**Ransomware Outbreak**

There are almost near daily news stories of ransomware outbreaks and estimates show that from January 2019 to October 2019, 491 hospitals have been the victims of ransomware attacks. With ransomware attacks increasing in frequency and attacks like WannaCry and NotPetya showing the level of devastation they are capable of, the threat of ransomware should be taken seriously by all hospitals. This scenario is designed to get organizations to think about the prevention, mitigation, detection, and recovery aspects of a ransomware attack.

# **Start of the Scenario:**

At 1:15 on a Tuesday afternoon, a phishing email slips through the hospitals spam filter and makes its way into the mailbox of several employees. The email purports to be from the hospital’s head of HR and prompts the employees to click the link in the email to watch a mandatory training video as part of their annual education. Several employees click the link not realizing that the link points to a server that hosts malware. An employee reports problems with the link to HR, but no one reports the issue to IT. The malware does not yet have a known signature and slips past the hospital’s endpoint security system to infect a hospital PC.

## **Questions to consider:**

1. What controls could be implemented to provide better protection than just basic spam filtering (e.g. a sandbox, etc)?
2. How well are employees trained to recognize phishing within your organization?
3. What are phishing reporting procedures?
4. What controls could be implemented to reduce the likelihood of successful connection to the malicious URL (e.g. web filtering, etc)?
5. Does your organization’s Web filter block uncategorized URLs (e.g. any URL never seen by your Web filter vendor before – a signatureless way to stop new attacks)?
6. What endpoint security protections are in place?
7. Does your organization use any signatureless defenses such as software restriction policies or application whitelisting?
8. If the phishing had been reported, what would your procedure be identify who clicked the link and how would you prevent others from clicking?

## **Inject 1:**

The now malware infected PC is used as a staging ground by the attackers to laterally move through the organization and begin to infect other endpoints in the organization with the same malware. Within a period of a few hours the threat has spread to a large number of PCs throughout the organization. No payload has yet been triggered on any PC, so the malware is spreading but otherwise lying dormant on PCs. Infected PCs establish communication with command and control servers.

## **Questions to consider:**

1. Is any network segmentation present within the organization to prevent the spread of such threats? If so is it fine grained enough?
2. Are any controls in place to detect the spread of a threat internally through the network?
3. Does adequate network visibility exist within the organization?
4. Would the C&C server traffic be detected?
5. Does your organization make use of any threat intelligence feeds which may alert you to any potential IOCs?
6. Does your organization make use of the Ransomware Tracker block lists or other block lists as part of a dynamic block list strategy?
7. How is DNS protected within the organization?
8. Is network traffic logged? If so, are the logs audited with enough frequency?
9. Is SIEM utilized?
10. Any controls to prevent pass the hash attacks which are a common component of lateral movement strategies (e.g. Microsoft LAPS)?

# **Inject 2:**

Three months are allowed to pass and at 4am on a Saturday morning the malware authors send the command via C&C to unleash the malware payload. Within minutes dozens/hundreds/thousands (choose one that fits a significant portion of your organization’s PCs) of PC are encrypted and displaying a ransomware screen.

## **Questions to consider:**

1. How the immediate clinical needs met to ensure patient care is not jeopardized?
2. While most hospitals have downtime plans, some hospitals that experienced ransomware attacks had downtimes that extended for weeks. Does your organization have an extended downtime plan?
3. WannaCry and NotPetya, both impacted medical devices? Does your organization’s downtime plan also include the potential loss of medical devices and lab equipment due to ransomware?
4. Has your organization had a conversation about paying a ransom vs attempting recover from backups?
5. Does your organization have anyone with the know how to buy bitcoin if paying the ransom is an acceptable solution?
6. Does your cyberinsurance policy cover ransom payments?
7. If you pay the ransom, how do you deal with the fact that you are still compromised?
8. Does your organization have a reliable and regularly tested backup system? Does your testing include testing system restores?
9. Does your organization just back up data or does it back up applications too? Some hospitals with backups still took weeks to recover because they had their data backed up, but applications needed to be reinstalled.
10. How far do your backups extend back? Do they go back long enough to recover to a preinfected state?
11. Are any backups offline?
12. What is your organizations IR plan?
13. Is there an IR firm on retainer or will you need to find one (assuming this is now too big a problem to handle in house)?
14. Who will be responsible for making a decision to involve law enforcement and when?
15. How will Public Relations be handled? Who will ensure families with resident patients that their loved ones are safe?
16. Who will determine if this is a reportable incident or not?
17. When should hospital legal counsel be involved? Should legal counsel be used to bring in the IR firm to ensure that any forensic data collected is protected by attorney client privilege?
18. What are your plans for beginning to bring systems back on line while at the same time ensuring they do not become infected as soon as they are connected to the network?