

# Disruption

Baseline, Monitor, Detect, Analyze, Respond, & Recover

Based on SROC class given by Hervey Allen, Chris Evans, and Phil Regnaud 2009 Santiago, Chile



# Overview

- Disruption
  - Concepts, Examples, Motivations
- Hands-on Cyber Attack
  - Concept
  - Establishing a Baseline
  - Demonstration of the Attack
  - Monitoring & Detection
  - Analyzing the Attack
  - Response & Recovery
  - Enacting Mitigation Actions

Router Re-config  
DoS via DNS Queries




# Disruption

- Disruption is the act of denying, degrading, or otherwise limiting the availability of services provided by a system or application

# Disruption

Some Examples:

- Network Denial of Service – using the network protocols against themselves to saturate or overwhelm services or the links required to access them (e.g. SYN flood, DNS query flood)
- Hardware Denial of Service – making a change to the hardware which prevents the device from operating correctly (e.g. BIOS flashing) 
- Service Reconfiguration – changing configurations or operating requirements such that the service, application or system no longer functions as intended (e.g. changing sshd\_config to an unexpected port, disabling Windows services, overwriting system boot files)

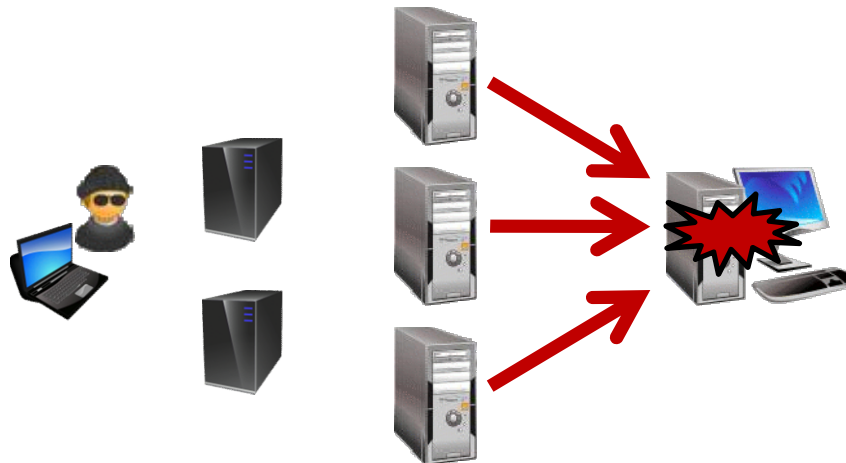


# Disruption

- Disruption can be done without any access to the systems affected
  - DoS, DDoS, Traffic Floods, Amplification Attacks, ...
- Disruption is also possible (and easier) with access to the system
  - Rebooting hosts, router configuration changes, ...

# Disruption

- Network disruption attacks are a battle between attacker's and defender's provisioning capabilities.
  - The one with more bandwidth, servers, capability, etc wins.
- They are typically done with BotNets since they offer an easy method of provisioning more than the defender can muster
- They take many, many forms – bandwidth saturation, malformed packets, server overload, etc



# A Brief Aside – BotNets

BotNet – “A collection of software robots, or bots, which run autonomously and automatically”

- Compromised Hosts (Zombies) are Centrally Controlled by a Single Entity (a Bot Herder)
- Typically Used for Malicious Purposes
  - DDoS, spam, Non-attribution Attacks



