SPOOKY SECURITY EXERCISES

PREPARING FOR THE MONSTER MASH

Amanda Berlin & Jeremy Mio

ROADMAP THROUGH THE HAUNTED HACKINGCAST

- Tabletop Terror Exercises (TTXs)
- Macabre Playbooks
- Haunted Gamification
- Game Bot Overview & Mini Haunting
- Q&A

QUICK OVERVIEW OF INCIDENT RESPONSE

INCIDENT RESPONSE FRAMEWORK

"If you're ready for a zombie apocalypse, then you're ready for any emergency."
- Center for Disease Control

Learn to build a survival kit and make a plan

Meet fire and police staff and tour their vehicles

Form a Shoreline Watch group with your neighbors

Learn basic first aid and CPR techniques

ZOMBIE PREPAREDNESS
& Family Safety Fair

Tabletop Terror Exercises (TTX)

are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation….in this case….zombies, werewolves, vampires, and teenagers

TTX GOALS & OBJECTIVES

- ❖ Break the scenario into meaningful learning points
- ❖ Screech it loud and clear for all to hear!
- ❖ Have a discussion page to facilitate a conversation on main IR talking points:
  - ➢ Identification and Detection
  - ➢ Containment and mitigation
  - ➢ Preventative and Communication

Objective is to have a productive and engaging discussion and identify gaps to prioritize Organizational resources/tasks.

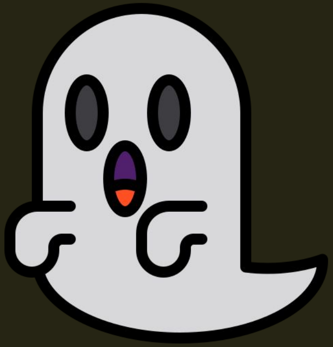
DO:

- ★ Designate a single individual to facilitate
- ★ Be sure to include applicable members of other business units
- ★ Keep track via discussion guide
- ★ Wear garlic necklaces and carry holy water

DON’T:

- ★ Stray from scope of the exercise aka scope creep
- ★ Forget to complete AAR and follow up
- ★ Be THAT Person
- ★ Invite vampires inside

