Name: Alhambra, Berna Marie C.

Course/Section: CS301

Date: 12/13/2024

Ransomware Simulation

Objective:

To educate students on the dangers of ransomware, demonstrate how ransomware attacks are executed, and understand the impact on victims using a ransomware simulator in a controlled environment. This module aims to provide hands-on experience in both attacking and defending against ransomware, fostering a deep understanding of the technical, emotional, and ethical aspects of cybersecurity.

Materials Needed:

- VirtualBox software
- Windows 10 ISO file
- Ransomware Simulator

Part 1: Setting Up the Virtual Environment

1. **Create a New Virtual Machine:**
   - Open VirtualBox and click on "New".
   - Name the VM "Windows10-LastName".
   - Select the provided Windows 10 ISO file or download a legitimate copy from Microsoft's website
   - For the account, use "12345" as the password
   - Use the product key provided by your professor to proceed to the Setup properly.
   - Allocate at least 2GB of RAM and 20GB of hard disk space.
   - Follow the prompts to create the VM.

2. **Install Windows 10:**
   - Follow the installation prompts to set up Windows 10.
   - Once installed, create a user account and complete the initial setup.

Part 2: Understanding Ransomware

What is Ransomware?

Read the article **A Guide to Ransomware** provided by the **National Cyber Security Centre** and answer the questions below:

1. What is ransomware, and how does it typically prevent access to your device and data?

   According to National Cyber Security Centre ransomware is a type of malware in which this prevents you from accessing your device and the data that is stored in it, usually the criminal group will demand for a ransom for you to take control of your device or data again.

2. Describe the three main stages of a ransomware attack.
   The 3 main stages are:

- 1. Access – The attackers will gain access to your network and they will establish control
- 2 Activation – After stage 1, it will now proceed to malware activation which causes the device and data to be no longer accessible

- 3 Ransom demand – At this stage, the cyber criminal will ask for a ransom for you to take over your computer and data again

4. Why isn't it advisable to pay the ransom? What are the potential consequences of paying said ransom?
Because even if you pay them the ransom that they are asking for, there will be no guarantee that they will grant you access to the computer and data, it is still also vulnerable or infected and is susceptible to future attacks.So it is not advisable to pay the ransom without thinking about the after effects of it

5. What measures can you make to prevent ransomware attacks?
The counter measures you can do to prevent ransomware attacks are: backing up your data which is one of the most effective way to counter data loss and reading about guidelines to be aware and recognize if you are vulnerable to ransomware attacks

6. Why is it important for organizations to carry out monitoring and detection on their networks?
Because an organization affects everyone, it is not a sole attack where only one person will be affected. Organizations are susceptible because they will have a large population that can be affected once they are attacked.

7. What steps should an organization take immediately after discovering a ransomware infection?
The steps they should take are: consider the payment in ransomware incidents, knowing how to recover an infective device, recovering the hacked account, mitigating malwares and ransomware attacks, how to effectively detect and respond to these dire situations.

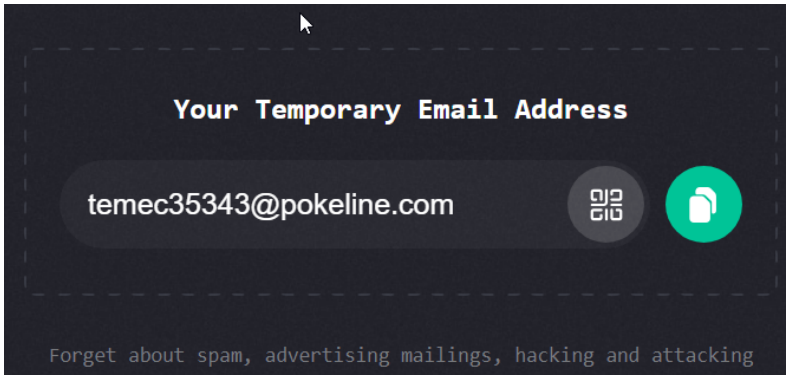
8. What are the legal implications of a ransomware attack for both the victim and the attacker?
Victims might face financial loses and potential regulatory compliance issues while the attacker will face legal consequences for their said actions.

