Milestone 2 – Malware Case Study: Ransomware

Student Name: \_\_\_James Jordon \_\_\_  
Date: 2025-09-011  
Course: CYBR-1100 Security Awareness  
Milestone 2-Malware Case Study5

**Case Project 3-4: Banning Ransomware Payments**Different state legislatures are now considering legislation that would ban any state or local government agencies from paying a ransom. The reasoning is that if the attackers know that a state or local government is prohibited from paying a ransom, then these entities will no longer be victims of attacks since the attackers know they will never be paid. It is also said that the laws would also decrease the total level of ransomware, since paying ransoms only encourages more of this malicious activity. Some have suggested that any ransomware payments by any business or organization should be deemed illegal. But will this actually stop ransomware? What would happen to those entities that are hit with ransomware and are unable to restore their systems from backups? Debate the pros and cons of banning ransomware payments and write a one-page paper about these two sides. What is your recommendation? Why? **In my opinion, will ransomware stop if politicians stop allowing payments to hackers? Absolutely not. That does absolutely nothing for the actual problem of the hackers in the first place and how they were able to use phishing or other methods to gain access to your system and shut it down. The hackers will find other ways to blackmail you instead as they still will be there either stealing or demanding payments. Those entities hit with ransomware and were unable to restore their systems would have to revert back to their last saved backups, hoping the ransomware is not on it. According to** Tehrani (2023)**, the pros include ensuring critical systems such as healthcare would not be interrupted, could potentially decrease data leaks, and has the potential to decrease financial losses or downtime. This path could also reduce the damage to the company’s reputation. The cons include the inability to know or guarantee if the data had not been tampered, partitioned, or deleted. The other cons include hackers selling the data even after payment. This also puts a target on that organization to other hackers aiming at making a quick buck. The only responsible methods for protecting yourself are always keep and use dedicated and scanned back ups and having extra back ups off-site. Another method would be to use some sort of** Endpoint Detection & Response (EDR) **to check for early malware invasions. Holding trainings for staff about cybersecurity and how to spot and report phishing emails and scams and maintain security of the network on the data and physical layers.**

# Malware Type

Instructions:

Identify and define the malware discussed in your selected Chapter 3 Case/Hands-On Project.

Response:

\_\_\_We have chosen ransomware due to the high possibility that our target audience, elderly Boomers in assisted living facilities, will come across it if they are victims to social engineering phishing scams. The phishing scam, if opened, downloads the ransomware onto their computer or cellular device and locks it until ransom payment is made (Tehrani, 2023). \_\_\_

# Infection Method & Symptoms

Instructions:

Explain how the malware spreads and what symptoms appear on an infected system.

Response:

\_\_\_There are several infection methods used to introduce ransomware into a system, but by far the most common is the social engineering phishing scams such as phishing emails that lure unsuspecting users into being unknowingly hacked. SAGE reports that beyond phishing scams, ransomware can be introduced into a system in a variety of ways including but not limited to drive-by-downloads from malicious websites, worm-like ransomware such as WannaCry can exploit unpatched vulnerabilities, malvertising, and even insider threats. \_\_

# Evidence

Instructions:

Insert notes, screenshots, or log excerpts collected during the guided lab.

Response:

**Figure 2A-1: SAGE AI (ChatGPT) Notes on Ransomware:**  
A screenshot of a computer

AI-generated content may be incorrect.

**Figure 2A-2: Cisco NetAcad on Ransomware:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Figure 2A-3: SAGE AI on more Ransomware Infection Methods A close-up of a document

AI-generated content may be incorrect.**

# Defenses & Mitigations

Instructions:

List at least three concrete defenses or countermeasures.

Response:

According to Forbes (2021), the paying of a ransomware is not a smart move financially as there is no guarantee your data has not been corrupted, stolen, or will be re-locked for another ransom. The only way to make sure your data stays safe is to have strong safety protocols in place in terms of physical, hardware, and software security. You should also make sure to utilize appropriate backups that have been scanned and are protected both on-site and off-site. And finally, using firewalls as well as Endpoint Detection & Response (EDR) tools to monitor and stop malware invasions before they become a larger issue are three ways to mitigate the issues (Tehrani, 2023).

# NetAcad Linkage

Instructions:

Explain how this connects to NetAcad Modules 2.1–2.2 (Analyzing a Cyber Attack, Methods of Infiltration).

Response:

\_If you look to Figure 2A-2. You will see NetAcad refer to ransomware as malware built to hold computer systems hostage until the ransom is paid. This is a rather simplified statement as ransomware has so many modes of infection, can shut down entire cities as in the case of Atlanta, GA (Newman, 2018). This is also a very common method used by phishing scammers to lock their personal computers or cellular devices which is why it is so important our target audience, elderly individuals in assisted living communities, be instructed on how to spot phishing scams and stop them.

# References

Instructions:

Add References here.

Response:

Author not explicitly given. (2021, July 12). *Why paying ransomware is typically a bad idea and what you can do instead.* Forbes. [https://www.forbes.com/councils/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/](https://www.forbes.com/councils/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/?utm_source=chatgpt.com)

Newman, L. H. (2018, April 24). *Atlanta spent $2.6m to recover from a $52,000 ransomware scare*. Wired. <https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/>

Tehrani, R. (2023, September 15). *Should I pay? The pros and cons of paying ransomware hackers.* TMCnet. [https://blog.tmcnet.com/blog/rich-tehrani/security/should-i-pay-the-pros-and-cons-of-paying-ransomware-hackers.html](https://blog.tmcnet.com/blog/rich-tehrani/security/should-i-pay-the-pros-and-cons-of-paying-ransomware-hackers.html?utm_source=chatgpt.com)

Wilson, M. (2024, August 12). *Why paying ransomware is typically a bad idea and what you can do instead*. Forbes. <https://www.forbes.com/councils/forbestechcouncil/2021/07/12/why-paying-ransomware-is-typically-a-bad-idea-and-what-you-can-do-instead/>