# A Brief Aside – BotNets



Bot Herder Establishes a Presence

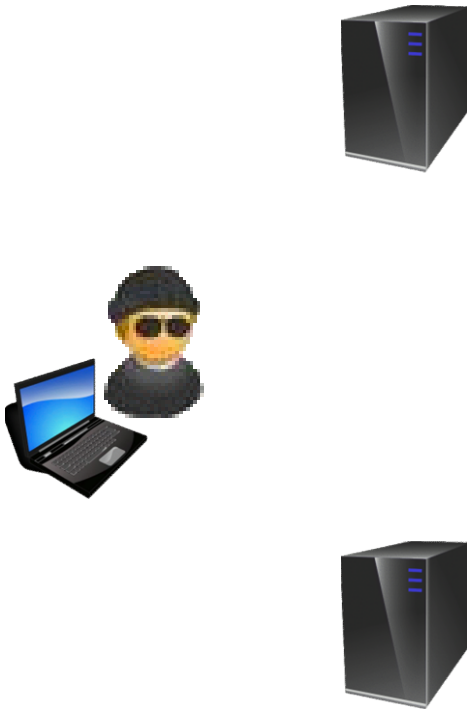


# A Brief Aside – BotNets



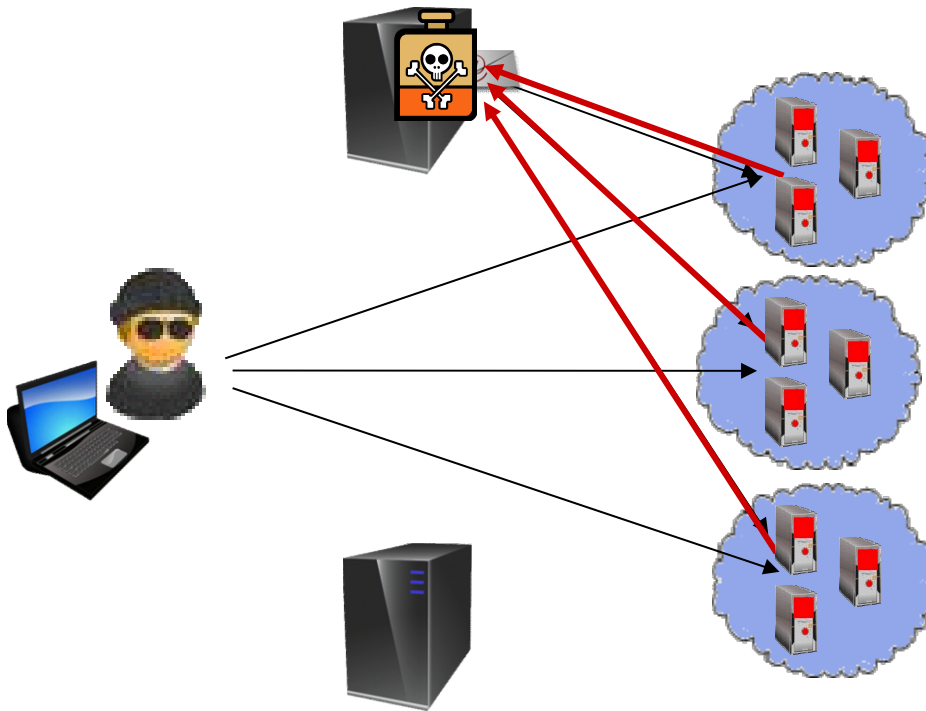
Bot Herder Creates a Delivery System  
- Delivers "BotNet" Payload to Hosts

# A Brief Aside – BotNets



```
Bot Herder Creates DNS Control Server
- Issues Commands to Bots
- Receives Data From Bots
```

