Your group will select a cybersecurity current event to discuss with the class. Please find an article from the last three months which is related to one of the topics from the cybersecurity topics we discussed last week. You can use the network security documents (1 and 2) in Canvas as a reference.

Your group should strive to answer the following questions:

What is your article about? Think about what happened, who is affected, etc.

* This article is about APT41, a state-sponsored Chinese cyber threat group. They conduct espionage as well as state-sanctioned/sponsored cyber attacks. The main target for the group is mostly the Chinese market-driven video game market where they have done various attacks including digital currency market manipulation. What makes this scary is that they have the protection from the chinese government but also access to government/non-public level malware for espionage.
* The group’s main financial motivation is in the video game market, but it also has constant access to various critical systems:
  + Healthcare
  + High-tech firms
  + Telecommunications
  + Higher education
  + Travel services
  + news/media firms.
* The group has been notoriously hard to combat. If counter measures are taken they are up and running back in their system within hours. They are sophisticated in their abilities. They get into a system with simple but effective spear-fishing attack and from there may install root kits and bootkits to hide their advanced malware and prevent themselves from being detected. They work well within a targets network obtaining access to certificates to authenticate the installation of their malware.
* The security implications are enormous and they obviously have the ability to target any kind of organization they deem fit. This is why the topics discussed this week are so important and relevant. Having a well-planned and implemented access control protocol in place is an example of effective deterrence. Limiting access control to only where its needed prevents these attackers from moving laterally through the network at their will when searching for information and valuable resources.
* This example article showcases the need to have proper detecting protocols and systems in place. Having the data available for analyzing and detecting attacks could help mitigate the problem and get it solved sooner. The ability to adjust is key.
* Also keeping your software up to date is a good way of preventing this. I dont feel like its one of those things that should be said, as its an obvious one but gets overlooked too often giving attackers a way into the network.
* The thing is, if it werent this group it could be another. The consumer facing implications of a group like this is enormous. If they can crash hospital systems or change records what would be the damage? This also goes for any of the other vulnerable industries they already have access to. Their fate is already determined to change at the flip of the switch. This makes our whole system vulnerable.

- The article is about APT41, and the responsible group is using malware, code exchanged and stolen certifications to gain control of the intended victim's information. They have targeted video gamers, health care networks, and espionage political campaigns, and personal informations.

How does it relate to one of the topics we discussed last week? (I.e. access control, perimeter security, etc.)

The article relates to the following points. Management of software update mechanisms, Policy enforcement for configurations, and security services for inbound/outbound traffic.

What are the security implications for organizations?

The best security implications that an organization can use is enabling the ability to download any virus protection from the web, educating all personal about spear phishing, and setting up a system that can monitor digital signatures and placing an expiration date on the signatures.

What are the security implications for consumers? (If applicable)

For consumers, they need to be careful as to keeping their information stored on their gaming systems. Also, they need to fully research the different software that they download and the source that they’re getting it from. Because APT41 has the ability to disguise its software as something that a consumer needs it is important that the consumer checks their digital signatures and cleans their system on a regular base.

What can be done to mitigate the risk associated with the issue? (I.e. software updates, stronger passwords, etc.).

Unfortunately because their technics are so advanced it’s really hard to find a sure fire way to mitigate the risk. The only good thing that I will say about APT41 is that they do not target just anyone. They have specific targets and limit their malware so that it does not affect those that are not on its list. Although that is an upside to it. A person must make sure that they are careful with that, and the website is veridic and not a fake copy.