An Introduction to Malware

Before discussing why malware matters, we need to know what it is. Malware is a software that intends to damage the system that you are using by stealing the data you have on your device, or harming you in some other way. Another symptom of malware is that it could make your system slow and inefficient. Malware can sometimes be described as spyware, a virus, or even have its own name like “Pegasus”. The website known as Radware states that the first malware, known specifically as “The creeper”, was discovered in 1971. The creeper displays a screen daring you to capture the creeper, but it caused no harm. Hackers have continued to develop malware over to become more harmful. Malware is used nowadays to damage users’ systems and to steal data.

As mentioned, one example of a malware is Pegasus. The spyware was first found in August 2016. Pegasus got exposed after an attack that failed against a human rights defender. After investigating it, some details about the spyware was revealed. The spyware is capable of reading the text messages on a phone, tracing the phone, stealing passwords, stealing call data, and stealing general information from many other applications that are installed on the phone. In many cases it is very difficult to detect ample amount of malware on the web. Malware can impact everyday users and massive businesses as well.

Why Malware Matters

Impact on Everyday Users

An important first step for end users to stay safe is to realize why knowing about malware is important. 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. Most users 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 6th, 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.

Impact on Business

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, and fast, in order to stop the devastating destruction malware has on businesses.

E-Business has been very important in the 21st 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, which 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 loss for a business with its 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. Fortunately, 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 infected by 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.

Current Approaches to this Problem

(start here..)

1. How businesses defend against malware (current approaches to this problem)
    a. Existing measures against malware (JIBRIL)

The Gap

While existing measure to prevent malware exist, creating end user awareness is one of the most difficult tasks that businesses can have. Employees often just expect everything to work and don't treat the threat of malware as seriously as they should. This can stem from the fact that employees often want to focus on their own specific tasks and expect network security responsibilities to fall into the hands of IT professionals. The reality is that IT professionals can often only do so much due to the nature of the internet, and end users as a whole need to take some responsibility to reduce threats.

Creating awareness around a subject is another way of saying educating. End users, in this case, need to be be educated on what malware is and what threats they pose. Studies show

people learn more efficiently when they are involved in the teaching process. Though end users would rather focus on their own responsibilities rather than focus on “computer stuff”, it’s important for them to set some time to the side to learn about malware without IT staff being overbearing. The level of involvement and engagement in this case can be a little difficult to gauge. End users can not be expected to take a full course on information security, but their involvement should be more than just reading an e-mail sent out by the CIO. The more money and time spent on creating end user awareness, the more prepared and knowledgeable the end user will be. A middle ground can be found in dedicating a day of training.

Rather than asking employees to read a paper like this one on end user awareness on malware, which they may or may not do, the IT staff can set up a day focusing on the topics of: How people get affected, how malware affects people and businesses, what malware actually does after it infects a host, how businesses defend against malware, and how these measure are sometimes ineffective. One of the reasons these measures are actually ineffective is because of unaware end users, and these training modules will hopefully remind them of the part they play in the grand scheme of information security in a memorable way.

One of the biggest tasks of IT professionals running these training modules is convincing the end users that malware threats are real. Often people live in the bubble of, “it won’t happen to me”, but time and time again, even the biggest and seemingly most untouchable companies are attacked due to low end user awareness. Training on end user awareness of malware needs to make the threat of malware feel more personal rather than something to be handled by the IT staff. Perhaps even a controlled demonstration of malware being sent out to ends users will be effective in showing end users what not to do.

While not all seeing, IT staff often do have some degree of control on what employees can see and click on. If an employee is caught clicking on a suspicious link through an e-mail or their browser and downloads malware which is hopefully immediately quarantined by an antivirus, IT staff can kindly explain to the end user the specific nature of the malware, why they might have been targeted, and what damage the malware might have caused. Even with a day of training, it’s likely that employees will still make mistakes from time to time. This is why there is also some responsibility on the IT staff to be open to continually communicating with their team. The educating process can not end after a single training day. This type of engagement will once again push users back into their bubble of “it won’t happen to me.” IT staff can keep in touch with their employees to ask if, for example, they have seen anything suspicious. This involvement will make end users more likely to speak up rather than leave them in a state of, “I’ll remind them when I have time”.

Pegasus specifically is a dangerous malware because it provides full access to a phone. As dangerous as Pegasus was, being infected by it was pretty preventable in the way most malware is also preventable. Pegasus was a case of trying not to click on the wrong thing and making sure patches were downloaded promptly to prevent infection. This sort of malware could pose a great threat to a business that provides company phones, and training provided by companies to their end users could use Pegasus as an example of how such a preventable mistake could cause so much damage to a business.