PLAYBOOK OVERVIEW AND EXAMPLES

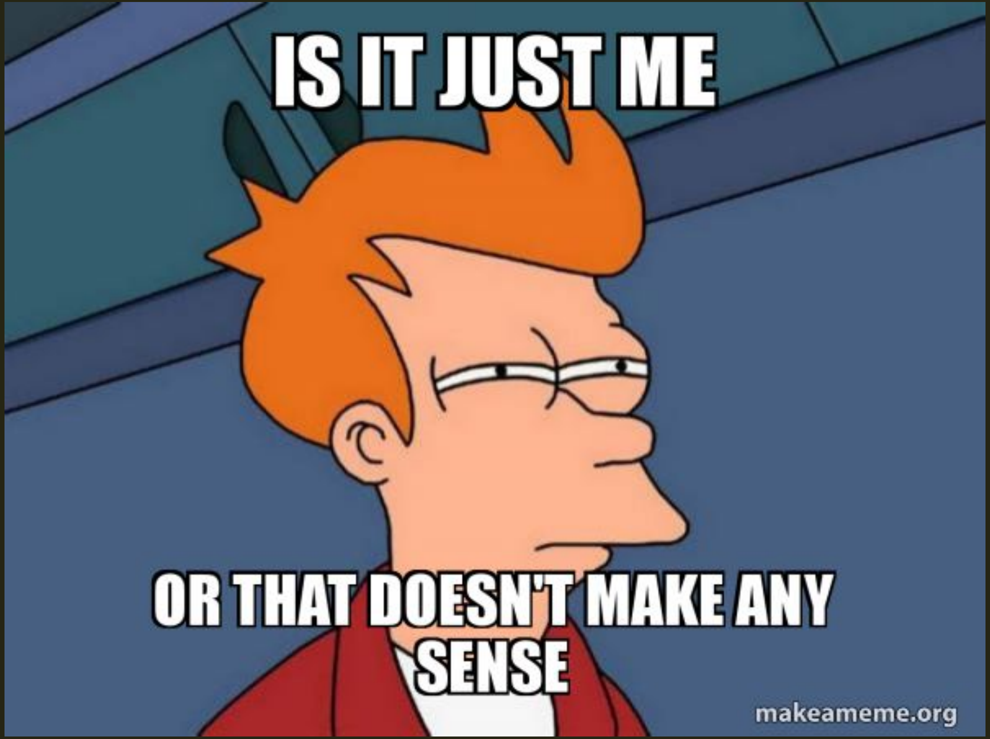


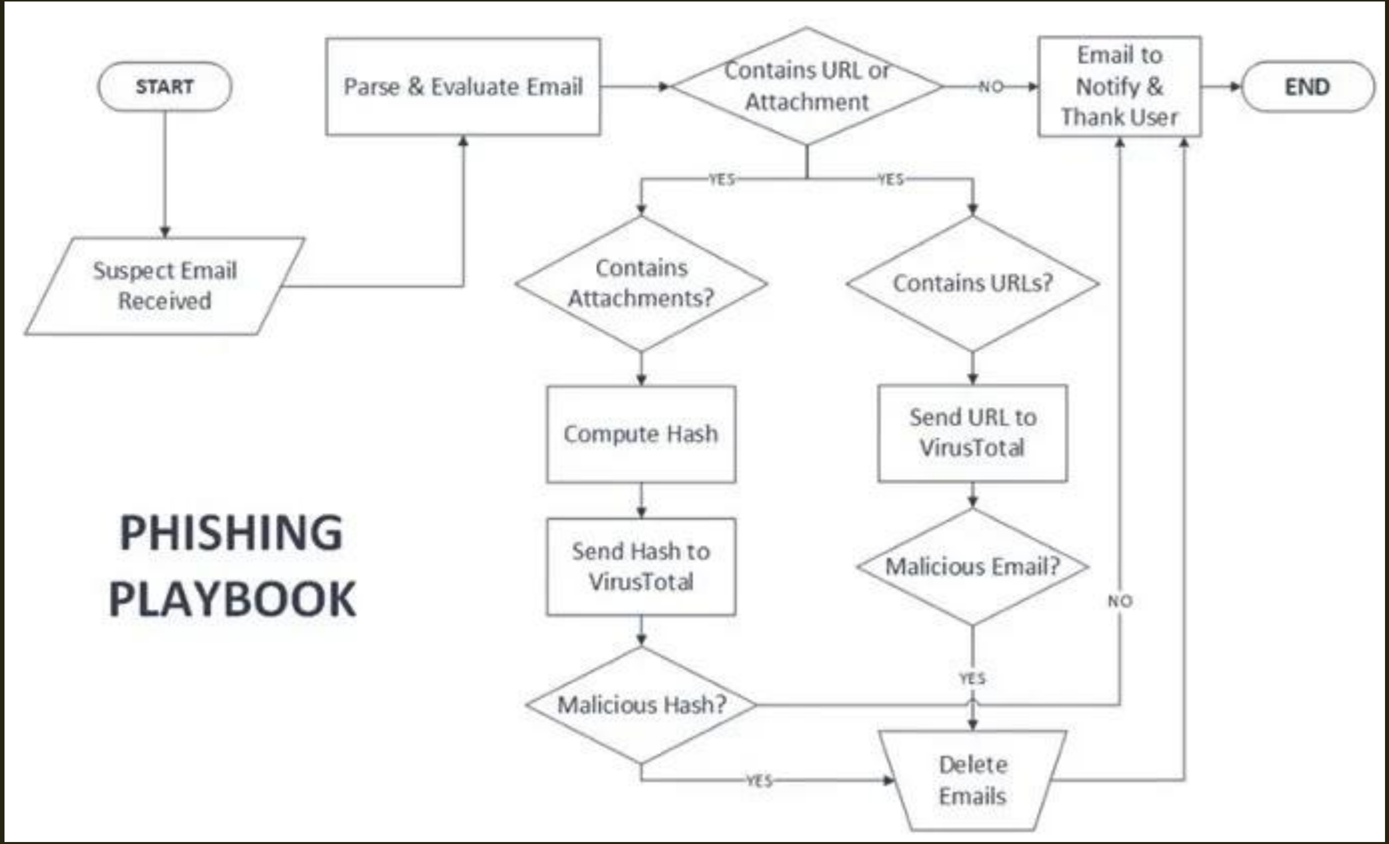
```
index=main AND (event_simpleName=ProcessRollup2 OR
event_simpleName=SyntheticProcessRollup2 OR event_simpleName=DnsRequest OR
event_simpleName=NetworkConnectIP4) | eval falconPID=coalesce(TargetProcessId_decimal,
ContextProcessId_decimal) | fields aid, event_simpleName, falconPID, FileName,
CommandLine, DomainName, RemoteAddressIP4, ContextTimeStamp_decimal,
ProcessStartTime_decimal | eval CommandLine=substr(CommandLine,1,100) | stats
dc(event_simpleName) AS events, values(ProcessStartTime_decimal) as fileExecutionTime,
earliest(ContextTimeStamp_decimal) as firstConnection, latest(ContextTimeStamp_decimal) as
lastConnection, values(FileName) as executingFile, values(CommandLine) as cmdLine,
values(DomainName) as domainNames, values(RemoteAddressIP4) as remoteIPs by aid,
falconPID | search events>1 | where isnotnull(executingFile) | convert ctime(fileExecutionTime)
ctime(firstConnection) ctime(lastConnection)
```

