Ransomware

Intruders may design ransomwares and release them via the Internet to extort money. If a user computer is unknowingly injected with this software, all files of specific formats, such as documents, spreadsheets and digital photos, stored on the computer or the intranet will be encrypted. The intruder will then demand a ransom from the user. Unless the user pays the intruder to purchase the corresponding decryption program and decryption key, he will not be able to open the encrypted files.

Causes of Infection

Usually, the user computer can be unknowingly injected with ransomware when the user:

- browses dubious websites;
- installs or opens files or software of unknown origin;
- opens emails of unknown origin and their attachments.

Security Measures

Since ransomware is quite a complicated malware, we must apply basic security measures to protect our computers against ransomware. This includes installing anti-malicious code software like anti-virus software, installing firewalls and the latest security patches, conducting full system scan at least once a week and activating the auto-update function of the relevant software.

Backup important files regularly. Increase backup frequency if necessary to ensure the most updated data are protected. Be vigilant to Internet security. Never download and install software from unknown websites.

Avoid browsing suspicious websites, for example, online game, online gambling or social networking websites provided in the hyperlinks of spam emails.

Apart from applying basic security measures, an incident response arrangement should also be put in place. In case of a ransomware attack, the user can follow the procedures imperturbably and take appropriate actions.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk