Offense Must Inform Defense: Why Proper Incident Response is SO Important!

Jonathan Ham, GSEC, GCIF
jham corp.
jonathan@jhamcorp.com
@jhamcorp
Interlude: Not Quite The Talk That I Had Intended

- Storm blew through Missoula, MT
- Branches and entire trees down everywhere
  - power lines setting fires
  - trees blocking emergency vehicle routes
- Knocked out power for almost all residents
  - though not my office downtown
  - and also, UPSes :-)
MISSOULA: NO DATA FOR YOU!

- No Internets AT ALL!
  - Not via cable, DSL, or even CDMA! (for a while)
  - Upstream fiber disruption?
- Wanted to contact Dr. Cole about possible flight disruption.
  - Oops, no txt or email.
  - Tried to call. Land line dead.
- Voice via cell: Yay! But?
Interlude: When It Isn't Mz. Nature

- Step 1: Break the Infrastructure
- Step 2: ???
- Step 3: Profit!
The Necessity of Proper Incident Response: Topics

- We Are Engaged in Battle
- Bad Things Will Happen
- How We Respond Determines How Bad Things Are, or Become
- The Six Steps of Proper Incident Response
- Emphasis: Preparation
- Emphasis: Lessons Learned
- Offense Must inform Defense
We Are Engaged in Battle

- War in multiple contexts and scales
  - Nation State vs. Nation State
    - Stuxnet and other unknown efforts
    - SANS's Cyber Guardian program
  - Enterprise vs. determined adversary
    - "Smart Grid" attacks
    - Corporate espionage
    - Phishing and fraudulent transactions
  - Company vs. Company
    - Market share and mind share
    - Much of the same dynamics apply
  - Good Guys vs. Bad Guys
Bad Things Happen to Good People

- They will happen whether you're prepared or not
  - They will certainly happen if you're not prepared
    - and worse yet, then you're probably not instrumented
    - and so you won't even know...
    - *(unless your mouse starts moving on its own)*
  - They will happen even if you are prepared
    - and maybe you're even instrumented
    - but do you monitor and audit everything you can?
- We must be prepared to respond!
Every time you network, you are on the battle field.

If you are a Target of Interest (ToI), you will be breached.
- You might be watching, but...
- Very sophisticated attackers are for hire
- Always Pivot Technique (APT)

If you are a Target of Opportunity (ToO), you will be breached.
- You probably won't see it coming
- Then once breached, you become a ToI
- No one likes their ToIs taken away!
Security Monitoring, Intrusion Detection, Analysis & Response

- 20+ years. US federal agencies, private industry across all sectors
- dozens (?) of networks and data centers inspected
- hundreds (?) of incidents addressed
- one network without indicators of compromise (IoCs)
  - agency with real determination to be clean
  - ten years ago
  - probably I missed something
- Bottom line: defense is not dominant
How We Respond Determines How Bad Things Are, or Become

- The Six Steps of Proper Incident Response
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned

- Do them correctly, and the patients live
- Miss a step, and we near the tipping point where no one does
Emphasis: Preparation

- Please do not do this ad hoc. At. All. Ever.
- Learn from the preparation activities of other areas of human persistence!
  - Persistent readiness
  - Live-fire training
  - Team building
  - Expectation of fleet casualties
  - Expectation of team casualties too
- Be outfitted and ready to run an incident to ground
  - Forensics gear
  - Forensics training (at least for evidence extraction)
If you miss this step, you fail. Fail. Fail. Fail.

Did I say Fail?

Two lessons must be learned

The first is most obvious:

- How can we stop this from happening again?
- Needs to be a consensus report from the team that handled the incident.
- Dissenting opinions documented as well!
- Must feed back to the enterprise preventive posture!

The second is most often overlooked:

- WHEN this happens again, is there a better way we could have handled it?
- Must feed back to the IR team's internal documentation.
This is where incidents get run to ground.

- Offensive training is too often a low priority for our defenders.
- But how can one identify Indicators of Compromise (IoCs) if they have never seen them first hand?

We must train our responders and forensicators like hackers (ethical pen testers)!

We must train our ethical pen testers like forensicators, so they can share what they know about the IoCs they leave behind!

These are not separate disciplines.

- These are essential compliments!
- Yin/Yang
"Threat Intelligence" Starts at Home

- Please, do watch the public spaces
  - Vendor reports, ISC, etc.
- But also, find your own IoCs, and then share them!
- The Bad Guys learn from each other.
- If we don't do the same, we're sunk.
Questions? Comments?

Jonathan Ham, GSEC, GCIH
jham corp.
jonathan@jhamcorp.com
@jhamcorp