# A Brief Aside – BotNets

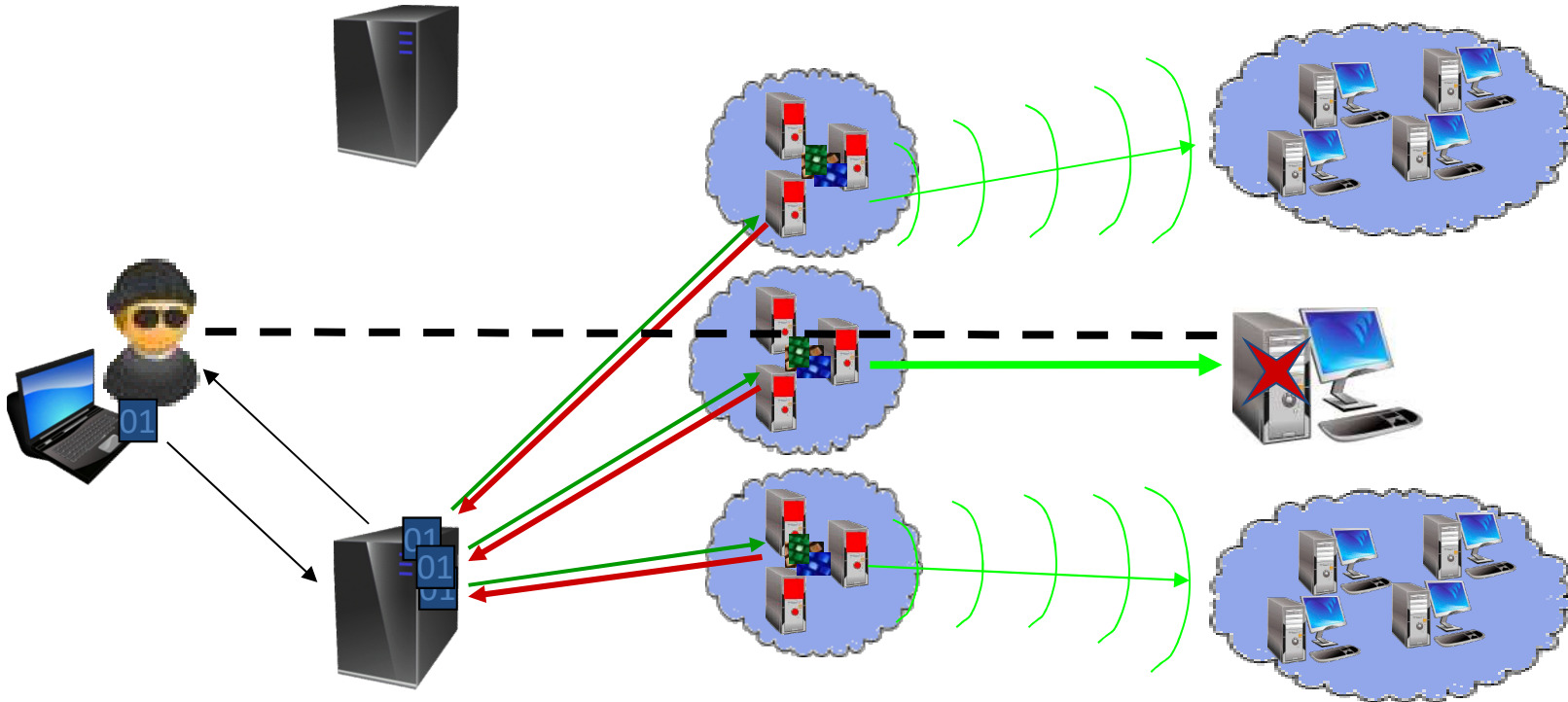


**Bot Herder Identifies Candidate Hosts**

- Sends Baited E-Mail to Hosts
- Hosts Download Bot Malware from Server
- Hosts Become Zombies



