RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

SESSION ID: TTA-R09

"Sophisticated Attacks"
The New Normal for Security Programs
Defining the Irari Rules

Ira Winkler, CISSP
President
Secure Mentem
@irawinkler

Araceli Treu Gomes
Principal Subject Matter Expert
Dell SecureWorks
@sleepdeficit_

Cyber Warfare…For Dummies?

The Media loves a good story, and we give them what they want

- Spoon-feeding
- Confuse the “who” with the “how”
- We love a bad drama
- We love a good conspiracy!

Why This Matters to Us

- Destroys focus
- Changes the story
- Asks questions that shouldn't be asked
- 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”

- Sony
- Target
- CENTCOM and TV5 Monde
- Everything is sophisticated according to someone

Internationalization

- Featured attacks are generally US targets
- However, they are nation-state or international criminal attacks
  - Examples are well researched
  - Other examples are hard to come by
- Same attackers and vectors used throughout the world
- Victims are irrelevant

It Can Also Help You

- Gets people talking about security
- Narratives can help the cause
- Highlighting common vulnerabilities can result in more funding
- Highlighting where existing security would have stopped the attacks can result in more support

Looking at Target

- Began with phishing message to vendor
- Used vendor network to compromise business network
- Identified targeted systems
- Set up exfiltration servers
- Exfiltrated data
- Went undetected

Sophisticated?

- Attackers were disciplined
- Attackers were persistent
- Preventable? HELL YES!
  - Network monitoring tools ignored
  - Phishing messages expected
  - Improper network segmentation
  - Lack of whitelisting on POS

Examining Sony

- Attackers were North Korean
  - Get over it
- Spearphishing attack stole admin credentials
  - Hardcoded credentials in malware
  - Accessed critical systems
- Destroyed key systems
- Downloaded lots of data

Sophisticated?

- Attackers were fairly disciplined
- Attackers were very good at getting in the network
- Preventable: HELL YES!
  - Malware should have been detected
  - No multifactor authentication
  - Passwords were static

CENTCOM/TV5Monde

- World reaction:
  - ISIS is so sophisticated!
  - How can US Government systems be so vulnerable? Are classified systems at risk?
  - How can a major media source be so vulnerable?
- Politicians horrified and demanded answers
  - “An unacceptable insult to freedom of information and expression”
- It was Twitter! It was YouTube!
- The password was broadcast on TV!

Sophisticated?

- Takes some work to figure out who has access to accounts
- But still a likely spearphishing attack, or an easily guessed password
- All you had to do was watch TV
- From there it was just a free-for-all

IRS Breach

- 104,000 records compromised through Get Transcript function
  - 200,000 attempted breaches
- Compromised authentication scheme
- Required “information only 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 was credit reports
- Used commercial identity challenge system that asked questions from credit reports
- Went undetected for 200,000 relatively intensive attempts

Preventing the Target Attack

- Management who knew not to ignore network monitoring tools
- Warnings to vendors
- Proper segmentation of business networks
- Configuration monitoring
- Whitelisting
- Better monitoring

Should any of this not have been in place?

Preventing the Sony Attack

- Multifactor authentication for admin accounts
- Changing admin passwords on periodic basis
- Network monitoring for unusual activity
- Anti-malware tools in place
- DLP for critical files…like movies

Preventing the ISIS Attacks

- Better passwords
- Multifactor authentication
- Maybe not putting passwords on TV?