Splunk Query Example

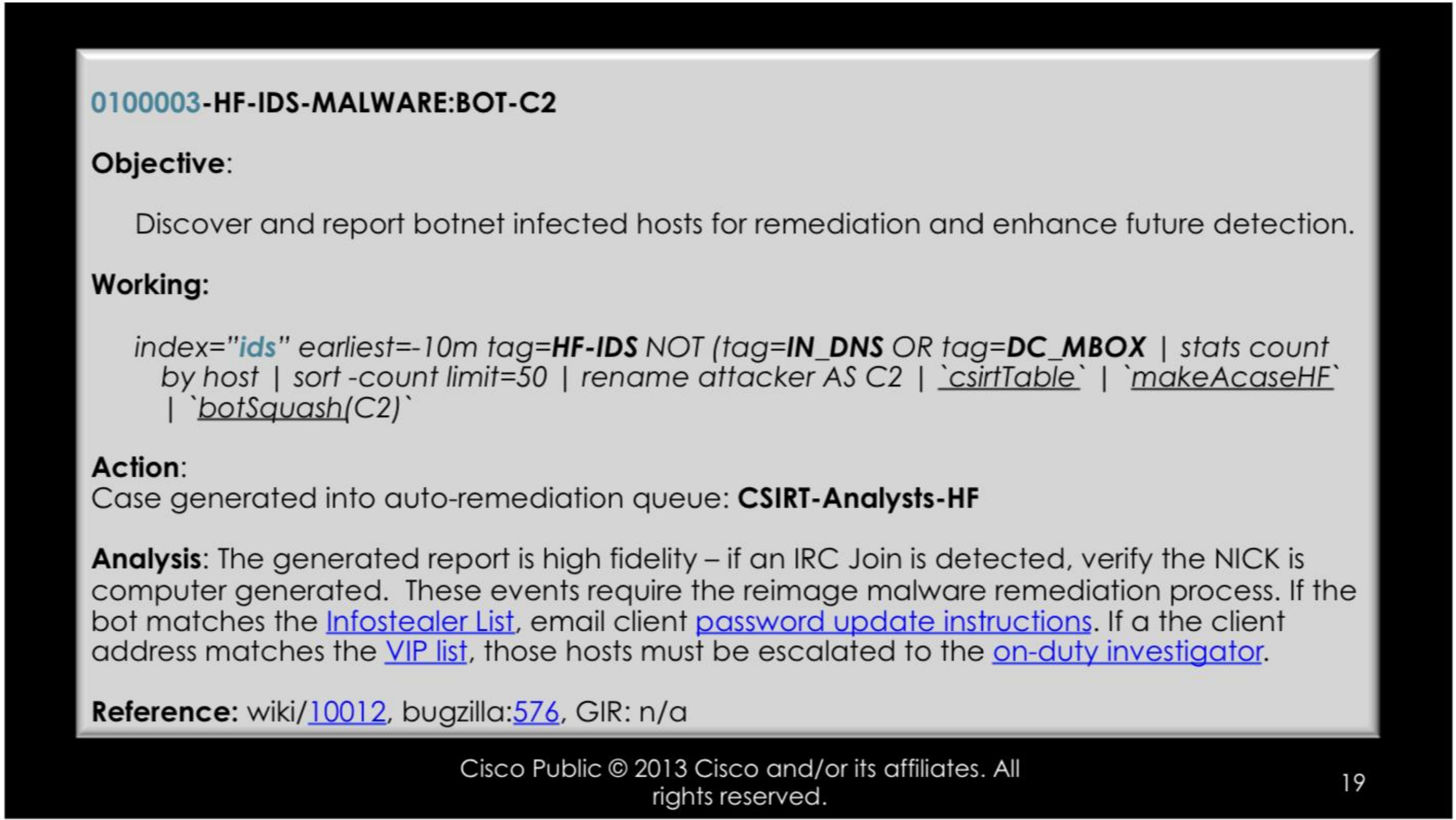
```
let workspaceid="your Sentinel workspace id";
let timeframe=1d;
let AZRoles = externaldata(Name: string, Id: string) [@"https://gist.githubusercontent.com/reprise99/363eee70938c9a3d662e3f6da4610fe4/raw/b25b2d7a626396684ab578363888a0e360e7b287/.csv"]
with(ignoreFirstRecord=true, format="csv");
let accesschange =AzureActivity
    | where TimeGenerated > ago(timeframe)
    | where OperationName == "Create role assignment"
    | where TenantId == workspaceid
    | extend TargetAADUserId = tostring(parse_json(tostring(parse_json(tostring(parse_json(Properties).requestbody)).Properties)).PrincipalId)
    | extend RoleDefinitionId = tostring(parse_json(tostring(parse_json(tostring(parse_json(Properties).requestbody)).Properties)).RoleDefinitionId)
    | parse RoleDefinitionId with * '/roleDefinitions/' AzureRoleId
    | where ActivityStatus == "Started"
    | project
        AccessChangeTime=TimeGenerated,
        Actor=Caller,
        ActorIPAddress=CallerIpAddress,
        ResourceGroup,
        WorkspaceId=TenantId,
        AzureRoleId,
        TargetAADUserId
    | join kind=inner (AZRoles
        )
        on $left.AzureRoleId == $right.Id
    | project-away Id;
IdentityInfo
| where TimeGenerated > ago(21d)
| summarize arg_max(TimeGenerated, *) by AccountUPN
| join kind=inner accesschange on $left.AccountObjectId == $right.TargetAADUserId
| project
    AccessChangeTime=TimeGenerated,
    Actor,
    ActorIPAddress,
    ResourceGroup,
    WorkspaceId=TenantId,
    AzureRoleId,
    AzureRoleName=Name,
    TargetAADUserId,
    AccountUPN
```

