Incident Handler's Journal Date: 10/21/2024, 04:34 AM

Entry: #1 (Monday) Description

A phishing email containing a malicious attachment that deployed ransomware was sent, encrypting a small U.S. health care clinic, which experienced a security incident on Tuesday at 9:00 AM. This incident severely disrupted their business operations. The hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key. Tool(s) Used

No security tools were used. The 5 W's

```
Who: An organized group of unethical hackers
What: A ransomware security incident
Where: At a health care company
When: Tuesday at 9:00 AM
Why: The incident happened because unethical hackers accessed the company's systems using a
```

Additional Notes

All of the company's files were encrypted. The group is a bunch of unethical hackers known to target organizations in healthcare and transportation industries. This means we could see the same incident happening in another company related to transportation. All of the computer systems are shut down and ready to mitigate and put a stop to the incident. Template for Future Entries Date: [Record the date of the journal entry]

Entry: #[Entry Number] Description

[Provide a brief description about the journal entry.] Tool(s) Used

[List any cybersecurity tools that were used.] The 5 W's

```
Who: [Who caused the incident?]
What: [What happened?]
When: [When did the incident occur?]
Where: [Where did the incident happen?]
Why: [Why did the incident happen?]
```

Additional Notes

[Include any additional thoughts, questions, or findings.] Need Another Journal Entry Template?

If you want to add more journal entries, please copy one of the sections above and paste it into the template to use for future entries. Reflections/Notes

[Record additional notes]