Ransomware Teacher Instruction

Background:

Ransomware is a form of *malware* that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key. Learn these 14 Real-world phishing examples - and how to recognize them and Phishing prevention tips for best technology practices. Here are some additional resources you can use to better understand the dangers of Ransomware:

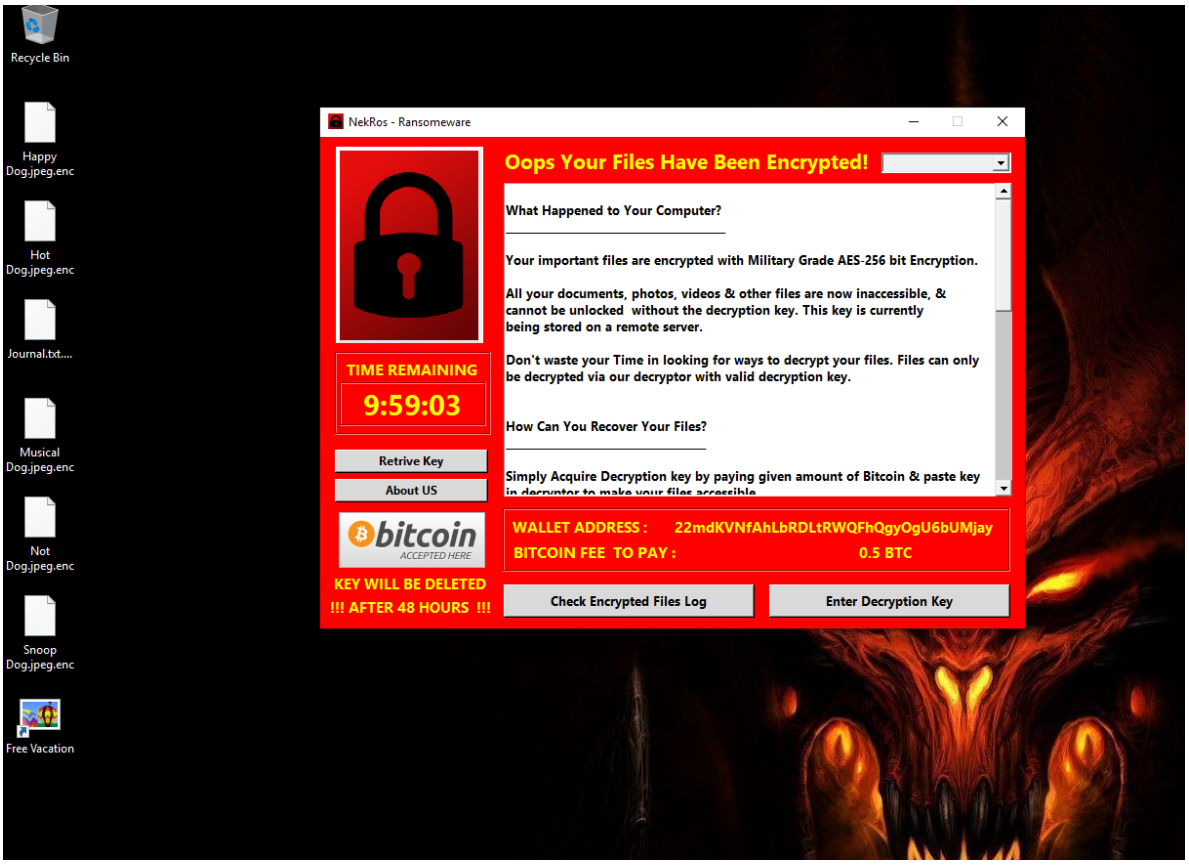
- https://us-cert.cisa.gov/Ransomware
- https://www.youtube.com/watch?v=d_dyi9CWieo
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware

The workout is derived from open-source training ransomware Nekros: https://github.com/PushpenderIndia/nekros . This only guides the user through the process of the attack, but does not actually harm the computer.