Microsoft KQL Example - Azure Sentinel


IS IT JUST ME
OR THAT DOESN'T MAKE ANY SENSE
makeameme.org



PHISHING PLAYBOOK



0100003-HF-IDS-MALWARE:BOT-C2

Objective:

Discover and report botnet infected hosts for remediation and enhance future detection.

Working:

```
index="ids" earliest=-10m tag=HF-IDS NOT (tag=IN_DNS OR tag=DC_MBOX | stats count
   by host | sort -count limit=50 | rename attacker AS C2 | `csirtTable` | `makeAcaseHF`
   | `botSquash(C2)`
```

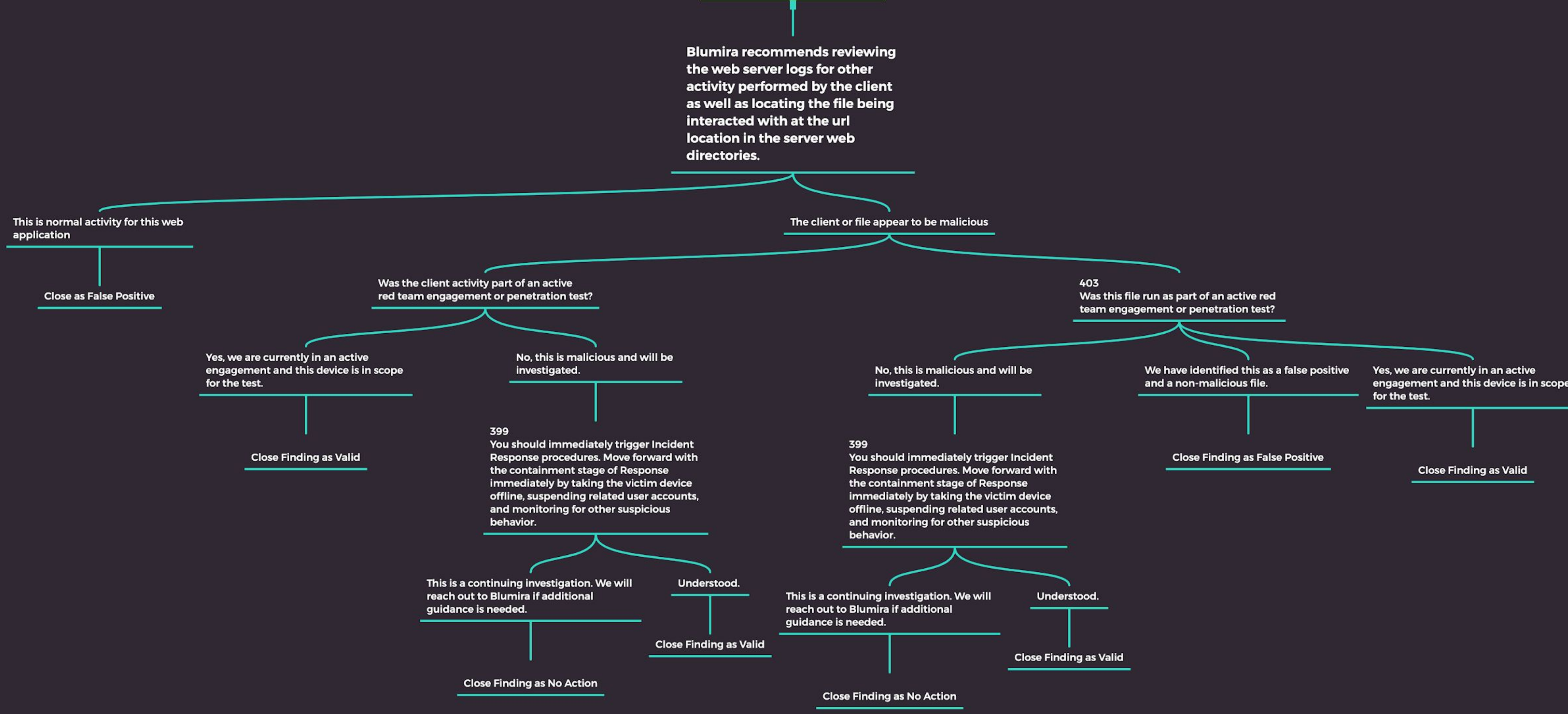
Action:
Case generated into auto-remediation queue: **CSIRT-Analysts-HF**

Analysis: The generated report is high fidelity – if an IRC Join is detected, verify the NICK is computer generated. These events require the reimage malware remediation process. If the bot matches the Infostealer List, email client password update instructions. If a the client address matches the VIP list, those hosts must be escalated to the on-duty investigator.

Reference: wiki/10012, bugzilla:576, GIR: n/a

https://www.first.org/resources/papers/amsterdam2013/bollinger-jeff-slides.pdf

T1505.003 Webshells via Access Logs



Blumira recommends reviewing the web server logs for other activity performed by the client as well as locating the file being interacted with at the url location in the server web directories.

This is normal activity for this web application

Close as False Positive

The client or file appear to be malicious

Was the client activity part of an active red team engagement or penetration test?

Yes, we are currently in an active engagement and this device is in scope for the test.

Close Finding as Valid

No, this is malicious and will be investigated.

399
You should immediately trigger Incident Response procedures. Move forward with the containment stage of Response immediately by taking the victim device offline, suspending related user accounts, and monitoring for other suspicious behavior.

This is a continuing investigation. We will reach out to Blumira if additional guidance is needed.

Close Finding as No Action

Understood.

