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 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.

Sources

https://en.wikipedia.org/wiki/Ransomware

https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

https://www.lifewire.com/what-is-a-boot-sector-2625815

https://en.wikipedia.org/wiki/Michelangelo_(computer_virus)

http://searchsecurity.techtarget.com/definition/spyware

http://whatis.techtarget.com/definition/Top-10-Spyware-Threats