DDOS Postmortem
Postmortem

Who, What, When, Where, Why, How
Who

• Bad Actor
  – Did anyone take credit for the DDOS?
  – Did they target your organization or were you collateral damage?

• Resolution Team
  – Who internally/externally was engaged to assist?
  – Were the internal resources the correct resources to engage?
What

• What was targeted
  – Did the DDOS target an IP, Host, URL, or App?
  – What was impacted; only the target or ancillary assets as well?
  – What was the scope of impact?
    • Internal Systems, Network / Internet Access, Customer facing systems, Business partners
  – What early warning indicators of impending attack exist?

• What systems alerted/failed to alert?
• What was goal of attack? Successful?
When

• When did the event occur (holiday, weekend, night, day)?
• Did the event occur at a business critical time?
  – Financial Reporting
  – Busy time of day
  – Special activity occurring
• When did the attack start?
• When was IR notified of attack?
Where

• Where was the attack focused?
  – Web Sites
  – Branch office
  – Corporate presence

• Are you sure?
  – Is it possible the DDOS was a distraction to obfuscate an exfiltration
Why

- Why were you attacked?
  - Was the attack designed to gain notoriety

- Why did the bad actor select the specific target?
  - Was the attack designed to hide other activity

- Why did we react the way we did?
  - Was our reaction appropriate
How

• How were you attacked?
  – Did the attacker use a strategy
  – Did the attack appear well coordinated

• How did you respond?
  – Did we take the correct response actions
  – Was the attack designed to hide other activity
Now what?

• Document – document the answers to the posed questions

• Document – document the responses to the incident

• Document – document the identified gaps

• Document – the process improvements
Conclusion

• When performing a post incident analysis of a DDOS event, the goal is to qualify the impact of the attack. This is done by answering the Who, What, When, Where, Why, and How of the incident. Along with answering the questions an analysis of the event should be performed to determine improvement opportunities and to update documentation to reduce the impact of the next DDOS attack.
Questions ?