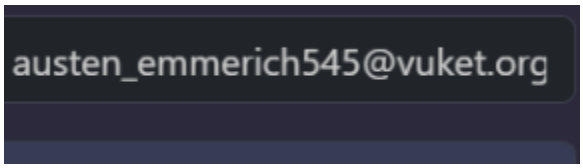
Part 3: Planning and Executing an Attack

1. **Planning the Attack:**
   - Form pairs or small groups. Each group will plan an attack that appears to come from a classmate.
   - Discuss and document the steps to deliver the ransomware simulator executable to the target VM. This could include:
     - Using a USB drive (simulated within the VM environment).
     - Sending an email with the executable attached.
     - Sharing the executable through a network share or cloud storage.

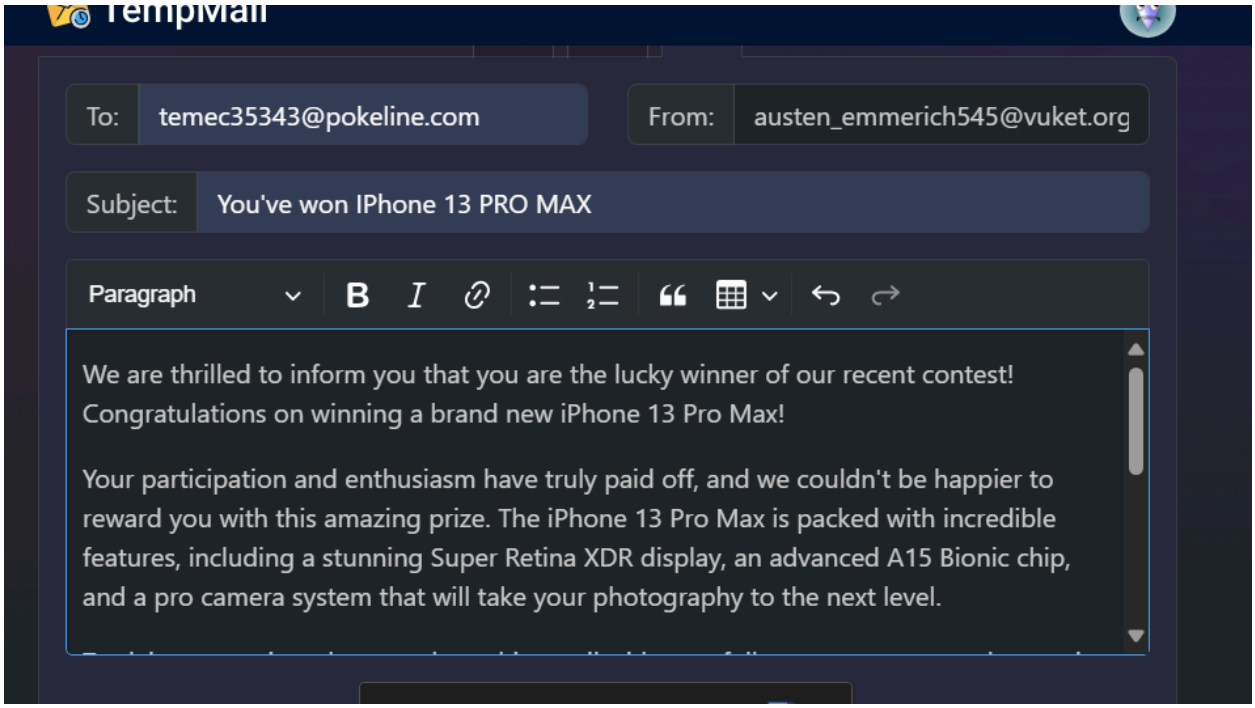
2. **Executing the attack**
   - Map out the details of your plan to attack your classmate. Add screenshots/images of your plan.

