Read the following articles:

 http://www.cbc.ca/news/technology/ransomware-europe-russia-ukraine-petya-

bitcoin-1.4179683

 http://www.cbc.ca/news/canada/toronto/oshawa-hospital-cyberattack-1.4114758

 https://www.thestar.com/news/canada/2017/05/13/ontario-health-ministry-on-

high-alert-amid-global-cyberattack.html

Ransomware Basics

1. What is a ransomware attack?

A ransomware attack is when a certain type of software seizes control of a

computer, and it encrypting its contents and rendering them inaccessible. Usually,

ransomware blocks the access to the computer until a sum of money is paid.

2. How does ransomware work and what does it affect?

Majority of ransomware is delivered via email that appears which usually entices the

individual to click the link or download an attachment which leads to the malicious

software. It can also be delivered via download attacks on compromised or malicious

websites. However, some ransomware could also be delivered through social media.

Majority of the time, ransomware does not really target individuals but they acquire

many different emails or websites and use that to deliver ransomware in order to make

money. Depending if the ransom is paid or not paid, attackers could also extract useful

and important information from the compromised machine

3. How could you be affected by a ransomware attack?

4. How can you protect yourself against a ransomware attack?

You can protect yourself from a ransomware attack by getting anti virus protection

services or by not clicking on un known links or emails that you have received

Canadian Attacks (In The Past)

1. What was affected in Canada in the articles above?

In Canada, ransomware affected a hospital located in Oshawa. This hospital is one of

tens of thousands of victims of an unprecedented cyberattack that hit around 150

countries prior. However, the hospital records were not breached at all and personal

ICS3C0/2O0 Case Study C.5 - Ransomware Analysis Name:

information of patients were safe. Also, Canadian health ministries were also affected in

Ontario due to the cyberattack that hit Lakeridge Health in Oshawa.

2. How badly was Canada affected?

Canada was badly affected due to the attack paralyzing computers and networks.

Many organizations and individuals were affected, majority however did not realize

there were also being affected with the ransomware. Many IT experts continued to

work on the problem with the aim of fixing the computers for the hospital

departments. Many cyber attackers took over many computers and encrypted the

information on them and demanded usually a payment of around $300 worth of

Bitcoin

3. What other countries were affected?

Countries that was hit the hardest due to the ransomware attacks were Ukraine,

Russia, USA, and majority of Europe. For the United States, the malware affected

many companies like drugstores, food brands and many more. Ukraine’s cyber-

attack included top level government offices where many officials posted photos of

darkened computer screens, as well as many energy companies, banks, cash

machines, gas stations and other supermarkets

4. Where did the attack come from?

The attack came from the malicious malware known as “WannaCry”. They used a

SMB protocol in order to help various nodes on a network communicate, and

Microsoft implementation can easily be tricked by specially crafted packets into

executing arbitrary code. This is how it managed to infect many computers.

5. Why was the attack started?

The attack most likely started due to the attackers wanting a large sum of money.

The attackers target many high populated areas in order to draw the most money.

Furthermore, since the attackers attacked the hospital, they most likely wanted to

steal patients’ info in order to most likely commit identity theft or fraud.

6. How was the attacked stopped?

The attack was stopped through companies and organizations updating their

operating system to ensure they aren’t vulnerable to another attack. Some

antiviruses managed to deflect the attack even though some of the “WannaCry”

software forced other computers to reset however.

Canadian Attacks (Present Day)

ICS3C0/2O0 Case Study C.5 - Ransomware Analysis Name:

1. Google “ransomware attack Canada 2019” and research an attack that occurred in

the past two months.

a. Summarize the attack in a paragraph that describes: who, what, where, when.

Nunavut, Canada&#39;s largest and most northerly territory, is working hard to recover from

a ransomware attack that struck over the weekend. The sophisticated cyber-assault

was launched on the sparsely populated territory&#39;s government network at

approximately 4:00 am on Saturday morning, resulting in the swift encryption of multiple

Word documents and PDF files. Users trying to access the infected government

network were confronted with a ransom note that read: &quot;Your network has been

penetrated. All files . . . have been encrypted with a strong algorithm . . . we exclusively

have decryption software for your situation. “The threat actors behind the attack

instructed users to download an encrypted browser and visit a specific URL within the

next 21 days. Users were told that the sooner they pay, the lower the price they will be

charged to recover their encrypted files.  In an attempt to contain the attack, the

government shut down parts of its network, leaving many government employees

unable to access their email or voicemail. All government services requiring access to

electronic information were impacted by the attack, with the exception of Qulin Energy

Corporation.