

Ransomware

Ransomware is a type of malware software, that aims at encrypting the users important files and folders that are store in computer and then demand ransom amount in exchange of data. It makes victim pay and this totally depend upon the types of virus. Like some malicious ransomware virus claims to make payment in order to avoid the punishment of Government authority (local agency or FBI). While some virus says that this is a way to get decryption code for encrypting the data. Some virus also terminate legitimate software and steal users important information and causes many likewise unwanted activities to disturb user.

Types of ransomware malware:

File-Encrypting Ransomware :- this gets spread with the help of Trojans and once it infiltrate the computer then it start encrypting the most important and used files to create problem for user. It includes music, video, picture, text, document, audio files for encryption. And then it display warning message that claims the only way t decrypt the data is to pay the ransom as directed. Some powerful malware also tends to delete the shadow copy of file in order to prevent the recovery.

Non-Encrypting Ransomware :- it blocks entire computer and then threatens the users to pay imaginary fine. For that it presents itself as the government authority warning message and mostly it uses the name of FBI, police and others. It infects the computer and then check for illegal files like unlicensed program versions or pornographic content on computer. Once it gets detected then it blocks computer and then display huge warning just like some government authority. And it inform user that some illegal files have been detected in users computer and for this user would have to pay fine in order to avoid going to jail.

Ransomware-as-a-service (RaaS) :- this one of main cause why crypto-malware business is grooming so fast all over the World. Those who have less programming skills and want to earn money easily contacts the ransomware developers through darknet and gets engaged in the distribution campaign. After they get access to malware configuration the criminal spread it all over the World through network.

Browser Locking ransomware :- it does not infect computer system but gives JavaScript in browser and then block the browser with lots of dangerous warning.

The distribution methods of Ransomware Malware

Spam Emails

Fake pop-up notification

Trojan Horse and other malware

Browser Extension

After exploiting the kit

Removal Steps

Automatic Removal:

It would be wise to opt professional anti-malware program it does complete scanning of computer as such it comprises of advanced and powerful algorithm. In case your computer has got infected with ransomware parasite then removal of such potential unwanted software can be done with automatic removal tool.

Manual Removal:

Since ransomware does encrypt the files with powerful algorithm and it is not wise to go for manual removal steps.