The Myth of Automated Hunting and Case Studies in ICS
Who Are We

• Robert M. Lee
  @RobertMLee
  • CEO and Founder, Dragos, Inc.
  • SANS Institute Certified Instructor and Course Author (FOR578 & ICS515)
  • Previously U.S. Air Force in the Intelligence Community
  • Writer, Little Bobby
Today’s Three Takeaways

• A Historical View of Threat Hunting
• Why Threat Hunting Cannot be Fully Automated
• Approachable Use-Cases in Industrial Control System environments
What is Threat Hunting?

**Little Bobby**

WHAT ARE YOU DOING?
INSTALLING NEXT-GEN SOFTWARE TO PROTECT ME AGAINST FOREIGN GOVERNMENTS.

WHY IS THERE A POPUP SAYING YOU STILL NEED TO PATCH YOUR SYSTEM?

I'LL GET TO THAT LATER.

by Robert M. Lee and Jeff Haas
Where “Threat Hunting” Emerged

• “Hunting” originated in Department of Defense in early to mid 2000’s

• Air Force Computer Emergency Response Team had “hunter-killer” missions and NSA had it’s “hunts” for “APTs”

• Richard Bejtlich published one of the first articles on it (right) in 2011 after taking the AFCERTs lessons learned to the GE-CIRT

• Focus was always on “hunting trips” of personnel searching for threats prior to an incident

Ref: https://taosecurity.blogspot.com/2017/03/the-origin-of-threat-hunting.html
Why Threat Hunting Cannot be Fully Automated
The Sliding Scale of Cyber Security

- **ARCHITECTURE**: The planning, establishing, and upkeep of systems with security in mind.
- **PASSIVE DEFENSE**: Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction.
- **ACTIVE DEFENSE**: The process of analysts monitoring for, responding to, and learning from adversaries internal to the network.
- **INTELLIGENCE**: Collecting data, exploiting it into information, and producing Intelligence.
- **OFFENSE**: Legal countermeasures and self-defense actions against an adversary.
Dissecting the Hunting Maturity Model

Ref: David Bianco
http://www.threathunting.net/

#ThreatHunting cannot be automatic. If it was automatic - we'd call it IDS.
Threat Hunting requires the focus to be on the people.

Your job focuses on human adversaries but you may not encounter adversaries.

You need the open-mindedness of a new person but hunting is not for new folks.

Product vendors will pitch hunting but it’s not about the product.

You need to rely on automation but you can’t fully automate hunting.
Approachable Use Cases in Industrial Control System (ICS) Networks
Stage I mimics a targeted and structured attack campaign.
Stage 2 shows the steps associated with a material attack that requires high confidence.
Hypothesis Generation

Friendly or Threat Intelligence

Situational Awareness

Domain Expertise
Case Study: Intelligence Driven Based Hypothesis in Manufacturing

Setting:
A manufacturer’s integrator’s networks

Intelligence:
Active adversary group potentially causing destruction (intention unknown)

Future Automation:
It’s on the external party; however notification of incidents required in Master Services Agreement and communication established for future

To transition to Stage 2 threat needs insight

Most sensitive data not stored in the ICS

Engineering documents and schematics

Check breach of integrator’s networks

Determine if there is risk to manufacturer
Case Study: Situational Awareness Based Hypothesis for Construction

Setting:
Construction projects around Africa

Situational Awareness:
Announcement of new construction projects offer opportunities to get in early for adversaries and build targeting decks

Hypothesis:
Adversaries will leverage these project announcements to start their campaigns

Test:
Gain access to data in those environments and set up honeypots/emails/etc. to search for early stage adversary recon

Hydroelectricity
Ethiopia opens Africa’s tallest and most controversial dam

The Gibe III dam has the capacity to double the country's electricity output at the flick of a switch
Case Study: Domain Expertise Based Hypothesis in a Water Utility

Setting:
Water facility in the plant networks

Domain Expertise:
Updates are performed during maintenance windows

Hypothesis: Spikes in bandwidth & version of patches
Test: Baselining of traffic and manual checking of patch versions
Uncovered: Bitcoin mining and adversary “defending the hill”

Future Automation:
Host based log collectors to identify updates and threshold setting for bandwidth
Additional detection around encrypted communications
Recap

• Threat Hunting is a human process pitted against human adversaries
• Automation is key to supporting hunting but must be leveraged appropriately
• Hunting for threats in an ICS is important for safety and reliability
Stay in Touch:

@_LittleBobby_
www.LittleBobbyComics.com

Questions?
@DragosInc
www.Dragos.com

@RobertMLee
RLee@Dragos.com

LITTLE BOBBY

WE NEED A CONGRESSIONAL BILL FOR ACTIVE DEFENSE.

YES! INCENTIVIZE FOLKS TO MONITOR NETWORKS AND PERFORM INCIDENT RESPONSE!

NO, I MEAN HACK-BACK.

BUT THAT'S NOT AN ACTIVE DEFENSE... NOR EFFECTIVE!

by Robert M. Lee and Jeff Haas

BUT IT SOUNDS SO COOL!