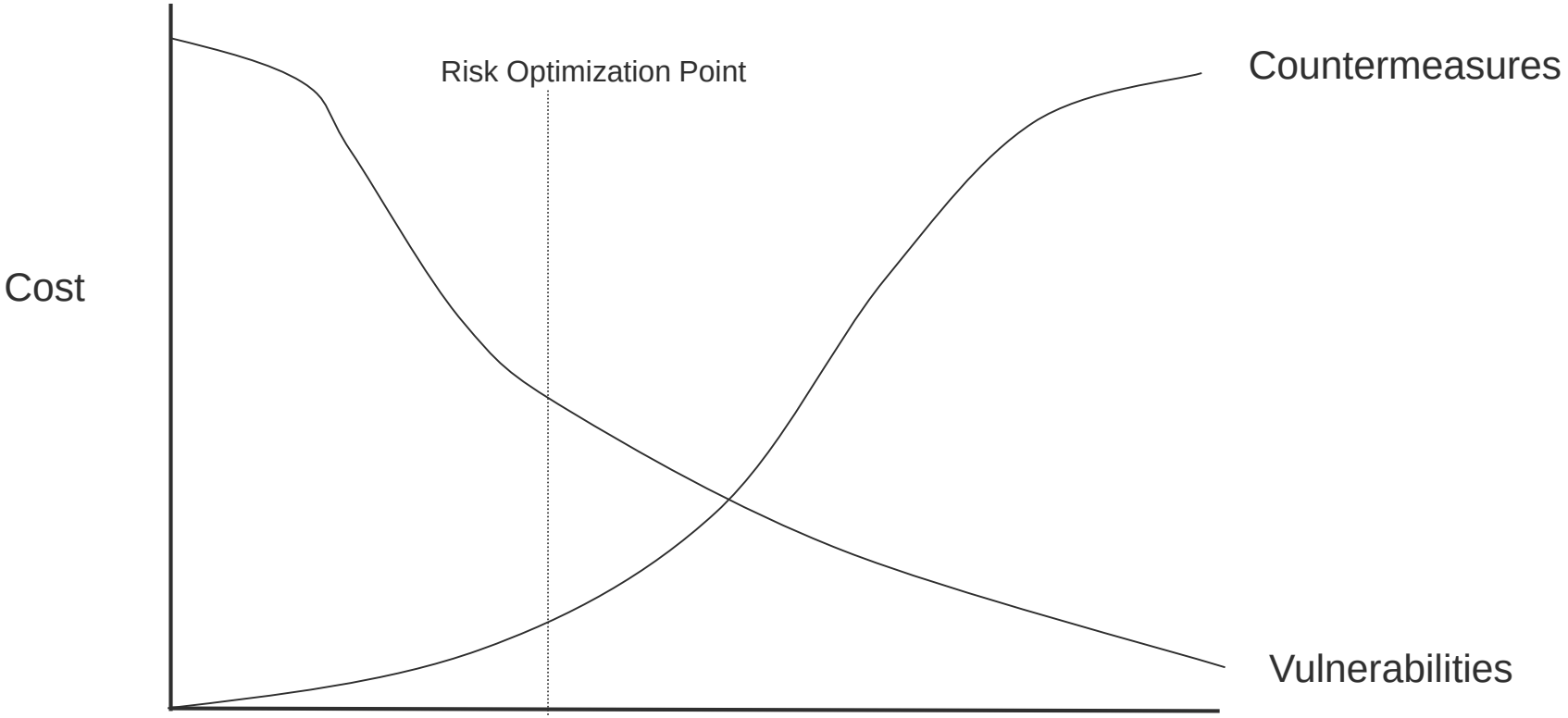
- Fight APT with APS
- Adaptive Persistent Security, but Advanced Persistent Security is a better buzz term
- Security programs must be adaptive
- Security programs must assume failure
- Designed to presume failure
- Extrusion prevention > Intrusion prevention

Risk Management Implies Failure is Acceptable

- IRS hack demonstrates availability requires better detection, not security
  - It can be more cost effective
- 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

