Ransomware Decryptors

Full Disk Encryption

Full Disk Encryption

Ransomware variants like THT, Mamba, or MCrypt use native or opensource encryption software to encrypt the entire hard drive of the system. Once the TA gains access to the system with administrator privileges, the TA will use a tool like Bestcrypt, DiskCryptor or even Windows Bitlocker to encrypt the full disk. Once encryption is complete, the system reboots and the victims are locked out.

Communication preference: Email usually protonmail, firemail.cc, or cock.li domains

Average ransom payment: $36,000 - $55,000

Preferred currency: Bitcoin (BTC)

Decryptor received: 100% of the time. TA will provide passwords per system for access

Watch out: MCrypt will hold volumes hostage and “re-extort” victims into making multiple payments. During the initial negotiation, the TA will not indicate multiple drives are encrypted. Instead they will negotiate a single amount for initial access to the Operating System; essentially allowing access into Windows. Once access to Windows is regained, victims often surprised to find their “data” partitions are encrypted causing the victim to return to the negotiation table to once again shell out more money to unlock their information.

Notes: After gaining access, the open source encryption tool still needs to be removed otherwise after reboot, the data storage will be locked again.