**Ransomware**

Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack.  Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity isn't known. Ransomware malware can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites There are number of ways, ransomware can gain access to victims computer, one of the most common ways is through email phishing, where spam mails are sent masquerading as an attachment that the victoms should trust. Once, those attachments are downloaded and opened, the attackers get access to victom’s system and if those attachments have some inbuilt social engineering tools, then those attackers can get administrative access to the system as well. There are several things that the malware can do, once it has taken victim’s computer access,but most common action is to encrypt the victim’s entire data or some of the user’s file. But at the end of the process, the data cannot be decrypted without the help of the mathematical key which known only by the attacker. The user is notified with the message that their data is now inaccessible by them and only will be decrypted if the victim sent a desirable untraceable bitcoin payment to the attacker. In some forms of malware the attacker might claim to be a law enforcement agency shutting down the victim’s computer due to presence of pornography or some pirated software on it, so that the victims wont be able to report the attack to the authorities.There is also a variation called leakware or doxware which goes further and releases the copy of victim’s private documents such as photos,videos,emails etc on the hard drive to public if you don’t pay up. But because finding and extracting such information is very tricky for attackers, encryption ransomware is the most used common type for performing the attack.

**Who is the target for ransomware?**

There are several different ways, attackers chose the organization which should be suffered by ransomware. For instance, it is a matter of opportunity, for example, attackers might target university organization as they have less security implementations on their systems and also they tend to have smaller security teams. On the other hand some organizations are tempting target because they are more likely to pay the ransom demanded by the attackers more sooner. For example, government agencies or medical facilities often need immediate access to their files. But don’t feel safe if you do not fit in these categories as some ransomware spreads automatically and indiscriminately across the internet.

**Why bitcoin?**

Bitcoins are used by the ransomware attackers for hiding their identity as no centralized banks are involved in this process of transactions. Bitcoin is open-source as well as public, anyone across the world can use it, no one owns or controls bitcoin. As transactions are made with no banks in between, it is highly impossible to even try or fetch to get any credentials related to the ransomware attackers. All the bitcoin users have a specified address which is known only to the owner and then transactions are done only on the basis of that address.

**Should you pay the ransom**

When speaking theoretically, most law enforcement agencies urge you not to pay ransomware attackers, on the logic that doing so only encourages hackers to create more ransomware.

 That said, many organizations that find themselves afflicted by malware quickly stop thinking in terms of the "greater good" and start doing a cost benefit analysis , weighing the price of the ransom against the value of the encrypted data.  According to research from Trend Micro, while 66 percent of companies say they would never pay a ransom as a point of principle, in practice 65 percent actually do pay the ransom when they get hit. Ransomware attackers keep prices relatively low — usually between $700 and $1,300, an amount companies can usually afford to pay on short notice. Some particularly sophisticated malware will detect the country where the infected computer is running and adjust the ransom to match that nation's economy, demanding more from companies in rich countries and less from those in poor regions. There are often discounts offered for acting fast, so as to encourage victims to pay quickly before thinking too much about it

There are a couple of tricky things to remember here, keeping in mind that the people you're dealing with are, of course, criminals. First, what looks like ransomware may not have actually encrypted your data at all; make sure you aren't dealing with so-called "scareware" before you send any money to anybody. And second, paying the attackers doesn't guarantee that you'll get your files back. Sometimes the criminals just take the money and run, and may not have even built decryption functionality into the malware.

**Ransomware examples**

While ransomware has technically been around since the '90s, it's only in the past five years or so that it's really taken off, largely because of the availability of untraceable payment methods like Bitcoin.

* **TeslaCrypt**, which targeted gaming files.
* **SimpleLocker**, the first widespread ransomware attack that focused on mobile devices.
* **CryptoLocker**, a 2013 attack that launched the modern ransomware age and infected up to 500,000 machines at its height
* [**WannaCry**](https://www.csoonline.com/article/3227906/ransomware/wannacry-ransomware-explained-what-it-is-how-it-infects-and-who-was-responsible.html), which spread autonomously from computer to computer using EternalBlue, an exploit developed by the NSA and then stolen by hackers

And this list is just going to get longer.