Applying Security Intelligence

Ira Winkler, CISSP
Ira.winkler@issa.org
+1-443-603-0200

Araceli Treu Gomes
The Sony Hype

• Everyone is focused on North Korean involvement
• Incredible PR for The Interview
• Reporting is tinged
• The focus takes away from the underlying problems
• It does deflect blame
APT – The Gift That Keeps Giving

• APT is the dragon of the modern age
• Everyone blames APT for attacks
• Responsible for power grid, government, banking, critical infrastructure, etc. hacks
• People tune out
• To the average person, it just makes it seem impossible to stop
• It’s like fighting a dragon…you can’t
What is Intelligence?

• Data vs Information vs Intelligence
• Data is raw fact
• Information is organized data
• Intelligence is organized information
• Some intelligence is actionable
What is Security Intelligence?

- Intelligence about the Cyber Threat in this context is Security Intelligence
- Defines who is targeting you and how
- Defines why you are a valuable target
  - Unfortunately some organization, don’t realize this
- Should help define your security program as a whole
Characteristics of Good Intelligence

- Current
- Relevant
- Actions
- Willingness to refine and discard
  - Too many people don’t want to concede that some seemingly valuable data is not useful
It Does Matter

• The “Who” tells you a great deal
  – Their methods
  – Their targets

• Allows you prioritize countermeasures
Methods

• Threats have preferred attack strategies
• They have preferred tools
• They operate in predictable ways
Predictable Targets

• They value different pieces of information
• They will target specific types of systems
• If you realize they are into some systems, you know what other systems and data to look at
Syrian Electronic Army

- They target media outlets
- They want to embarrass the organization by compromising their website or social network accounts
- Search for random people employees through the Internet
- Set up fake login site to get User IDs and passwords
- Send spear phishing message using ruse to look at an article link
- Addressed from an executive
- No direct technical damage
SEA Continued

• Target third parties to get at their victims
• Victims are not usually aware that they are intended victims
• Leave some accounts unexploited to use later
• Exploit email accounts to send out to mailing lists and coworkers, others from an apparent legitimate source to expand compromise
Implementing Countermeasures

• Intelligence tells you which vulnerabilities will be exploited
• Prioritize countermeasures based on likely attacks
• Prioritize protecting most targeted data
SEA Countermeasures

- Lock domains
- Implement multi-factor authentication
- Alert staff to pending attacks
- Alert staff to report suspicious messages
- Upon attack, block offending domains
- Delete potential phishing messages on server
- Force password resets for all employees
- Monitor for unreported or undetected compromise
Intelligence Application

- Programs don’t need intelligence, but it would make them more effective
- Prioritizes spending
- In-house vs contracted
- More is not always better
  - The Paradox of Choice concept
- Requires ongoing effort and collection
Final Notes

• Security Intelligence requires continual effort
• Can create useful security programs without Security Intelligence, but they are more effective with it
  – Only if its good intelligence
For More Information

http://www.securementem.com
@securementem

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