CONFIRMED and VETTED FINAL PROJECT OUTLINE:

1. What is malware?
    a. What is MALWARE (Pegasus)? (OMAR)
        i.

First of all, we need to know what malware is. Malware is a software that intend to damage the system that you are using, steal the data you have or harm the user. Malware could make your system slow and not very inefficient. Also, malware could steal important data that the user is saving in the device, and in that way it could harm the user. Pegasus, viruses and spywares are all a different kinds of malware, they all do the same thing. According to radware website, the first malware was discovered in 1971. It was called “the creeper”, and it did not cause any damages to the user. The creeper displays a screen daring you to capture the creeper, but it caused no harm. Malwares started to develop and became more harmless.

Malwares now are used to damage users’ systems, and steal data. Pegasus was first found in August 2016, and Pegasus is a spyware. Pegasus got exposed after an attempt that failed against a human right defender. After investigating about it, some details about the spyware got reveled. The spyware is capable of reading the text massages on the phone, it can trace the phone, it can get the passwords of the phone, get the calls and get information from the applications that are installed on the phone.

2. How malware affects people/businesses (For the particular area you identify, provide evidence on why this issue is important and its impact on business.) Alex & Andrew, your parts are pretty similar so make sure they aren’t just stating the same thing.
    a. Provide evidence on why this issue is important (ALEX)

We must consider why malware would be important to end consumers. This is an important step because we must alert users what is really at stake in a malware attack, and users will want to avoid malware not only on their home computers, but while they are at the organization as well. Users would consider their files, privacy, system, and money important, and they stand to lose any or all of these things due to malware. Common types of malware include ransomware, boot-sector viruses, and spyware. A quick overview of each reveals they all have the ability to seriously disrupt a user’s workflow and data.

Ransomware affects the entire drive by encrypting people’s files.

Boot-sector viruses mess with a drive’s boot sector, making it unbootable.

Lastly, spyware monitors a user’s activity, and can even interfere with their computing.

Ransomware has become a very popular form of attack, especially in recent years. When a user is targeted, their files are encrypted, and a ransom is demanded to get the encryption key to decrypt the files. Without this key, there is no way to retrieve the files. One such example is a ransomware by the name of WannaCry, where attackers would encrypt the files, then demand the ransom in bitcoin, which is very common because transactions using bitcoin are untraceable. Additionally, after a specific amount of time passes, the ransom doubles, and after 7 days, the files are destroyed. Users suffering from this type of malware can not only lose their files, but also a significant amount of money should they choose to pay the ransom. By contrast, boot-sector viruses tamper with the boot sector of a hard drive, causing the computer to be unable to boot. This type of virus was more popular in the days of DOS, and one infamous example was the Michelangelo virus, which on March 6 th , would overwrite the first 100 sectors of the hard drive with nulls, making the data on the drive inaccessible. Users affected with this type of virus would lose their files, and possibly the system entirely, since the OS would not be able to be loaded.

Additionally, spyware will monitor user activities and even hijack said activity and redirect users to other places. Some, such as Hot as Hell, will dial toll numbers and cost the user money. Internet Optimizer hijacked error pages and redirected them to a controlling server. Keyloggers also track keystrokes and are able to steal information through what the user types including passwords. Because of this, users would lose money through the toll lines, and privacy through the keyloggers tracking everything they type.

This is just a small sample of malware that a user can be infected with and can seriously mess with their files, money, privacy, and their system. In order to keep all this from happening, we have to be aware of this, and keep malware off of the systems. Businesses are affected as well, as the ransomware has affected entire systems such as airports and hospitals.

b. Impact on business (ANDREW)

Today, malware is the most dominant issue in the e-Business arena. It has affected many aspects of a business from the end user to online services. Malware has been so impactful that it has triggered responses to combat it. For the most part, these responses have been playing catch up. Some of these responses have not been sufficient enough to combat the malware. A lot needs to be done quickly in order to stop the devastating destruction malware has on businesses.

E-Business has been very important in the 21 st century because it has contributed greatly to the world economy. In order for an e-Business to thrive, it needs access to the internet and web for it to continue its growth. There are lots of positives that come from the web. Lately, e-business have been using Web 2.0 technologies to further grow their business. On the contrary however, this brings in negatives like malware. Malware has been so impactful on businesses that in 2007, it has done US$ 67.2 billion in damages directly and indirectly. In addition to this, businesses have invested US$ 7.8 billion to fix and repair all the damages that malware has cost them. Not only are businesses affected financially but the confidentiality of classified material can be stolen or the availability of data to be lost, could lead to theft of personal information about customers or staff of your organization. After all of those damages this could also lead to the brand being damaged as well.

