**1. What is a ransom ware attack?**

A ransom ware attack is a malicious software that threatens to publish the victims data or block access to it unless a ransom is paid.

**2. How does ransom ware work and what does it affect?**

A ransom ware program/virus goes through the user’s computer and pretty much locks all their files by encrypting it with a encryption that is pretty much impossible to crack without the encryption key. It mainly affects your files, only your files so when it’s paid the attacker can unlock it.

**3. What was affected in Canada in the articles above?**

Oshawa hospital Lakeridge Health

**4. How badly was Canada affected?**

Canada wasn’t that affected as the systems were in the hospital were able to defend against the cyber-attack keeping patient records and details save. But smaller businesses may have not have been successful in the defend.

**5. What other countries were affected?**

Roughly 150 different companies within the recent days.

**6. Where did the attack come from?**

Beijing

**7. Why was the attacked started?**

I don’t know, for money hence the reason of a ransom attack.

**8. How was the attack stopped?**

A 22 year old that works for Kryptos Logic registered a garbled domain name hidden in the malware has warned the attack could be rebooted.

**9. How could you be affected by a ransom ware attack?**

It could happen by accident, this how most of them happen. When opening a “sketchy” looking email or even a trustworthy one, if you click to open a document it, could encrypt the hard drive making it impossible to access or retrieve anything stored on there.

**10. How can you protect yourself against a ransom ware attack?**

Anti-Virus software could protect against that but no software is perfect, criminals are always finding ways to work around the anti-virus and it’s security checks.