Creating fake email /name address





Curating the message



- In your own assessment, what is the success rate of your attack?
  The success rate of the attack was 90% since the ransomware got received by the user, however you would need to disable the windows security for this to work.

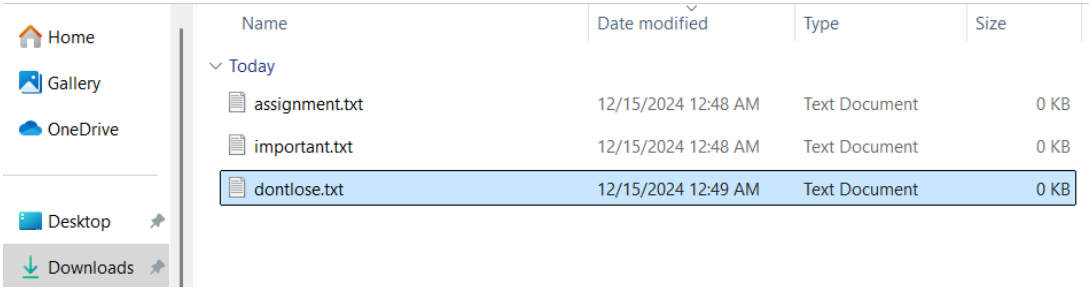
- What difficulties did you encounter while executing the attack? How did you overcome them?
  The main difficulty is having a hard time is to confirm that your windows defender antivirus is turned off and along with that it is always notifying that there is a ransomware detected

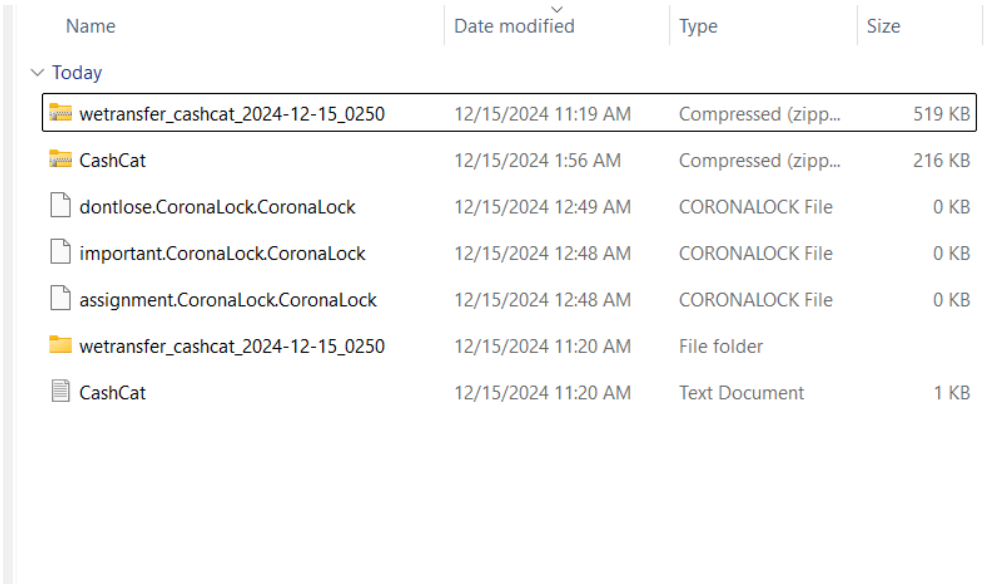
- How did you feel about simulating an attack on a classmate? Did it raise any ethical concerns for you?
  It raised ethical concerns since you are basically taking advantage of another person. Maybe they are gullible and the message looked so legit that they went and fell to click the link. Just thinking about it, if that happened to me, I would not want to do it to another person.

- How do you think your simulated attack affected your classmate emotionally and practically?
  Initially, there was a shock and then that shock led to panic. Asking what to do or what is the next step for the person to recover their files or their sensitive data. It is a great loss for the victim side.