PHISHLABS

Optimizing Risk



PHISHLABS

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

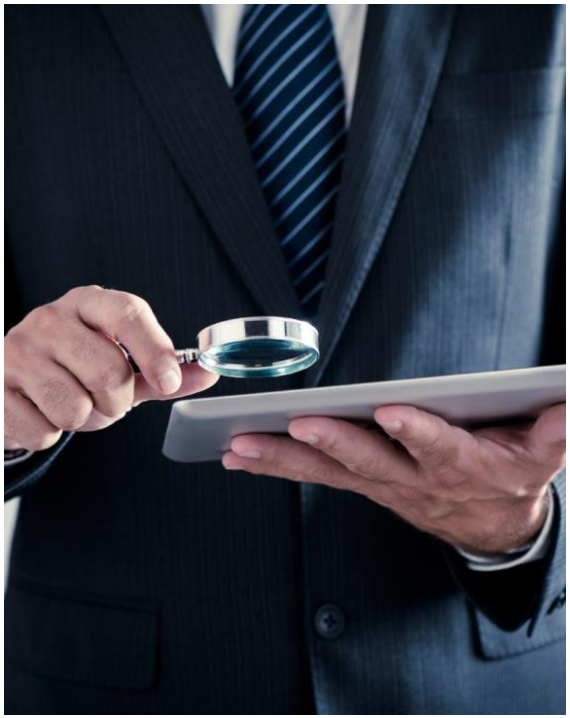
Defensive Information Warfare

PHISHLABS

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

PHISHLABS

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

PHISHLABS

The Role Security Culture/Awareness

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

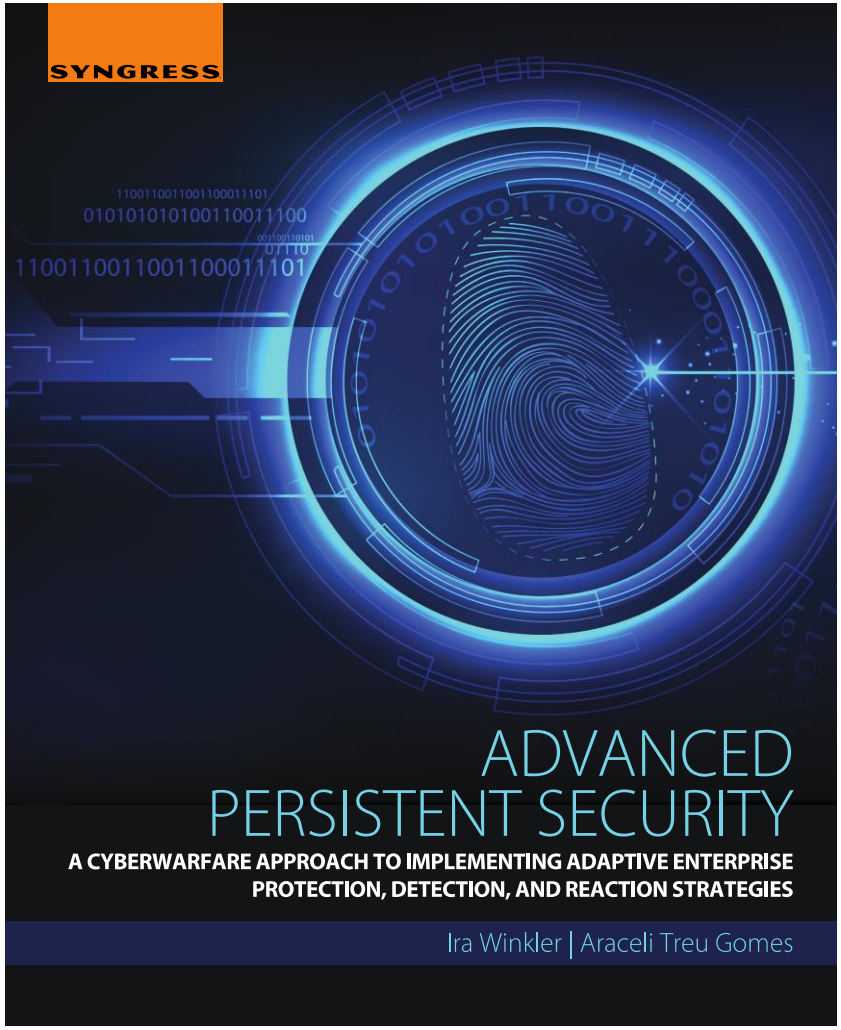
PHISHLABS

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

The Book, The Myth, The Legend

Subscribe at www.irarireport.com for info



PHISHLABS

For More Information

PHISHLABS