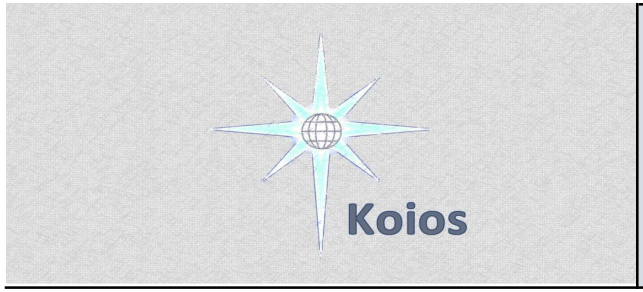

Game master Scenario sheet

Scenario number: 1

Scenario Name: Phishing Gone Ransom, - Information Theft

NOTES:

This scenario needs to be adapted to the company before starting to make it more immersive! Note: Incase of multifactor authentication. Add a scene with a vishing call where someone has gotten hold of the MFA and change the login attempts to just one per person.

Information to read before starting:

Succsessful login attempts has been done towards a system (insert system with sensitive data for the company) from a specific user acount (needs to have access to the system) and data has been exfiltrated. The data is sensitive (insert sensitive data related to the company, preferably customer data).
Later at the day of discovery, the director will recieve an email with a bitcoin ransom for the hacker not disclosing the data (- TIP! make a ransom email to present for immersiveness). The hackers belong to a hacker group and are known for this type of activity. They have a history of disclosing their bounty no matter if a company pays the ransom or not.

The data will show up being posted online no matter what the company decides to do. The company has to deal with the aftermath of this.

Further investigation into the specific user account being abused shows that the user recieved an email last week. The email was a phish disguised as IT, prompting the user to log into a system (using the same credentials as the one being breached). (- TIP: Make a fake email to make this more immersive, and go through the tells on why this was fake.)

Inject number	Inject details	Background Info	Needs to be examined before	Relevant Questions
1	[PLAYER] gets a phone call from [SOC OR OTHER RELEVANT LOG PERSONNEL]. There has been an increase in log activity. Several successful login attempts towards the [INSERT SYSTEM] has been done at odd times for the last two nights.	The log activitiy is successful logins to a system. Data is gone (decide what data this will be prior to the game)		Has any data been exfiltrated. What has been taken? How long did the logins last?
2	[DIRECTOR NAME] gets an email. It is a mail from a hacker group stating they have your data. - The mail reads: "Pay up 3 million USD to this bitcoin wallet or have the data publicised for everyone to see"	Create an email for imersiveness. You can use local currency, language and APT group name as you wish.	4	Is there anyone else being attacked by this group? Background check? Will the data still be disclosed even if we pay up. If the lack of data has not been discovered yet, what is gone?
3	[DIRECTOR NAME] calls [PLAYER] to get information. There is a lot of questions. Roll (without modifiers) to see if you will be able to end the call quickly or if you are out of commission to help the team for some time.	The roll is to take a player out of commision to see how the others fill in he gap. Take out an important player or someone playing a ke role in incident handling to see what happens.		What will you do without this player? How to proceed when someone with a key role is gone?
4	[PLAYER] gets a call from [DIRECTOR]. Media has alerted them of a tip they have gotten about some data that stems from your company. Regardless of your actions, the hacker group has publicised your data on Pastebin.	The data is out		How to handle this initial phase? Is someone handling the media? What is planned to disclose, and how? Will they ask for what the media know? How to remediate the leak?
5	Several media companies has called and wants a statement about the information leak	A statment is needed to the media.		Has eveyone been alereted. Customers, partners etc? Maybe they don't want to find this out by media, but from you first?
6	[SUPPORT/RECEPTION-CONTACT POINT] are being flooded with stressed out [CUSTOMERS/USERS]. Each demanding answers on what has been lost of information relevant to them.	A little distraction into the incident handling		How to lower the pressure for information? What can be disclosed? Is it important to answer every call? (Probably) How to keep the information flow between 1st line and operational support/incident handlers?

Main Focus for the Scenario:

Investigative techniques
- How quickly did they investigate the background for the breached user?
-Was the investigation done methodologically?

Media and customer handling
- Is anything done prior to the disclosure?
-How is media handled after the disclosure?
-What information will go out to the customers?

Remediation after breach
- User management of the breached user
-Check for more possible breaches in the same manner, there is probably more than one getting that email
-Is all data that has been lost accounted for, do they have an overview and can give information to the correct people?

How to avoid this from happening again
- Awareness training plan?
-Block logins at certain times during the day and from different regions? (if this is already blocked, what else could have been done?)

7	[PLAYER] Gets a phone call from [DAYCARE/SCHOOL, find someone with a kid]. Their child has a fever and you need to pick up the kid. Roll without modifiers. 1-10 = you are stuck at home with a sick kid until tomorrow. 11-20 = You only have to make a few phone calls to arrange pick up. Take a small timeout until the game master says you are back from making calls.	Sometimes life happens. Even during crisis	How to deal with the things you cannot control? Not everyone can be available. What do you do? How do you aquire the skilleset if a person is not available? Consultants? When to call those in?	
8	Logs shows another user account has been trying to log on [UNUSUAL SYSTEM ACTIVITY TOWARDS ANOTHER SYSTEM].	So there is more stuff going on…	Could this have been discovered sooner? How to respond to it when it is not a one-time incident?	
9	A talk with the owners of the user accounts shows that they both got an e-mail last week requesting them to log in.	Phishing emails are not always fun. Create the email to show for imersiveness. It is a nice way to idoctrine some awarness raining regarding phishing	How to remediate this? How many has gotten an email? Password changes? For just these two, or the whole company just in case? How to avoid this from happening again? - awareness training? Password policy?	