Preventing the IRS Attack

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

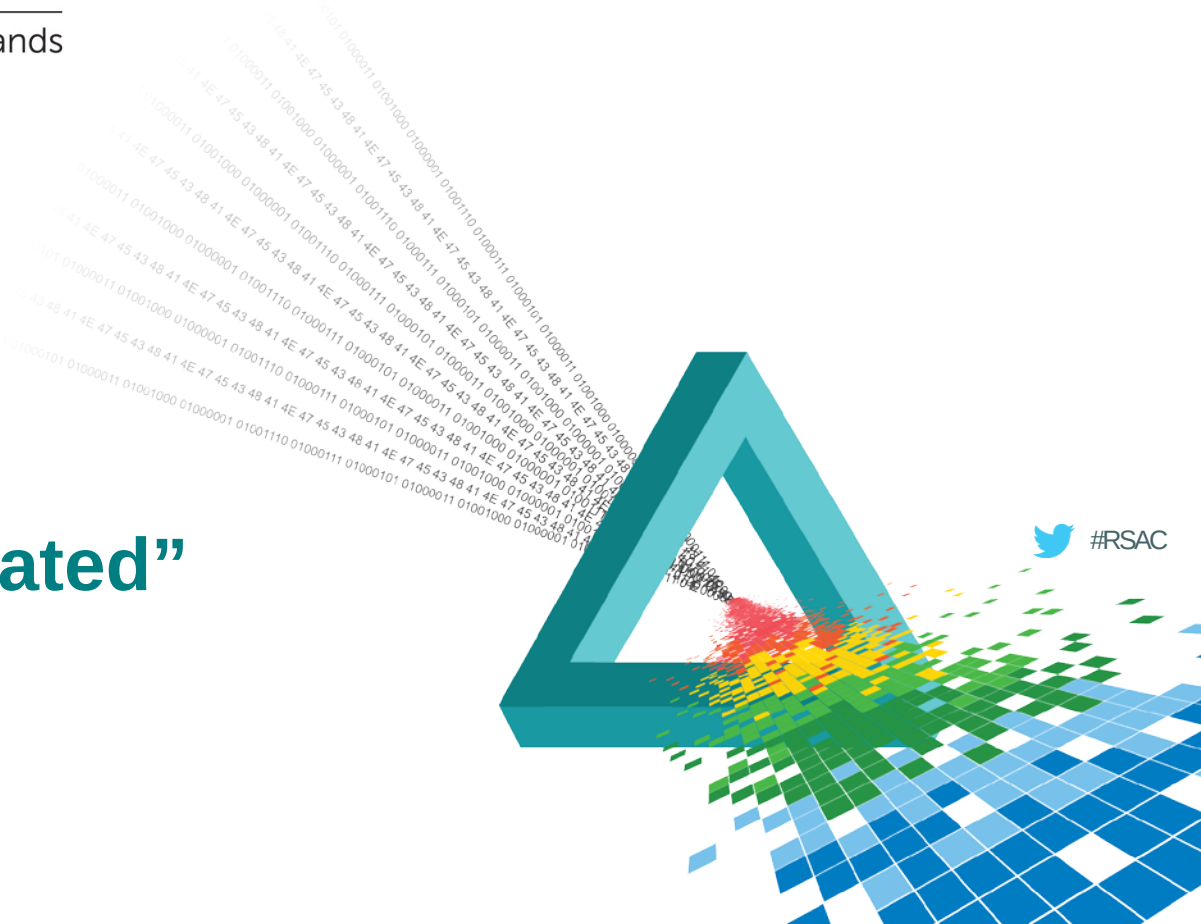
Operation Lotus Blossom

- Just to prove the point
- More than 50 attacks against governments and military organizations across Southeast Asia
- Launched with spearphishing attack
- Exploits well-known Microsoft Office vulnerability
- Installs “Elise” backdoor
- All preventable

The Common Threads

- Known vulnerabilities
- Lack of multifactor authentication
- Poor or lack of network monitoring
- Poor user awareness
- Poorly configured access controls
- Lack of or outdated anti-malware
- No DLP

A Real “Sophisticated” Attack



The Equation Group

- Sup ystems
- Exp ntrol
  vuln
- Insta
- Und
  look
- Req
  hard drives

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

What Constitutes a “Sophisticated” Attack?

#RSAC

You Know It When You See It

- It’s like pornography
- It’s complicated
- It can’t be stopped with security countermeasures that “should” be in place
- Methods make attacks sophisticated
- Not based upon the damage or results
- Not based upon the “persistence” of the attacker
  - APT attacks are persistent, but not necessarily sophisticated

It’s easier to say what is NOT “Sophisticated”

The Irari Rules:

It Is NOT A Sophisticated Attack If…

…The Attack Began With A Phishing Message

- Limited advanced techniques against people
- Stupidity/Ignorance doesn't take a lot to exploit
- The "Stupidity" is often on the part of the security team for assuming Common Knowledge (common sense?) among users
- Default cause is that awareness programs are insufficient
- For a phishing message to be successful, it has to go through many layers of security countermeasures, not just a user
  - Refer to Ira's other presentation on the phishing kill chain

…The Malware Used Should Have Been Detected

- Too many attacks, such as Sony, used known malware
- Failure to detect known malware is a sign of a poor security program
- There really isn't much more to discuss
- Sadly, this needs to be said

…Passwords Were Likely Guessed

- Easily guessed passwords are way too common
- Usually results from account access being shared or poor security policies
- Again, this is just indicative of a poor security program

…User Awareness Exploited With Poor Awareness Program In Place

- CBT is not an awareness program, it is training
- Phishing simulations are not awareness programs, they are usually teaching people to detect simulated phishes

…Known Vulnerabilities Were Exploited

- Known vulnerability means attacks could have been prevented
- If a string of known vulnerabilities was exploited, the attack should have been prevented…
- Even if a patch was not available, other mitigations can be put in place, such as turning off unnecessary services and ports

Big indication of poor security program

…Multifactor Authentication Was Not Used On Critical Systems

- Critical systems, and especially admin accounts, should have this basic protection in place
- Stops password reuse, bad passwords, password sniffing, etc.

Props to JPMorgan Chase for acknowledging a recent hack resulted from not having multifactor authentication in place

…Passwords Were Hardcoded Into Malware

- Just like the Sony Attack
- Demonstrates that even if there is no multifactor authentication, they don't regularly change passwords

Big indication of poor security program

…Detection Mechanisms Were Ignored Or Not In Place

- Should be IDS/IPS in place
- Should be DLP in place on critical systems
- Should be network monitoring in place
- Should see movies go out of your organization
- Should see 100,000,000 credit cards go out of your network
- If you're not looking for that, shame on you

Most important, you should not ignore the warnings when they occur

…Poor Network Segmentation Was In Place

- Vendor networks should not connect to POS
- Business networks should not be connected to SCADA systems
- There should be a conscious network design in place that incorporates risk, not just cost

…User Accounts Had Excessive Privileges

- Low level account compromises should not lead to critical data
- Demonstrates poor administrator procedures

Big indicator of a poor security program

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
- Detection capability was in place and not ignored
- Proper network segmentation in place
- User accounts had minimum privileges

Apply Slide

- Hype impacts our ability to be effective
- Make use of the hype
- “How” dictates sophistication; “how” first, “who” later
- Unsophisticated attack vectors tell where countermeasures are required
- If it happens to someone else, it is likely happening to your organizations, so get countermeasures in place

For More Information

Ira Winkler, CISSP

- ira@securementem.com
- +1-443-603-0200
- @irawinkler
- www.securementem.com
- www.linkedin.com/in/irawinkler
- Facebook.com/irawinkler

Araceli Treu Gomes, Dozens of Certs

- ari@killchain.net
- @sleepdeficit
- www.linkedin.com/in/sleepdeficit
- Facebook.com/sleepdeficit
- www.irarireport.com
- @irarireport.com