# A Brief Aside – BotNets

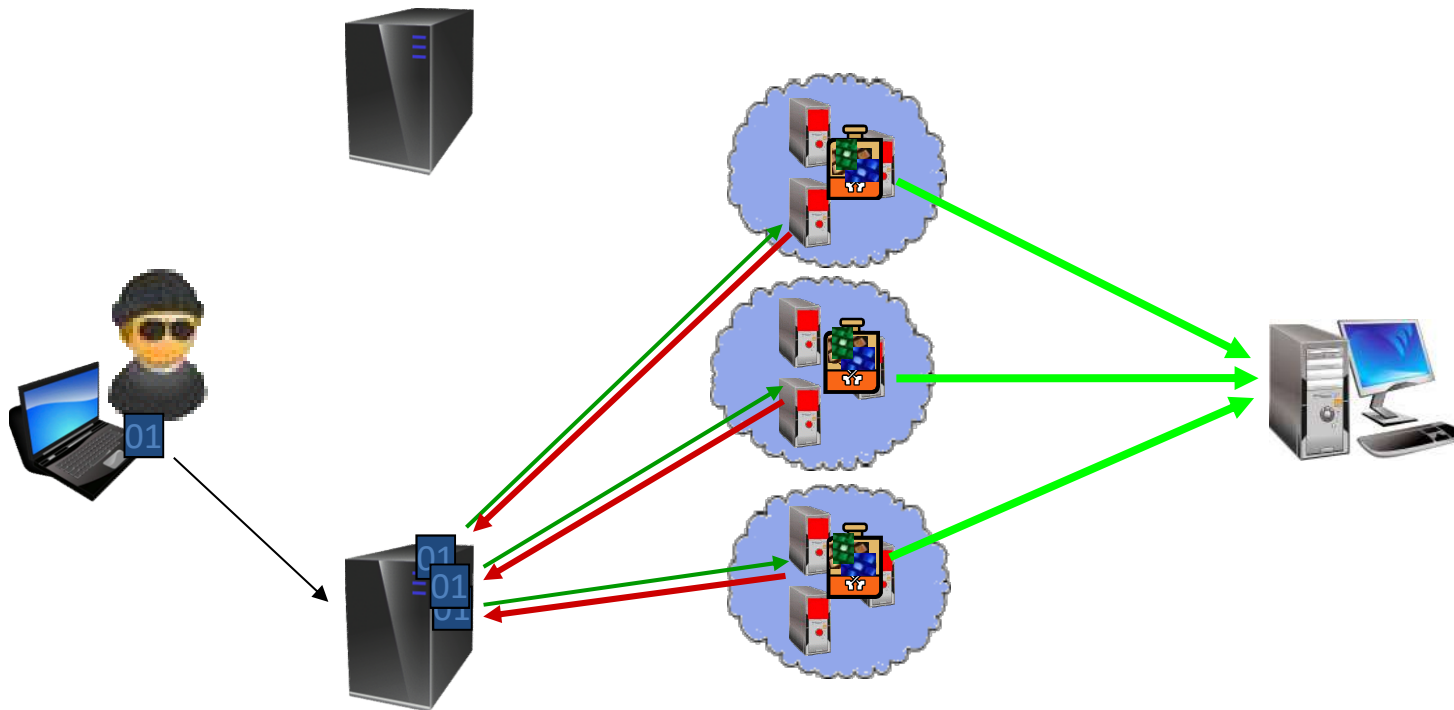


## Bot Herder Identifies Target

- Issues Command via Control Server
- Zombies Receive Command from Server
- Zombies Locate Target
- Zombies Report Back to Server



# A Brief Aside – BotNets



**Bot Herder Launches Attack at Target**  
- Issues Command via Control Server  
- Zombies Attack Target  
- Bot Herder Issues Stop Command



# Disruption

- Hardware disruption attacks can be done remotely, but are easier to pull off with physical access
  - Ease of system administration = vectors for attack
  - Some hardware manufacturers allow remote flashing of system BIOS
  - Physical access = complete control
  - Don't forget the obvious hammer to the PC trick



# Disruption

- Service reconfiguration attacks can be done remotely or locally, but almost always require some sort of access (recall privilege escalation)
  - Overwrite boot files
  - Delete critical OS files
  - Modify or create a hosts file
  - Modify application configuration files
  - Stop or disable MS Windows services
- System administration tasks can turn into service reconfiguration attacks in the blink of an eye
  - This could be malicious or accidental!