Close Finding as Valid

403
Was this file run as part of an active red team engagement or penetration test?

No, this is malicious and will be investigated.

399
You should immediately trigger Incident Response procedures. Move forward with the containment stage of Response immediately by taking the victim device offline, suspending related user accounts, and monitoring for other suspicious behavior.

This is a continuing investigation. We will reach out to Blumira if additional guidance is needed.

Close Finding as No Action

Understood.

Close Finding as Valid

We have identified this as a false positive and a non-malicious file.

Close Finding as False Positive

Yes, we are currently in an active engagement and this device is in scope for the test.

Close Finding as Valid

TABLE TOP AND PLAYBOOK USE CASE EXAMPLE

BEC – TABLE TOP

Igor received a call from the Monster Mash sister company, Monsters Inc. Shelley asked if he had sent over the wire payment yet for all of the spare parts they've been supplying.

After asking his assistant he assures her that everything has been paid to the new account number she provided but Mary hasn't been receiving payment OR any of his emails.

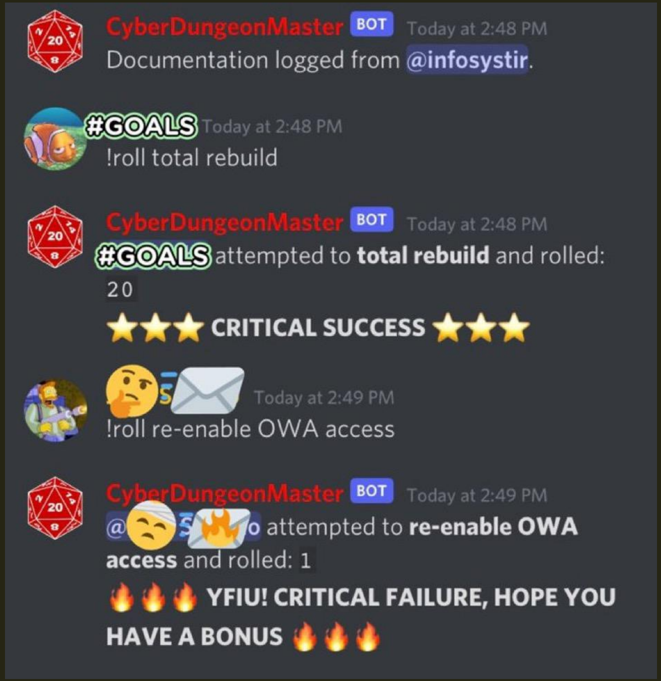
BEC – PLAYBOOK CREATION

- Prepare
  - Does Igor know that he should contact someone in security?
  - If you haven't already done so, is your organization considering implementing multi factor authentication?
  - What communication protocol do you have in place for notifying users of particular phishing attempts to be aware of?
  - Does your staff feel comfortable confirming with the "sender" that this type of request is genuine?
- Identify
  - Where did the emails go?
  - Where do you look?
  - Can your provider or vendor offer additional support in blocking phishing attempts from reaching end users' inboxes?
- Contain/Eradicate
  - Did the attack go any further than BEC?
  - What tools can you leverage to decrease the effects of these attacks?
- Recover
  - Who outside of your organization should be notified of this type of incident?

(TABLE TOPS + IR FRAMEWORK + PLAYBOOKS) * GAMIFICATION

=

CYBER GAME MASTER BOT OVERVIEW



CyberDungeonMaster BOT Today at 2:48 PM
Documentation logged from @infosystir.

#GOALS Today at 2:48 PM
!roll total rebuild

CyberDungeonMaster BOT Today at 2:48 PM
#GOALS attempted to **total rebuild** and rolled: 20
⭐⭐⭐ **CRITICAL SUCCESS** ⭐⭐⭐

🤔S✉️ Today at 2:49 PM
!roll re-enable OWA access

CyberDungeonMaster BOT Today at 2:49 PM
@😒S🔥o attempted to **re-enable OWA access** and rolled: 1
🔥🔥🔥 **YFIU! CRITICAL FAILURE, HOPE YOU HAVE A BONUS** 🔥🔥🔥