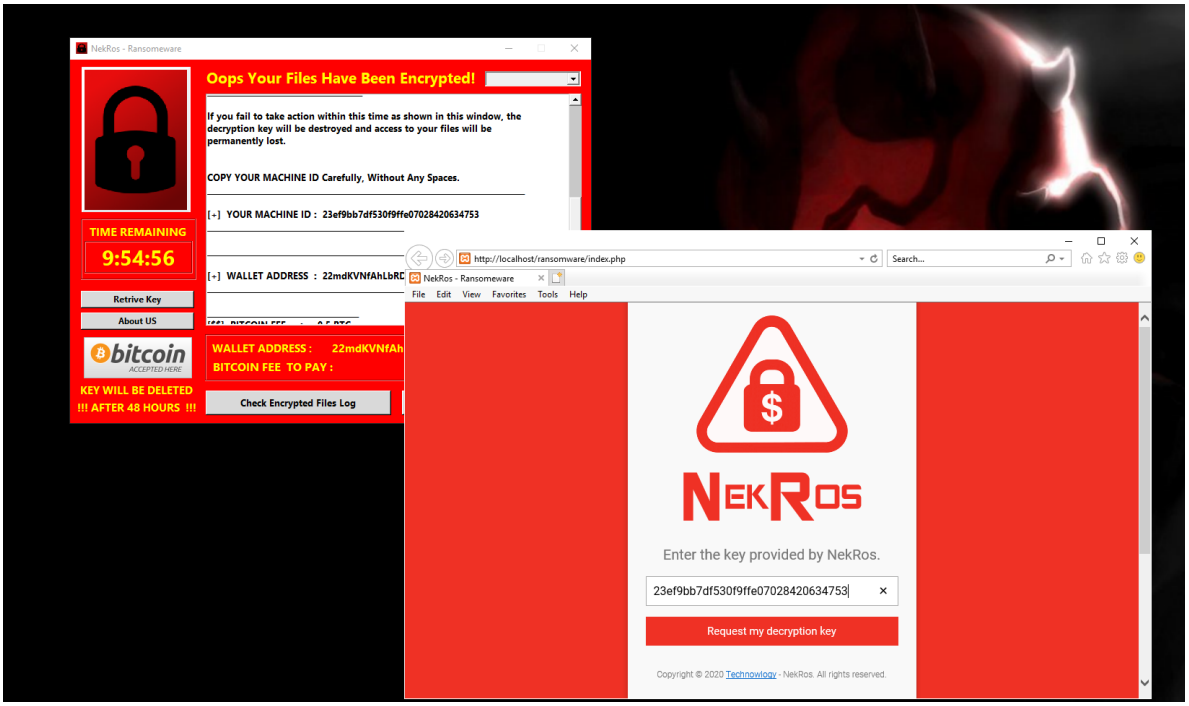
Attack Mission:

After logging in let the computer finish all of the startup processes. This sometimes takes a few minutes. If nothing happens for students, tell them to wait a few minutes and try again.

Students begin the ransomware attack by opening ‘Free Vacation’ located on the Desktop. This is a Python file that launches the attack to encrypt all of the files on their Desktop. They can open the files in Notepad to see the random text. Once the attack successfully completes, the students should see something similar to the image below:



This is very similar to what they would see in a real attack, and it will probably take them some time to read through and understand what to do next. In a real attack, the “Retrieve Key” would not be enabled until the victim paid the ransom. However, the student can click the retrieve key button to open up the local website. The student will also need to scroll down and copy over the machine key as shown in the diagram below.



Understanding this process will be the most time-consuming portion of the workout, and students may need to struggle with this for a while before they understand the process. The learning objective here is to understand the adversary's approach to ensure the files remain encrypted until they have given information for recovery.

Once they click to request my decryption key, they will copy and paste over the decryption key into the tool. Then after clicking OK to the warning message, the tool will decrypt and restore their files in the original format.