# Disruption

- Why are these attacks important to you?
  - They keep you from offering services to your customers
  - Potentially tarnish your reputation as a service provider
- These attacks may coincide with other attacks
  - The “loudest” attack usually receives administrator attention
  - Be sure to watch the bigger picture - this may be a smoke screen
- These attacks will definitely affect your network
  - The intent of the attack is to disrupt your operations



# Disruption

Cyber Attack  
- Router Re-Configuration -

# Disruption Cyber Attack – Router Re-Config

- Your routers perform a critical service to your operation
  - If they don't work – you can't provide service to your customers
- We will assume that you have a malicious user (an administrator) operating on the inside of your network who wants to disrupt the gateway router
  - They have the credentials to conduct this attack

# Disruption Cyber Attack – Router Re-Config

- Malicious actors might target your gateway routers:
  - Because they are central points in the network
  - Affecting one usually has broader effects
- Why?
  - The obvious one: deny service
  - Political statements
  - Demonstrations of “power”
  - Cyber “Riot”

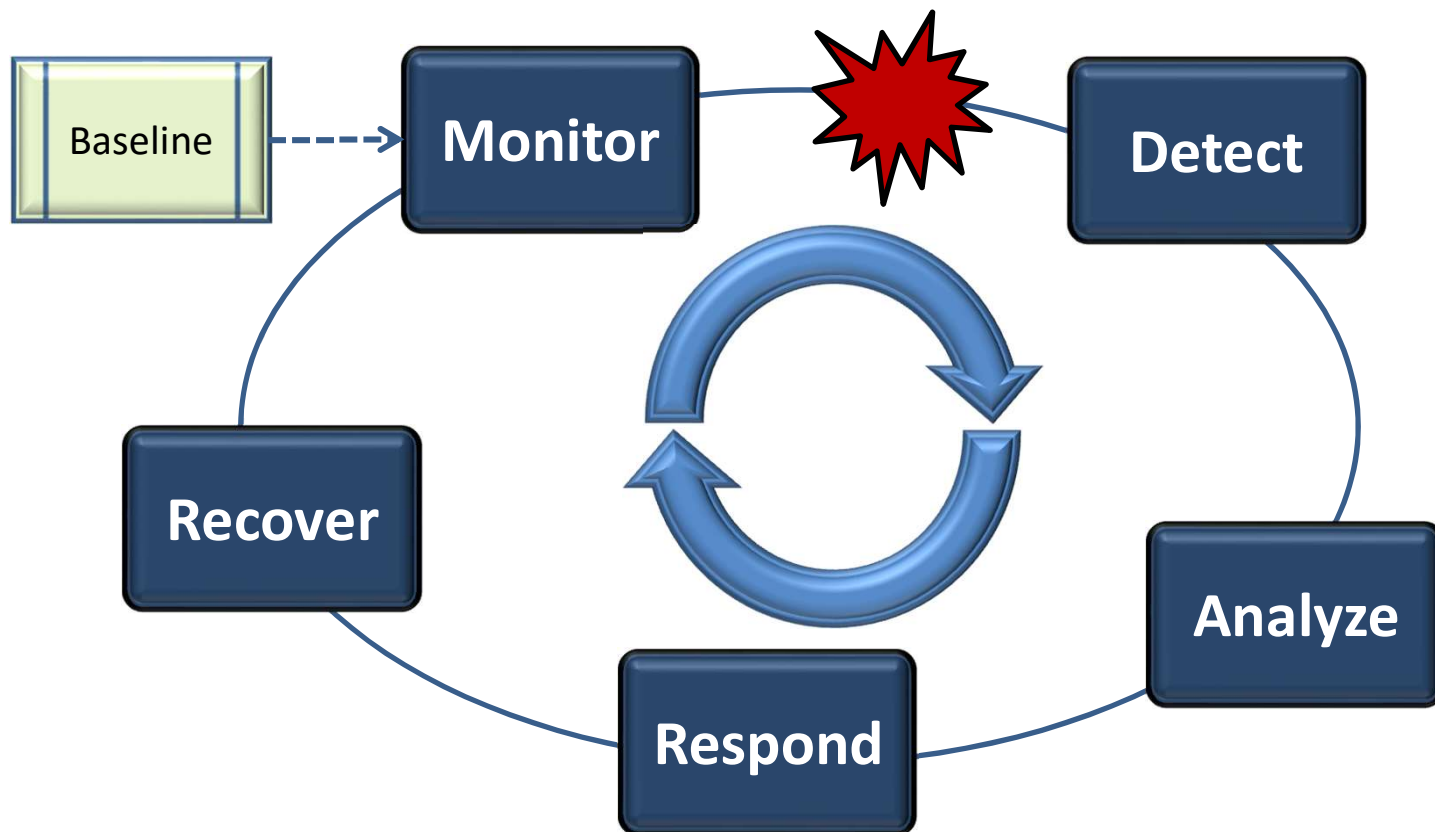


## Disruption Cyber Attack – Router Re-Config

- The components needed for this attack
  - Target IP address, credentials

# Disruption Cyber Attack – Router Re-Config

- Recall Our Secure Operations Framework

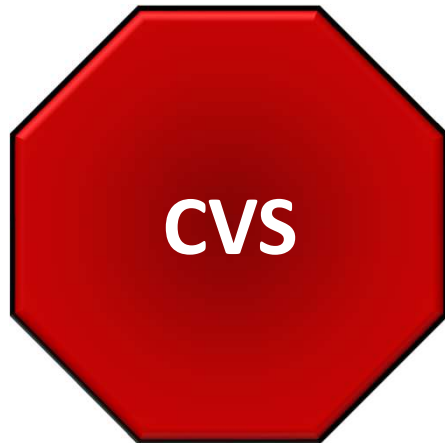


# Disruption Cyber Attack – Router Re-Config

- Establish a Baseline for What's Normal for Your Network:
  - What are your current router configurations?
  - Are your external links up? (silly question – but you may have authorized outages from your provider)
  - Do you see fluctuations in your links over time? (e.g. poor service quality, satellite link outages, rainstorms, etc)
