ICS3C0/2O0 Case Study C.3 - Ransomware Analysis Name:

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>

Guidelines for writing a supported opinion paragraph (SOP)

· <http://schools.peelschools.org/sec/fletchersmeadow/studentlife/OSSLTprep/Documents/Sample_%20Writing%20a%20Supported%20opinion%20paragraph.pdf>

**Level 1: Ransomware Basics**

1. What is a ransomware attack?

Malicious software that locks up computer files with all-but-unbreakable encryption and then demands a ransom for its release.

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

Security vendors including Bitdefender and Kaspersky said the NSA exploit, known as EternalBlue, lets malware spread rapidly across internal networks at companies and other large organizations."Once activated, the virus can automatically and freely distribute itself on your network," Ukraine's cyber police tweeted.One reason the attacks appeared to be slowing down was that the ransomware appears to spread only when a direct contact exists between two networks — such as when a global company's Ukraine office interacts with headquarters. But once it hits a computer on a network, it spreads quickly, even among computers that have applied the fix for the NSA exploit.

**Level 2: Canada & Other Countries**

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

A hospital in Oshawa is among the tens of thousands of victims of an unprecedented "ransomware" cyberattack that's hit 150 countries in recent days. Lakeridge Health — one of Ontario's largest community hospitals — said it appeared the ransomware threatened its computer system, but a spokesman said the facility's system was able to deflect the attack.

2. How badly was Canada affected?

"Our antivirus software contained the attack and so while we've had to reset some of our systems we weren't affected in the same way that other places were," said Lloyd Rang.

3. What other countries were affected?

The cyberattack has paralyzed computers and networks around the world, including the ones that run Britain's hospital network, Germany's national railway and scores of other companies and government agencies worldwide.

**Level 3: Canada & Other Countries**

1. Where did the attack come from?

A Lakeridge Health spokesperson Lloyd Rang said they “don’t know for certain yet” what enabled the attack because the focus has been “on fixing the immediate problem.”

2. Why was the attack started?

The cyber attackers took over the computers, encrypted the information on them and then demanded payment of $300 or more from users to unlock the devices. As people fretted over whether to pay the digital ransom or lose data from their computers, experts said the attackers might pocket more than $1 billion worldwide before the deadline ran out to unlock the machines.

3. How was the attacked stopped?

According to a provincial government source, the emergency management branch of Ontario’s health ministry opened a command centre at its downtown Toronto offices Friday afternoon to provide technical assistance to any hospitals experiencing trouble. And the office of the ministry’s chief information officer established a call centre to aid the sector. Oshawa remained in a Code Grey Saturday morning as IT experts continued to work on the problem with the aim of first fixing the computers in the ER and critical care departments. Connection to patient records had been restored but “performance was still not optimum,” the source explained.

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

If you are on inappropriate websites, or websites that aren’t considered secure by your antivirus software. By doing this, you are in uncharted territory where you are not protected and have no safety net if something goes wrong. You could also be affected if your operating software is not up to date, exploiting a loophole only on an older version.

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

By staying within the boundaries of your antivirus bubble, as well as frequently updating your operating system to provide a relatively stable experience.