Part 4: Experiencing the Victim's Perspective

3. **Simulating a Victim's Experience:**
   - Create important-looking .TXT files on your VM (e.g., notes, assignments).
   - Run CashCat to simulate the attack.
   - Reflect on the emotional and practical impact of discovering these files have been "encrypted".
   - Discuss how it feels to be targeted by a classmate and the sense of betrayal and frustration that can arise





4. **Initial Reaction**
   - How did you feel when you discovered your files were "encrypted"? What was your immediate reaction?
     As a victim, the initial reaction was being shocked. Within a simple click and all of your important files are now gone without the guarantee that you will get them back even if you pay them the amount of money they were asking for. If this happened to me in a real situation, my reaction would be more intense and I am not sure what will be my next step.

   - What emotions did you experience knowing that a classmate simulated an attack on your system?
     I was mainly anxious. Even if this is just a simulation, come to think of it, anyone who knows their stuff well can attack you and persuade you. Even if this person is someone you know or worse, your friend. So it had a quick reflection on me to really think well in terms of who to trust and what is the extent of your trust on them.

   - If you're in this kind of situation, what will you do in response to the attacker? What will you do to recover your files?
     I would not do anything by myself first, since I am not that knowledgeable about this. I would consult an expert and ask them what the next steps I need to conduct. I do not want to make matters worse by acting based on my emotions and intrusively.

   - What security practices could you implement to prevent such attacks in the future?
     Have a daily checkup on my computer to see the security patches are turned on and updated. Be educated to even if the email may seem legit is to never ever click on external links. If this is from a legitimate source, have to contact the customer service first before moving to the said instructions they sent.

Part 5: Testing the Effectiveness of Windows Security

1. **Enabling Windows Security:**
   - Ensure Windows Security (Windows Defender) is turned on in your VM.
   - Go to Settings > Update & Security > Windows Security > Virus & threat protection.
   - Ensure that Real-time protection and Cloud-delivered protection are turned on.

2. **Running the Simulator with Windows Security Enabled:**
   - With Windows Security enabled, run the ransomware simulator again.
   - Observe if Windows Security detects and blocks the simulator's activity.

3. **Analyzing the Results:**
   - Compare the results with and without Windows Security enabled and answer the following questions:

   - When you ran the ransomware simulator with Windows Security enabled, what was the immediate response from Windows Security?
     It did not allow me to run the app and had me notified that the app has been blocked due to my protection. It also displayed that the app is detected to be a ransomware and it provided me further details to what is the nature of the app

   - Did Windows Security detect and block the ransomware simulator? If so, how did it notify you of the threat?
     It displayed a pop up notification on the lower right corner that this app is detected to be a ransomware and also I encountered a lot of notifications and warnings telling me that this app is unsafe or detected to harm my computer.

- How did the Real-time protection and Cloud-delivered protection features of Windows Security contribute to detecting the ransomware simulator?
  The real time protection immediately scanned the file and once it found that the file is malicious it instantly notified me, when I tried to execute the file it provided me warnings and blocked its execution. This also allowed me to not be able to execute unauthorized apps in my computer.

- Were there any additional features or settings in Windows Security that enhanced its effectiveness?
  One feature that is really helpful in this simulation is the controlled folder access in which this feature will help prevent unauthorized applications like the ransomware simulator from accessing or modifying protected folders.
- Based on your observations, how effective do you think Windows Security is in protecting against ransomware attacks?
  Based on the simulation, it was really effective since it instantly notified me that this application was ransomware. I had to tweak the security in order for me to run this application and also while downloading the file I was also notified that this app has potential security threat. So I can say it is pretty effective.

- What are the strengths and limitations of using Windows Security as a primary defense against ransomware?
  The strengths are it provides real time scanning which notifies the user of the security threat that they are encountering. It also provides a control folder access in which unauthorized apps are not able to change the contents of the files or protected files/folders. The weakness is that if other features are disabled the performance dramatically decreases with that the user must know how to configure since windows always conduct regular updates.

  _