- Use this baseline to compare what you currently see to what you expect
  - The key is expectation, if you aren't expecting it, analyze it!

# Disruption Cyber Attack – Router Re-Config

- Monitoring & Detection
  - External Service Availability
  - Router Configuration Monitoring



# Disruption Cyber Attack – Router Re-Config

- Monitoring & Detection
  - Configure your network to monitor service availability and router configuration changes
  - Monitor your detection tool(s)
  - Establish a Baseline

EX:  
Detecting  
Changes with  
SWATCH

EX:  
Configuring  
RANCID



# Disruption Cyber Attack – Router Re-Config

- Response Actions
  - aka “I’m Under Attack – What Do I Do Now?!”
  - 1) Prioritize – is anything else happening?
  - 2) Reload configuration from known good copy
- The actions you take:
  - Should focus on restoring service – punish the guilty afterwards!



# Disruption Cyber Attack – Router Re-Config

- Response Actions
  - aka “I’m Under Attack – What Do I Do Now?!”
  - 1) Prioritize – is anything else happening?
  - 2) Reload configuration from known good copy
  - 3) Make changes by hand?!

# Disruption Cyber Attack – Router Re-Config

- Recovery Actions
  - The attack is over – how do I prevent this again?
  - 1) Ask yourself “What *could* have happened here?”
  - 2) Use your analysis tools to determine where attack originated from and who may have done it
  - 3) Consider use of a management VLAN or otherwise restrict infrastructure administration to certain IPs
  - 4) Setup automatic alerts for service availability and configuration changes

# Disruption Cyber Attack – Router Re-Config

- What Other Mitigation Steps Would You Take?
  - What is appropriate for your network & resources?



## DISCUSSIONS

# Disruption Cyber Attack – Router Re-Config

- Attack Discussion
  - Everyone hopes their employees are trustworthy
  - but history tells us otherwise

**Trust But Verify**

- Other Thoughts Before We Move On?

