SESSION ID: EXP-F03

The Sophisticated Attack Myth: Hiding Unsophisticated Security Programs:

The Irari Rules of Classifying Sophisticated Attacks

Ira Winkler, CISSP

President
Secure Mentem
@irawinkler

Araceli Treu Gomes

Principal Subject Matter Expert
Dell SecureWorks
@sleepdeficit_

Preamble

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

We the People

- Spoon-feed it to them
- Want to know who is responsible for attacks
- Confuse the “who” with the “how”
- We love a bad drama
- We love a good conspiracy!

Why This 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"

- Sony
- Target
- CENTCOM
- 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

Looking at Target

- Went in through phishing message to vendor
- Worked through 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 NO!
  - Network monitoring tools ignored
  - Phishing messages expected
  - Improper network segmentation
  - Lack of whitelisting on POSs
  - No monitoring
  - Etc.

Examining Sony

- Attackers were North Korean
  - Get over it
- Likely spearphishing attack
- Used credentials in established malware
- Accessed critical systems with credentials
- Destroyed key systems
- Downloaded lots of data

Sophisticated?

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

CENTCOM

- 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

Sophisticated?

- It does take some work to figure out who has access to the accounts
- But again, it was likely a spearphishing attack, or more likely an easily guessed password
- From there it was just a free-for-all

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 a periodic basis
- Network monitoring for unusual activity
- Anti-malware tools in place
- DLP for critical files…like movies

Preventing the CENTCOM Attack

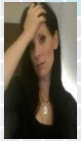
- Better passwords
- Multifactor authentication

The Common Threads

- 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

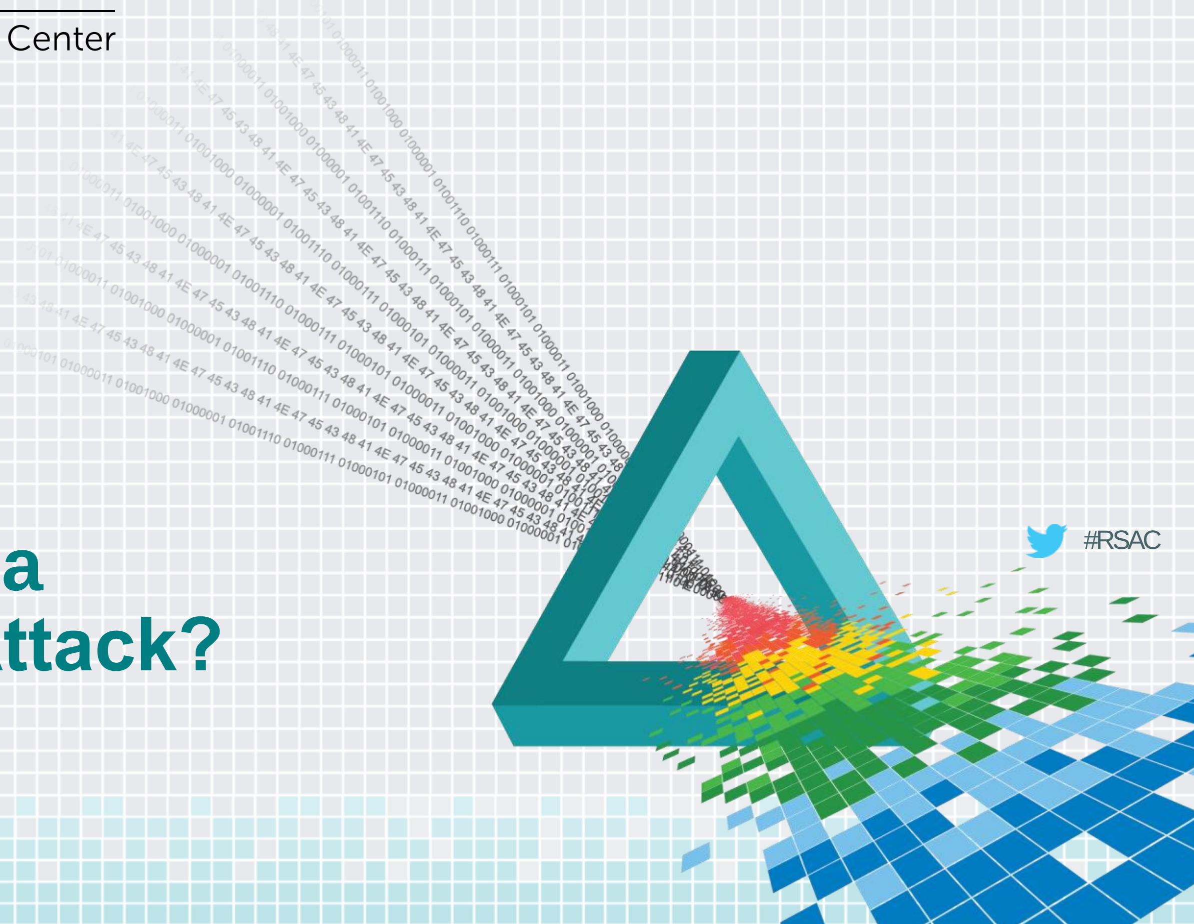


- Sup ... nd
- Exp ... vuln ... &
- Insta
- Und ... look ... aps
- Req ... years hard drives

RSAConference2015

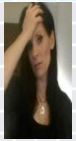
San Francisco | April 20-24 | Moscone Center

What Constitutes a “Sophisticated” Attack?