ROLL ACTIONS

- <10 - action fails 😈😈😈 + Roll for DAMAGE
- 11-20 - action is successful 🐱🐉🐱🐉🐱🐉
- 1 - critical failure, bad things happen… 🔥🔥🔥 + extra DAMAGE
- 20 - critical hit, good things happen… 😎😎😎
  - *re-roll for chance for 19-20 for killing blow, unicorns happ*
- ***Modifiers*** 🐱💻🐱💻🐱💻
  - +2 if you have the response or procedure documented i
  - +1 if you have skilled staff trained based on organization

EXAMPLE ACTIONS

- Identify additional information
- Detection of activity or threat using: Manual Analysis, System/Toolkit, etc.
- Response or Containment e.g. reset all password, block at firewall, etc.
- Recovery action: restore backups, failover to redundant system, reboot systems, etc.
- Request internal assistance - Legal, Management, etc.
- Request external assistance - vendor/consultant
- Issue statement to PR/Media

EXAMPLE GAME PLAY TIPS

- Always have a set of actions ready or back up actions!
- Roll for additional information to decide on an action or set of actions. If you request additional clarification, be ready to roll for it.
- GM have final say!
- Do not forgot to use your special skills!
- Make sure to use your titles properly
- Try and follow an incident response framework
- Use your Playbooks!!!
- Take notes!! Keep track of your actions and outcomes!

Ransomware – Table Top

Your software app is about to be released. PoltergeistBNB, “Vacation home rentals for ghosts”, has the ghostly community ready to scream.

Frank in AppDev calls to explain the computer that they’re using for development testing now has a splash screen with a countdown timer after updating some packages.

Ada attempted to reboot, but the screen doesn’t go away.

This computer is not an asset on file, but it is directly connected to the endpoint vlan and not connected to any version control… 6 months of coding lost and the final sprint is next week.

CHOOSE YOUR DESTINY… PART 1 OF 3

1 - Investigate internally… more?

2 - Reach out to Third Party or LEO?

3 - Recode…. EVERYTHING and ask for extension?

4 - Other?

⭐⭐⭐ CRITICAL SUCCESS ⭐⭐⭐

OR

🔥🔥🔥 YFIU! CRITICAL FAILURE, HOPE YOU HAVE A BONUS 🔥🔥🔥

CHOOSE YOUR DESTINY... PART 2 OF 3.

1 - Investigate internally... more? >> You find nothing... no matter what 😭

2 - Reach out to Third Party or LEO? >> If success, they will review, roll again!

3 - Recode.... EVERYTHING and ask for extension? Roll an additional workplace initiative...😬

4 - Other? Entertain me... we will roll a see what happens 🎰

⭐⭐⭐ CRITICAL SUCCESS ⭐⭐⭐

OR

🔥🔥🔥 YFIU! CRITICAL FAILURE, HOPE YOU HAVE A BONUS 🔥🔥🔥

CHOOSE YOUR DESTINY... PART 2 OF 3.

1 - Investigate internally... more? >> You find nothing... no matter what 😭

2 - Reach out to Third Party or LEO? >> They find a decryptor and all is well!

3 - Recode.... EVERYTHING and ask for extension? If success you are transition to a new cybersecurity initiative with budget... If fail the company goes under due to bad leadership and over committing to clients, but you find a happy company 🤓

4 - Other? Entertain me... we will roll a see what happens 🎰

RANSOMWARE - PLAYBOOK CREATION

- Prepare
  - How do you secure test dev machines?
  - What steps would you take to prevent this from happening again?
- Identify
  - How do you validate the package?
  - How would you find out the capabilities of the malware (if any)?
  - How could you identify all potentially compromised devices?
- Contain/Eradicate
  - What actions will you take during the event?
  - How would you find and fix the vulnerabilities exploited?
- Recovery
  - How would you disclose this incident to the impacted parties? What if the package was valid...
  - Will you pay the ransom? 6 months of code was lost.

WRAP UP…

- Table Top and Incident Response Overview
- Playbook Concepts
- Gamification
- Game Bot Overview and Mini-Demo

Q&A

FOR ADDITIONAL WISDOM OR OFFERS OF GOLD

@infosystir

@blumirasec

Blumira

@hackershealth

MENTAL HEALTH HACKERS

@brakesec

BRAKEING DOWN SECURITY

@cyborg00101

SECURITY DDTTX