Ransomware Analysis and Solution to its attacks

RENJITH ROY
IMCA-253

INTRODUCTION

A ransomware is basically a malware that is installed on a personal or office computer without the user's knowledge which encrypts all the data present in the system, completely blocking off the user's access to it.

The data stays encrypted until the victim pays a ransom fee to the attacker usually in a cryptocurrency such as Bitcoin due to its anonymity.

Phishing emails that contain malicious attachments, embedding malicious JavaScript code in SVG files and minor software or operating system flaws are some of the common delivery agents of such malware.

The targets include individuals, companies and even government sectors.

EVOLUTION OF RANSOMWARE

Ransomware has evolved from being just a computer virus present on a floppy disk in the year 1989 to its most advanced form today, which uses the latest encryption standards to completely encrypt the user data.

The next major breakthrough happened when the first locker ransomware emerged in the year 2007. This version targeted Russian users by locking their computers.

From 2007, when the first locker ransomware appeared to the current date, locker ransomwares are still widely used by hackers.

CryptoLocker, CryptoWall, Locky, and TeslaCrypt are some the most advanced ransomware till date.