Hunting: How To Start, Go Down a Rabbit Hole, and Get Out

DR. CHELSEA HICKS
TWITTER: @THEDRPINKY
About Me

• I’m a Linux & Windows threat hunter for the USAF
• Also enjoy research in DFIR
• PhD in Information Technology, MS in Information Technology, BS in Computer Science
  • Dissertation Title: Redefining Information Systems Risk for Automated Severity Risk Assessment
• Help coordinate various groups in San Antonio, including BSidesSATX
• Mandatory Disclaimer: All views/thoughts/opinions are of my own, and are not representative of my employer or any official policy.
What are we talking about today?

• Define Threat Hunting
• What’s a Rabbit Hole?
• Are Rabbit Holes Worthwhile?
• Recovery from Rabbit Holes
• Conclusion
Define: Threat Hunting

❖ Process of proactively and interactively searching through your enterprise to potentially find the bad guy

Image from: https://www.recordedfuture.com/cyber-threat-hunting/
Threat Hunting: How It Works

- Baselining
- Investigate
- Malicious
- New IOC
- Improve

Threat Hunting with Intel
How Do You Become Better?

- Data collection
- Intelligence utilized
- Tools utilized
- Automation
- Improving yourself
## What Does Every Threat Hunter Have in Common?

<table>
<thead>
<tr>
<th></th>
<th>Beginner</th>
<th>Expert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tools:</strong></td>
<td>Heavy Reliance</td>
<td>Some Reliance</td>
</tr>
<tr>
<td><strong>Data:</strong></td>
<td>Overwhelmed</td>
<td>Better Sifting</td>
</tr>
<tr>
<td><strong>Specialization:</strong></td>
<td>None</td>
<td>One/Multiple</td>
</tr>
<tr>
<td><strong>Intel:</strong></td>
<td>Basic</td>
<td>Always</td>
</tr>
<tr>
<td><strong>Hunt Technique</strong></td>
<td>Poor/None</td>
<td>Hypothesis Based</td>
</tr>
<tr>
<td><strong>Pattern Recognition?</strong></td>
<td>Little</td>
<td>Often</td>
</tr>
<tr>
<td><strong>Utilize Lifecycle</strong></td>
<td>Little</td>
<td>Always</td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>Ineffective</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Rabbit Holes</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
“In another moment down went Alice after it, never once considering how in the world she was to get out again. The rabbit-hole went straight on like a tunnel for some way, and then dipped suddenly down, so suddenly that Alice had not a moment to think about stopping herself”

-Lewis Carroll, Alice’s Adventure in Wonderland

Image from Janice Tauro (“journeybunney”), image titled “Falling Down The Rabbit Hole”.

Image obtained from: https://journeybunnyart.tumblr.com/post/125112143225/falling-down-the-rabbit-hole-commission
What is a Rabbit Hole?

• Threat Hunting Definition: The trip a hunter takes when they’re investigating a potential lead that becomes out of control/outside of scope

• Examples in Threat Hunting:
  • Nessus Scan Creating Strange Logs
  • Jumping into Forensics over Blue Team Artifacts
  • Alert Indicating That Chrome is Malware
Rabbit Hole Conceptions

In this instance, the detection is revealed as a false positive, my digging stops and the rabbit hole is dodged. By reducing the amount of information to triage, I can see clearly that there were no malicious triggers. In this instance I was able to determine that the user clicked a link in an email in Outlook, that it took them to a legitimate website running on the local network, and that the only processes running were from known good locations.

While we were unable to identify any additional information related to the state board of election attacks, reviewing hosting resolutions for the 5.149.249[.]172 IP address clued us into another target of these actors. Passive DNS analysis of this IP revealed domains typosquatting a website for Turkey’s ruling AK Party hosted between March and August 2016. Investigation of this typosquat took us down the rabbit hole that ultimately uncovered evidence of a recent spearphishing campaign primarily targeting individuals affiliated with Turkish and Ukrainian political organizations.

https://threatconnect.com/blog/state-board-election-rabbit-hole/
Summary

LET IT GO, LET IT GO

YOU WILL FALL DOWN A RABBIT HOLE
Why Are Rabbit Holes So Scary?

• They’re potentially never ending
• Can result in nothing noticeably gained
• May miss out on something else actually bad
• Can result in the hunter being demoralized
So What Should You Do?

Never Go Down A Rabbit Hole
Rabbit Holes Are Worthwhile

• There is ALWAYS something to be gained
  • Experience
  • Knowledge
    • OS
    • Tool
    • Artifacts
  • Quirks about the network
  • Lack of policies/Disobeying policies
What To Do?

• It’s a balancing act

• Need to control:
  • How long spent on a rabbit hole
  • When you are no longer ACTUALLY obtaining information from it
  • Priority of assignments/tickets/hunts
  • Sanity
Tips

• Try to provide time limits (but be flexible!)
• Take careful notes
• Keep in mind the initial question that lead you to this rabbit hole
• Have a teammate pull you out/double check
Teamwork

TEAMWORK

SOMETIMES YOUR TEAM JUST SUCKS

makeameme.org
A Threat Hunting Team

Images from http://www.cleanpng.com
Recommended Team Layout (Small)

Images from http://www.cleanpng.com
Recommended Team Layout (Medium)

Images from http://www.cleanpng.com
How Teams Tie Into Rabbit Holes - Story Time

• No Team Example:
  • Blue Team vs Red Team Competition
  • Linux member refused to collaborate
  • Stuck in loop of kicking red team out for 1-2 minutes, before it occurred again
  • Never resolved underlying issue
  • Resulted in team defeat
How Teams Tie Into Rabbit Holes - Story Time

• With Team Example:
  • Suspicious traffic discovered
  • Host and Network analyst both investigated
  • Able to limit scope of traffic to a beacon
  • Customer resolved traffic as legitimate
How Teams Tie Into Rabbit Holes - Story Time

• How the Team Structure Helped
  • Network Analyst well known for finding strange activity
    • Habit results in identifying lots of strange traffic, but not necessarily a resolution
  • Host Analyst was able to help confirm the traffic was strange, and brought to leadership
  • Two analysts together worked together to confirm if intrusion occurred
  • Leader quickly found answer from customer
• Total time spent on rabbit hole was reduced over 50%
Teams - Summary

• Be flexible to what works for your organization

• Must haves:
  • Do not have only one person for a role - always have a partner/backup
    • Does NOT mean two people on every task - just allow natural overlap/pull in for help
  • Try to resolve conflict ASAP
  • Allow rabbit holes to naturally occur, but be willing to step in when frustration occurs and re-vector
  • Make sure rabbit holes turn into learning experiences
What if...

• Hunter goes through same rabbit hole multiple times
• Verify:
  • Hunter is actually learning what is happening and what resolved it
  • Improve training if it is due to lack of knowledge
  • Share the lessons learned with rest of team, to help remind each other “Hey, remember this is X”
  • Improve process (Is there a procedure that results in this rabbit hole?)
• Dissect and fix the issue
Practice. Improve. Repeat
Conclusion

• Rabbit holes are expensive - time and effort
• Don’t aim to eliminate rabbit holes (impossible)
• Aim to learn and naturally reduce them
• Improve processes and hunters via rabbit holes
• Practice and Repeat
Questions?
Find me at:
Twitter: @TheDrPinky
E-mail: dr.c.hicks@icloud.com

Image from https://www.pexels.com/photo/ask-blackboard-chalk-board-chalkboard-356079/