# Disruption Cyber Attack – DoS via DNS

- Your authoritative DNS servers are open to the world and remotely accessible
  - They ***have*** to be, otherwise, what's the point?
- We will generate large numbers of DNS queries to saturate your upstream link
  - Note that we are NOT targeting your DNS server!
- The effect is that external users will not be able to resolve DNS queries to your domain

# Disruption Cyber Attack – DoS via DNS

- Malicious actors might target your DNS servers:
  - Because they are remotely accessible
  - You are guaranteed to have them
  - DNS queries are easy to generate
- Why?
  - The obvious one: deny service
  - Political statements
  - Demonstrations of “power”
  - Cyber “Riot”



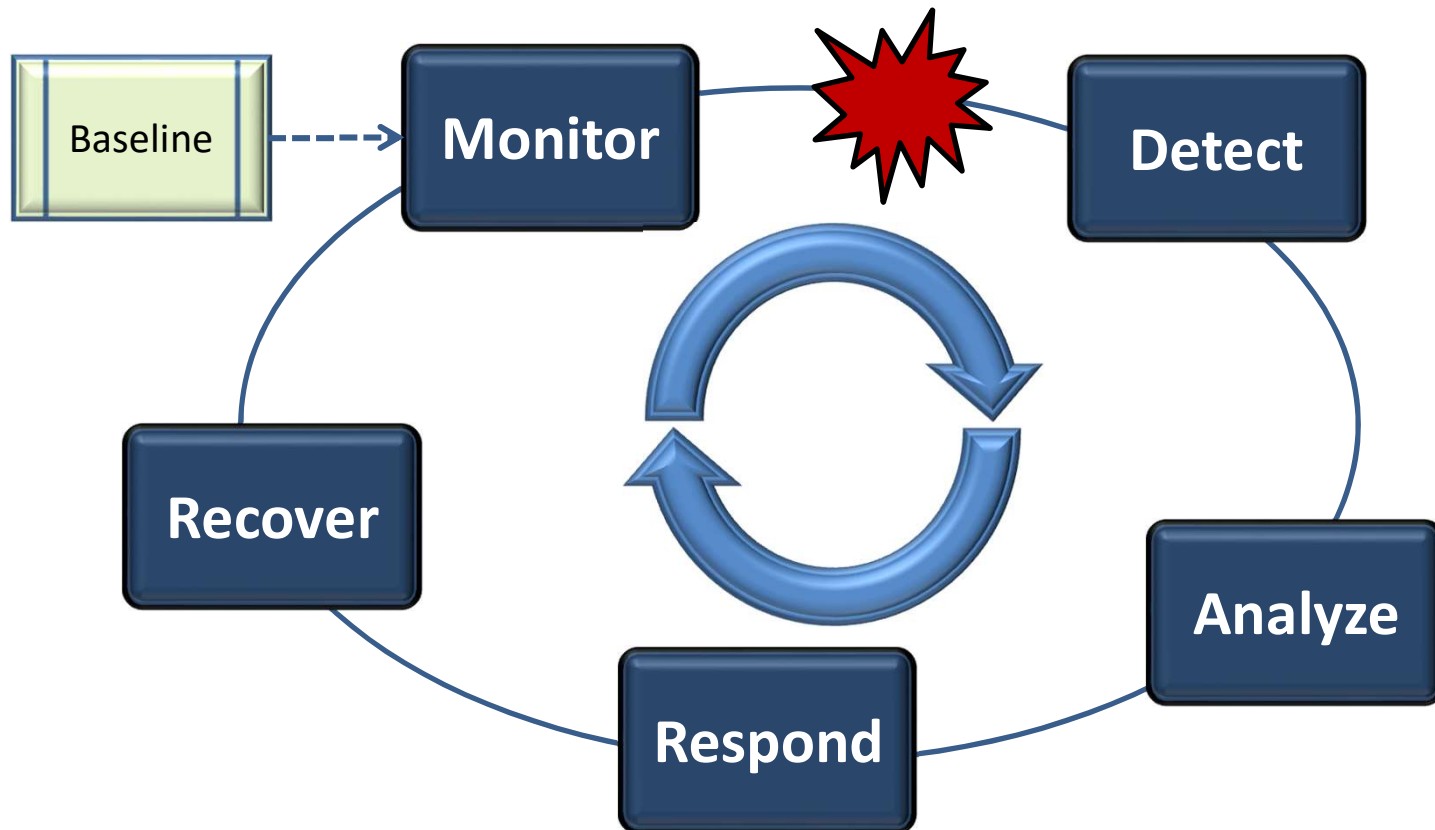
# Disruption Cyber Attack – DoS via DNS

- The components needed for this attack
  - Target IP address, DNS query generation