Plenty of customers will now try to avoid a business if they have learned that their customers credit card information has been stolen. Some companies are risk of facing fines if they are unable to keep data from being breached. Adobe fell victim to this incident as they were fined US$ 1 million for a data breach back in 2013 for having more than 3 million encrypted customer credit card records were stolen. This will obviously result in a lost for business with the consumers. In 2009, Amazon and Walmart were both victims of a DDoS attack during the Christmas season. Both of their websites were taken down. Amazon and Walmart were eventually able to fix the problem but they already suffered from heavy losses from the attack. Amazon and Walmart are big enough to recover from these attacks. Small businesses however have a much harder time to recover and could potentially destroy the entire business. Most small business fall prey to ransomware. Experts in the information security field estimate that small businesses account for more than 60% of all malware attacks.

On average small business lost over $100,000 dollars within 25 hours of being infect of the ransomware. To prevent all of these attacks many businesses now invest in security to protect their business from further attacks. Many of these attacks are carried out because of the end user. A Microsoft employee, Dandelion, said that weakness link to malware infection is human stupidity that lead to many successful social engineering attacks. Many business now take action to stress to their employees to practice good security habits through education and reminders to prevent further attacks. A lot of this includes reading emails carefully and report any suspicious email to the higher ups in your business. Small and large businesses install the latest versions of anti-malware software will help prevent any current mainstream malware attacks. With all that said, malware will always be ahead in the game and business will always have to play catch up in order to protect their business and of their assets.

3. How malware actually infects people/businesses [more technical than 2, Pegasus](corp / end-user) For the particular area you identify, provide an in-depth technical description of how an attacker may use/capitalize on end-user’s folly.
    a. How they got the malware? (OMAR)
        1.

Malwares are easy to get if the user is not careful. There are many ways to get malware, such as, emails, unsecure website, unknown links, applications, and attackers. The first thing that makes it easy for the user to get malware is not having a good security system. Security systems can help the user to not get malware and keep the system safe. It can detect malwares in the user’s system and fight them. Also, visiting unreliable websites can get you infected. Websites can be full of viruses that can harm your device and get malwares all over the system.
If the user wants to download any program, the user should download it from the official website. Some websites might tell you that you can download the program from here, but instead you get infected by malware and viruses. Moreover, suspicious email is one of the easiest ways to get infected by malware. A lot of people get emails from unknown resource and it gets them infected easily. The email can say anything just to make sure that you click anything to get infected by malware. Links are also one of the ways the user can get infected by malware. Some links could have viruses and they get the user infected as soon as the user click it. Links are easy to spread through the social media, the user can get them in twitter, facebook, or whatsapp. So users should not click in any link before making sure that they know the source of it. Downloading applications could get the user infected by malware. Some applications have malwares on them, and as soon as the user download them, they get infected. Lastly, attackers also one of the ways to get malware. Some attackers can get the user infected using any of the ways I mentioned.

4. How businesses defend against malware (current approaches to this problem)

    a. Existing measures against malware (JIBRIL)

5. Why these measures are ineffective
    a. End user awareness (RAOUL)

6. Our innovative solution to prevent users from being affected
    a. Identify a “gap” within this existing measures (The “gap”: Now tell us about the “GAP” that exists even after all the current approaches have been taken into account. In other words, you would be making statements such as “despite all the current progress and the existing efforts listed above, there is still [this gap that exists…] and we wish to fill this gap by [coming up with this new approach/idea]…”) (GROUP)
    b. Provide an innovative approach that fills the gap you identify (GROUP)

By the way I put together a quick template presentation on prezi. I think this would be easier to make rather than using Wix. We still need to ask our teacher if this is ok but I think it should work. https://prezi.com/p/42z7mlyodhye/

1. AHMED

    What does the attacker get from the user?

    Attackers usually use malware to get important data, financial data and personal information. Attackers might use malware against the government and organizations to get guarded information and use it for their benefits. Some can get money from the attack, some can get secret information and some can get fame as a hacker, not all attackers want the same thing. Attackers can get every personal information that the user have in the device. They can get pictures and videos that the user does not want anyone to see and use it to blackmail. They can access the user’s social media information, and this happens a lot to celebrities. We always see celebrities say something on social media that they should not say, and days later, we find out that the account was hacked and the hackers was controlling it. Moreover, attackers can get credit card information, and take a lot of money. For example, in 2007, Max Ray Butler who was called Iceman was a prolific hacker. According to VPNmentor, Butler was arrested for stealing over 2 million credit card which he was using to purchase what worth $86 million. Attackers might use malware to get very important data from big companies, and ask for money to give the data back.