Rançongiciel

Depuis quelques années, des attaques se propagent à l'aide de rançongiciels. Les programmes usités par les pirates sont particulièrement efficaces et bloquent totalement les ordinateurs des victimes.
Cette attaque est accompagnée d'une demande de rançon au propriétaire de l'ordinateur, contre le déblocage du code malveillant.
Il ne faut pas payer cette rançon car, de toute façon, le pirate ne vous enverra jamais de solution palliative à ce problème. La seule possibilité est souvent une réinstallation complète du système d'exploitation.

RANCONGICIEL*(ransomware) : C'est un programme malveillant qui s'installe sur un ordinateur et bloque l'accès aux données et au système d'exploitation. Le propriétaire ne peut plus utiliser son ordinateur, même après un redémarrage.*

Explications :
Ce type d'attaque particulièrement sophistiquée relève d'une escroquerie du crime organisé, principalement, venant des pays de l'est. Le rançongiciel est un faux avertissement d'une autorité gouvernementale (gendarmerie, police, hadopi), signalant que l'ordinateur infecté serait utilisé à des fins illégales par son propriétaire (réseaux peer to peer, films pornographiques, copies de logiciels etc.). Le but ultime des pirates étant de faire payer une forte rançon à la victime mis sous pression par de telles accusations.

Le modus opérandi