# Disruption Cyber Attack – DoS via DNS

- Recall Our Secure Operations Framework

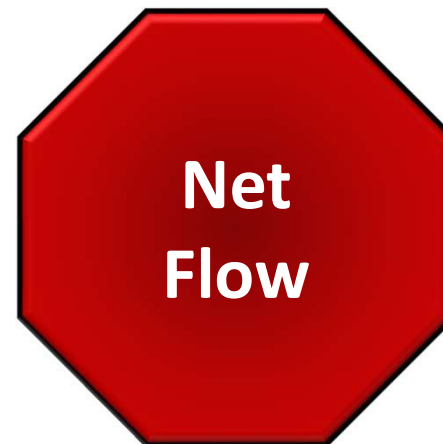


# Disruption Cyber Attack – DoS via DNS

- Establish a Baseline for What's Normal for Your Network:
  - What is your current bandwidth?
  - How much of your bandwidth is normally in use?
  - How many queries do you normally see?
  - Do you see fluctuations over time? (e.g. more queries in the morning than in the evening)
- Use this baseline to compare what you currently see to what you expect
  - A spike in queries might indicate undue “interest” in you!
  - You don't want your first indication of an attack to be a customer calling you!


# Disruption Cyber Attack – DoS via DNS

- Monitoring & Detection
  - Bandwidth Monitoring Tools
  - External Service Availability



# Disruption Cyber Attack – DoS via DNS

- Monitoring & Detection
  - Configure your network to monitor bandwidth and DNS queries
  - Monitor your detection tool(s)
  - Establish a Baseline



EX:  
Configuring  
NfSen



# Disruption Cyber Attack – DoS via DNS

- Analysis - what did your detection tools report? Is this really an attack?
  - Bandwidth Usage
  - Queries per second
- Where is the attack coming from?
- Was your external service availability affected?

# Disruption Cyber Attack – DoS via DNS

- Response Actions
  - aka “I’m Under Attack – What Do I Do Now?!”
  - 1) Prioritize – is anything else happening?
  - 2) Filter at your gateways based on the attack traffic
  - 3) Contact your upstream providers to filter
  - 4) Provision more services (bandwidth, secondaries, etc)
- The actions you take:
  - Should focus on restoring service to your customers
  - Depend on the extent of attack and where its originating from
  - Depend on your connectivity and where your customers are located
    - Recall establishing an architecture baseline – you don’t want to figure out where your links are while you are being attacked
    - You may determine that you can mitigate the attack by closing your servers to queries from outside your country – your in-country customers are OK

# Disruption Cyber Attack – DoS via DNS

- Recovery Actions
  - The attack is over – how do I prevent this again?
  - 1) Ask yourself “What *\_could\_* have happened here?”
  - 2) Provision additional bandwidth over separate links
  - 3) Provision geographically separated secondaries
  - 4) Anycasting
  - 5) Mutual Aid Agreements with other ccTLDs
  - 6) Response procedures for contacting upstream providers
  - 7) Procedures for determining customer priority

# Disruption Cyber Attack – DoS via DNS

- What Other Mitigation Steps Would You Take?
  - What is appropriate for your network & resources?



## DISCUSSIONS



# Disruption Cyber Attack – DoS via DNS

- Attack Discussion
  - DoS attacks can take many forms; effective monitoring is the only way to detect them
  - External service monitoring (e.g. what does your network look like from the outside) can help too!
- Other Thoughts Before We Move On?

# QUESTIONS?

- Do you have any questions about ...
  - Disruption Attacks
  - Detecting This Type of Attack
  - Responding & Recovering From This Type of Attack

