**Cubicles and Compromises Incident Response Tabletop Game Scenario 2**

1. **Your student portal stops responding:**

In the middle of registration your student portal stops responding. The systems admin for the front-end web servers looks that the systems. He finds that the CPU is pegged at 100% on all of the web servers and there are processes running called BCoinMine that is taking all of the CPUs cycles. He contacts the DBA, who finds the Database server is also CPU pegged and running BCoinMine. For this exercise assume all systems are running Linux. What should be done?

**Characters: Incident Master, CTO, Help Desk, Systems admin(s), DBA, CBO, Security Analysis, CISO, College President, College Board member, PR**

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. What is your first action? Do you reboot or isolate?
2. If you reboot the processes just start up again and you may have lost valuable forensic data
3. Do you need to take the system completely down? For how long?

**Initial Communication**

1. Who do you call first?
2. 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
3. Should you get the authorities involved and when?

**Forensic Investigation**

1. Do you have a record of all of the commands run on the system? What could provide this?
2. Find the executable BCoinMiner, analysis what it does, is it just a bitcoin miner? Does it have a spreader, command and control, or reverse shell capability?
3. Did the malware spread to other systems besides the ones already discovered?
4. How is the executable being relaunched when the system reboots?
5. What IP addresses has the server been communicating with?
6. Do you keep netflow stats for these servers?
7. How much traffic has been sent outside of the college and to who? Are there any outliers with much more traffic than any of the others?
8. Could any of the PII have been compromised? Why not?
9. How can you tell if the PII was transferred off of the system?
10. Do you have logs transferred to an external system such as Splunk that wasn’t compromised? Can you trust the logs on the local systems?
11. Could a rootkit have been installed?
12. Were they any known vulnerabilities present in the system, such as an old version of the web server with a known remotely exploitable vulnerability?
13. If so, why wasn’t it patched? When was the last time the systems were patched?
14. Do you have a patching schedule? Does it allow for emergency patching of recently found vulnerabilities if they are above a certain CVSS Score?
15. How did the malware migrate to the Database Server? Shared passwords? More unpatched vulnerabilities?
16. Was there any other malware besides the coin miner present on the server?
17. What are your suggestions to get the systems back up and running as quickly as possible? Are you confident this is the correct course of action?
18. Is it riskier than starting from scratch and restoring the data from backups?

**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?
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. The date stamps are not correct on the servers making analysis of logs difficult, correlating actions on different systems.
2. It starts to look like an inside job, who has access and motives to do this?
3. The lead security analyst appendix gets infected and he needs emergency surgery, he is out for the rest of the investigation
4. An unrelated DDOS attack breaks out.