All You Need to Know About the Wannacry Ransomware

The nature of crimes, its sources and reach have undergone a huge change within past 30 years with cyber -crime now occupying one of the top spots. According to global security strategists, there are half a million attack attempts that are happening on the cyber space every minute. The Internet of Things, thus presents huge opportunities for hackers in the current scenario.

The digital world was the witness of one such cyber-attack this May, when Wannacry Ransomware found its way into the systems of leading organizations and encrypted all the files and documents, thus preventing the users to access them.

For your reference, Ransomware is any kind of software that infects the system, blocking victim's data and threatening to delete it until a ransom is paid. On 12th of May 2017, the victims across the globe saw the following message displayed on the screens of their monitors

The display of the PC gets turned to "Oops, your important files have been encrypted," and a message pops up in the bottom-right stating facts about the hack. A document also is available with information about what has happened, the Bitcoin wallet that one should send payment to,

and how to make decryption work. Also, the timer starts and if the payment is not made within the given time, the ransom is increased to twice the initial value, if one fails to make the payment even after this warning, then the threat of loss of all the files is realized.

Here are Some Must Know Facts about Wannacry

- Within a day, more than 230,000 computers were hacked in over 150 countries.
- It can easily affect Windows Vista,7,8,10, XP and various versions of the Windows Software. However, MacOS/Mac OS X or Linux remains unaffected.
- It demands a payment in Bitcoins, it is a digital currency in which payment takes place directly between the parties without any intermediary. It is not controlled by banks or any Institution.
- This attack can reach you through any compromised emails or websites, though it is also believed that it may be a computer worm spreading without any human assistance.
- Though a kill switch was discovered that stops the spread of Ransomware, but it could hardly create any impact as the newer versions of attack were launched that corrected this flaw.

Advice from the Experts

Though awareness is the pride of the achiever, but is of no good if not utilized effectively. The major question that still lingers is what should be the necessary steps taken against the attack of such a ransomware?

The leading experts of the industry advice against the payment of the Ransom amount. One may question, that what about the loss of data and files then?

"If you pay, you'll enter a sort of blacklist of people who pay and can be targeted again," said Moty Cristal, a leading Professional Negotiator, "The thought process is that once you pay, you'll always pay."

The first step could be reaching out the Cyber- Security cells and filing a complaint. Various flaws and loopholes if detected can act as a savior against the attack. It is thus advisable to follow the instructions and guidance of the Cyber security police.

You are the key to your safety, protect yourself!