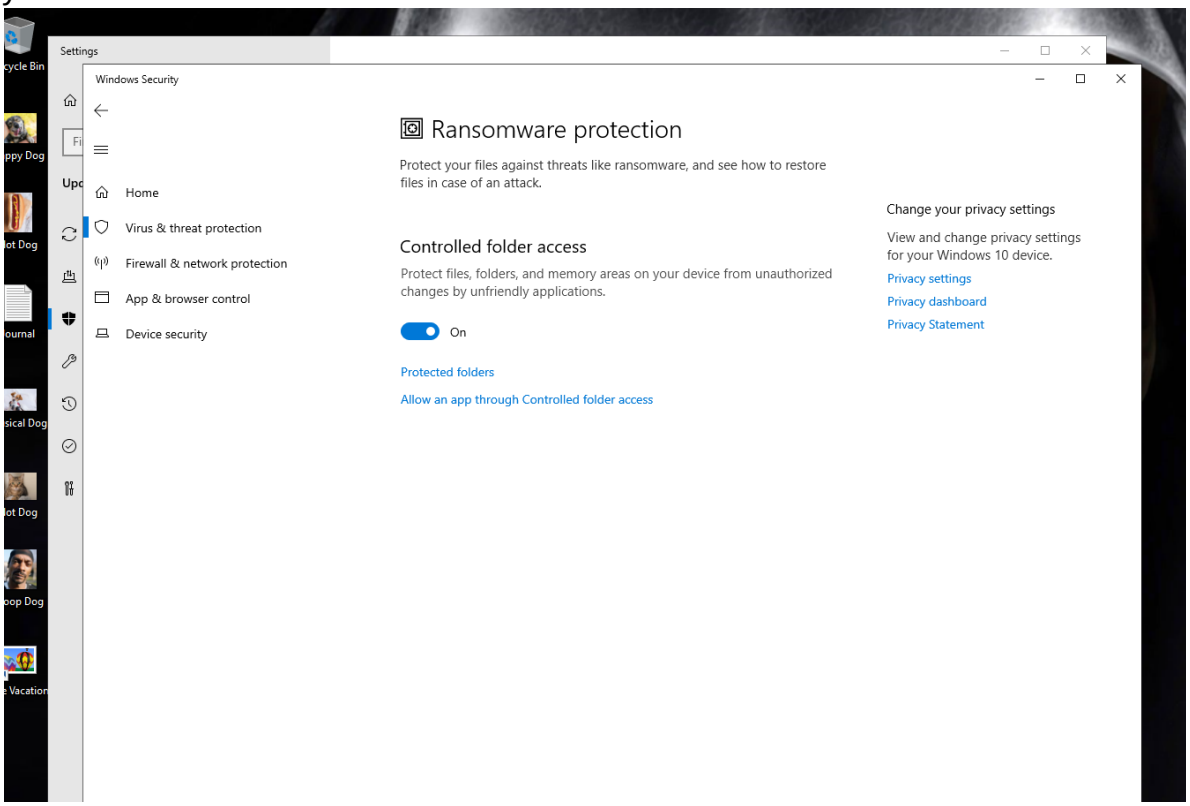
The mission will automatically assess as complete once they obtain the decryption key

Defense Mission

The objective of this mission is to show how Ransomware can be prevented and for the student to consider the tradeoffs for this type of protection. To begin this mission, open up Windows Defender Settings by going to the Start Menu and typing "defender". The students have a link to research the ransomware protection. They should spend some time troubleshooting the configuration. Protection does not come easy!

In Defender, you can click on Virus and Threat Protection. Then you should see *Ma nage Ransomware Protection* at the bottom of the screen. Click on this as shown below. To successfully protect against the attack, they should enable *Controlled*

folder access. They also need to click on *Protected folders* and add their Desktop folder. Once they have completed this step, there is a script that automatically assesses the mission as complete, and you should see the student's completion in your instructor view.



Assessment and Reflection

Feel free to use these questions in your own assessment tool for students to spend time reflecting on the workout and researching more about the experience.

1. What cybersecurity properties does the ransomware attack directly violate (i. e., confidentiality, integrity, availability) and how?
    a. **Answer:** Primarily this impacts the availability of data, but it also impacts the integrity of the system. Either answer can be correct. The confidentiality of the data may be violated, but the student will need to explain that confidentiality can be violated if the attacker chooses to exfiltrate the data.
2. Describe a system in which this type of attack would cause the greatest harm and explain why.
    a. **Answer:** The answer should describe the loss of availability for some system. It could be a hospital device, city services or some other

system, but the answer needs to describe the harm caused by loss of availability of the information.

3. Read the BBC report on the U.S. Justice Department's attribution of the Wannacry ransomware: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and. How could this attack be used by an adversary to perform additional harm beyond the ransomware attack? Why would an attack with additional harm be effective against the victim?
    a. **Answer:** The adversary has compromised the integrity of the system. The malware could contain code to allow the attacker to turn off the ransomware and perform some other malicious function. The attack would be effective because the victim would only expect a ransomware attack
4. Read the Wired report on Marcus Hutchins who managed to stop Wannacry before it became a global threat: https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/. This is a very good but very long article. You may want to skim over sections. How did he stop Wannacry and what malware had he written a few years prior to saving the Internet?
    a. **Answer:** He found a DNS server in the code that was used for activating the attack. Once authorities turned off the server, the attack no longer spread. The malware he developed was the banking trojan Kronos.
5. Consider the countermeasure you set up for Ransomware. Most countermeasures have tradeoffs. If you were setting this up for multiple people, what is one way this countermeasure fail? How might the countermeasure cause a lot of additional work for you?
    a. **Answer:** The countermeasure could fail if you did not protect the correct folders. Users may store important data in many different locations on their computer. It could create additional work by having to whitelist a lot of different applications. For example, cloud synchronization access files similar to ransomware, and these would have to be whitelisted and maintained.