LESSON NOTES

# CYBERSECURITY

## Domain 2.0 - General Security Concepts

### 2.4.2 - Ransomware

## Lesson Overview:

**Students will:**

- Analyze potential indicators to determine the type of attack.

**Guiding Question:** What is ransomware and cryptomalware and how can students defend themselves against these attacks?

**Suggested Grade Levels:** 10 - 12

## CompTIA Security+ SYO-701 Objective:

2.4 - Given a scenario, analyze indicators of malicious activity

- Malware attacks
    - Ransomware

*This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).*

# Ransomware and Cryptomalware

Ransomware is a type of malicious software, or malware, that encrypts and locks a victim's data and/or device, then demands a ransom to restore access to the locked resources. In most cases, the ransomware victim must pay the attacker within a certain timeframe or risk losing access to the resource(s) forever. Ransomware is especially harmful since data can be very valuable. Personal data, such as personal finance data, family photos, and videos, are examples of important data that could be lost. Organizational data could be employee and customer information, company financial information, and proprietary data or trade secrets. Imagine if you lost the last photograph of your grandmother or if a large company, like Apple, lost access to its designs for the newest iPhone. How much do you think you, or a malicious customer, would pay for access to these precious pieces of data?

There are many different types of ransomware attacks. A common term is cryptomalware, which has multiple meanings. One version of cryptomalware is when a virus encrypts files, folders, or entire hard drives. In most cases, your underlying OS (Operating System) remains available, but most of the data is encrypted. Cryptomalware can also be a form of ransomware, but instead of money, the victims are forced or asked to pay in cryptocurrency since it can be much harder for law enforcement to track. A third and final form of cryptomalware is when a computer has been taken over to help mine for crypto-currencies. In 2019, Baltimore City's governmental computer systems were infected with a new and aggressive ransomware variant named RobbinHood. All servers, except for essential services, were taken offline. In a ransom note, hackers demanded 13 bitcoins (about $76,280) in exchange for keys to restore access. The note also stated that if the demands were not met within four days, the price would increase, and within ten days, the city would permanently lose all its data.

Other versions of ransomware include lockers, scareware, and doxware. Lockers, also known as locker-ransomware, affect the operating system and completely lock out a victim from their computer or device. Lockers make it impossible for the victim to access any files or applications. Locker-ransomware is most often Android-based. Scareware is fake or phony software that acts as a cleaning tool or antivirus software. Scareware alerts users of issues found with the computer or device and demands money to fix the problems. Scareware can temporarily lock your computer and flood your screen with annoying pop-up displays. Doxware, also known as extortionware or leakware, threatens to release stolen data online if the ransom is not paid. Many people store sensitive data and personal photos on their devices, so it is understandable that a victim would panic and pay the ransom to avoid disclosure. Often, public officials and celebrities are the victims of doxware.

## Defense

Ransomware is profitable for cybercriminals because, many times, victims simply pay the ransom. Prevention is the best way to protect your data and devices. This often includes user training within an organization and learning to be on guard against potential threats. Data backups help defend against ransomware. If possible, use a cloud service. If the data is backed up, there is no need to pay a ransom to access the data. Any data between the time of the attack and the most recent backup will be lost, so be sure to keep software up to date, including the operating system, applications, and security software. Avoid paying the ransom. It is possible that access to the files is not restored even after paying. A cybercriminal could ask the organization to pay again and again, extorting more and more money from you but never releasing the data.