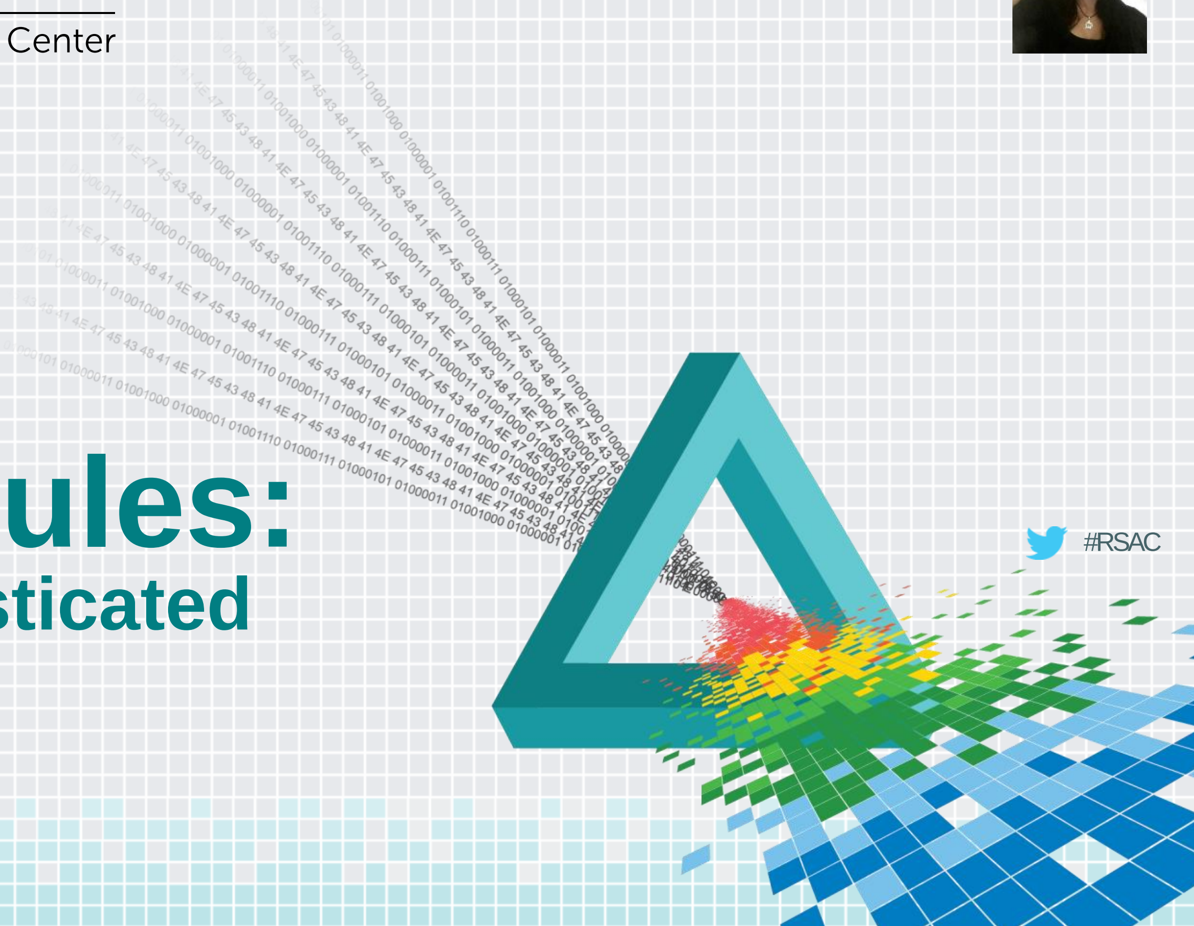


#RSAC

You Know It When You See It



- It’s like pornography
- It is complicated
- It can’t be stopped with security countermeasures that “Should” be in place
- Methods are what make attacks sophisticated
- It is not based upon the damage or results
- It is not based upon the “persistence” of the attacker
  - APT attacks are persistent, but not necessarily sophisticated
- It is easier to say what is NOT “Sophisticated”



The Irari Rules:

It Is NOT A Sophisticated Attack If…

…The Attack Began With A Phishing Message

- There are 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
- The 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 (TECH-R01)

…The Malware Used Should Have Been Detected

- Too many attacks, such as Sony, used known malware
- The 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

- If a known vulnerability was exploited, the attack could have been prevented, and likely should have been prevented…
  - It is another indicator of a poor security program in place
- If a string of known vulnerabilities were exploited, the attack clearly could 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

…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
- It demonstrates that even if there is no multifactor authentication, they don’t regularly change passwords, which demonstrates bad security programs

…Detection Mechanisms Were Ignored Or Not In Place

- There should be IDS/IPS in place
- There should be DLP in place on critical systems
- There should be network monitoring in place
- You should see movies go out of your organization
- You 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

© America Revealed

…User Accounts Had Excessive Privileges

- Low level account compromises should not lead to critical data
- It demonstrates poor administrator procedures
- Indicative of a poor security program in place

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

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

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

SECURE MENTEM