**Cubicles & Compromises Incident Response Tabletop Game Scenario 1**

1. **Spear phishing - Your manager of HR was sent the following spear phishing email at 3:45 PM on Friday:**

"From: Actual VP of Business Office"

To: "HR Manager"

Subject: Major problem please read immediately

Joe,

We have a major problem, we missed the deadline from the state to send our California tax holdings report. We will be fined $5,000 for each day that this report isn't submitted. I just went on vacation so the timing isn’t ideal for me. The good news is I have talked with Bill in HR and he had Jim whip up a report generator. It is attached and requires the Macro to pull the needed data in from ERP. Once it opens it will request your ERP username and password, this is needed to make the connection. Once it has you can export the report as a comma separated value file and email it to my assistant Beth, so she can send it to the state as soon as possible.

Thanks,

Tots legit CBO Tim

The email addresses where all correct and not forged, the CBO really was on vacation. The HR manager called this in to the help desk once she spoke to Beth the CBO’s assistant on Monday and she didn’t know what he was talking about. You job is to assume the role of the individual you are playing in this scenario, and walk through the incident response steps.

**Characters: Incident Master, CTO, Help Desk, Systems admin, PR, CBO, Security Analysis, CBO’s assistant, HR manager, CISO**

If you hold one of these positions you may play this character, otherwise everyone rolls the dice, highest number chooses first, then in descending order.

**For “Incident Masters:** Your team doesn’t need to follow the below steps, they are for leading the discussion forward, you can suggest some of these steps to keep going forward.

**Rules**: For each action the IR team takes, roll the dice. An 11-20 is successful, 10 or less, it fails.

You get +5 if your organization has a documented procedure for the action. +2 if your organization has someone trained to do the action. For example you role a 5, but you have a documented procedure and a person trained for the procedure, then you now have a 12 and the action is successful.

**Initial Investigation**

1. Do you have AV scanning for email attachments? Roll to see if it was detected
2. Did the manager open the attachment? On multiple computers?
3. Did it prompt him to enable macros? Did he?
4. Did he put in his username and password?
5. Did the email come from the CBO’s email account or were the headers forged?
6. Did the CBO’s email get accessed from any out of the ordinary IP Addresses?
7. Does he have local administrative access to his system?
8. Does the college use the same local administrative system for each computer?
9. Has any domain admin accessed the computer since it was last rebooted?
10. Do you have Windows 8 or above and have you set the registry key to isolate the LSASS program, that would prevent an admin from accessing cached plain text credentials?
11. Do you have windows 10 and have enabled the registry entry that protects admin users from accessing hashed passwords in LSASS?
12. Are you still using SMBv1, is SMB signing enabled?
13. Did anything get transmitted outside of the network? How do you know
14. Did the macro actually work and create a file from the banner system?
15. Did the manager email it to the CBO’s Assistant?
16. Do you have anything that prevents PII from being emailed?
17. Did anyone access the CBO’s assistants email account and download the attachment?

**Initial Communication**

1. If any of the above steps turn out to be the case then start working the incident
2. Who do you call first?
3. Do you have a contact list for incidents?
   1. Do you have any third party forensic firms on retainer, or at least have a reference for one? Should you be working this incident? For this game we will say yes, in reality probably not
4. Should you get the authorities involved and when?

**Forensic Investigation**

1. Analyze the excel macro, is it obfuscated?
2. What is the macro executing, reverse shell?
3. Is the reverse shell still active?
4. Is the malware persistent, or is it fileless?
5. What addresses is the computer communicating with
6. Is the network segmented, and firewalled, or can it access the whole internal college network?
7. Did the attacker pivot to other computers on the network? How can you tell? Which ones?
8. Could the attacker have gained access to the College VPN system? Why or why not?
9. Do you have a separate logging server, like splunk? Is the password the same as any of your other AD accounts.
10. Did the attacker delete any forensic data?
11. Does the manager have access to other PII (private identifiable information)? Did the attacker access it? How do you know?
12. Any other steps?

**Wrap up**

1. Supply a report to all of the management and key stakeholders, be sure to redact sensitive information if the document will ever be released publicly.
2. If any information was potentially compromised what do you legally need to do?
   1. In California a breach is defined as an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number, Driver’s license number or California identification card number, Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account, Medical information, Health insurance information.
   2. You are required to notify those affected as soon as is reasonable, this can now be electronically or written.
   3. You are also required to alert the California attorney general of the breach and provide a sample notification letter that was user to notify those affected.
   4. Note that government agencies are not required to offer credit protection for data breaches, only commercial businesses are. However, it is customary.
   5. Please consult your general counsel for legal advice in the case of a real security incident.
3. How could this incident be prevented? Would multi-factor authentication have helped?
4. What security controls could have narrowed the scope of the incident?
5. Are there any tools available freely from the Security Center that could have helped?

Injects:

1. While do forensics the hard drive of the HR Manager stops working. It is a hardware failure, what do you do.
2. The attacker sends a ransom request
3. The attacker releases sample data on pastebin