**Introduction**

Ransomware is a type of malware that locks users out of their mobile devices in a pay to unlock your device ploy. It is different from the typical malware which purpose to gain sensitive information and send out to the attacker. Obviously, the traditional security and antivirus applications cannot detect and remove ransomware.

Nowadays, Information Technology (IT) Industry influences many organizations to move towards digitalization. Tremendous amount of personal and unique information is stored in online database, cloud and even personal computer. Nevertheless, the concentration of individual and significant data in devices with poor or weak security configurations has made these platforms main targets for specific attacks with threats designed to secretly gather information or financially extort victims, the so-called ransomware.

Ransomware is best described as a scareware which cybercriminals use the ransomware to block the users from accessing their data files and hastily prompt them to pay the ransom in order to gain back their access. This high profit and undetectable business model become main reasons for criminal organizations that orchestrate the attacks. Payment is often via Bitcoin, with the ransom amount is in the range of 500-1000 USD. However, the set price is increasing as time goes on, making it look wiser to pay immediately. C. Everett in his paper estimated that almost 200 million USD per year is extorted illegally by the criminal organizations. Advice is often given not to pay the ransom, as this prolongs the criminal business model, however it may be the only way to recover lost data.

Considering the world economic growth, it is decided that the diversity and complexity of ransomware have been increased significantly. For instances, CryptoLocker, CryptoWall, TeslaCrypt and Locky are well known ransomware. In May 2017, WannaCry ransomware massively attack hospitals, companies and government offices around the world, seizing control of affected computers until the victims pay a ransom. Sixteen National Health Service (NHS) organizations in the UK have been hit, and some of those hospitals have cancelled outpatient appointments and told people to avoid emergency departments if possible. Media also reported that digital payment systems at PetroChina gas stations were offline, forcing customers to pay cash. The ransomware is spread by taking advantage of a Windows vulnerability that Microsoft (MSFT, Tech30) released a security patch for in March. But computers and networks that hadn't updated their systems were still at risk.

**Conclusion**

In conclusion ransomware attacks, has proved that its effects can be devastating to small business owners and organizations. Ransomware is not only a threat to small businesses and organizations it has an impact on people too. Ransomware is fierce, smart and dangerous. As we continue to watch its evolution unfold and numerous users becoming victims of its extorting ways, we see more and more lethal functionality. Ransomware now employs the use of rootkit technology and even modifies the user’s ability to boot in safe mode. The way to avoid damage from ransomware infections is to maintain regular up-to-date backups, use the an anti-virus and keep it up to date, keep your operating system and software up to date with patches and lastly review the access control settings on any network share that we have that stops malware seeing and stealing them.