Forum: Sécurité

Topic: Malware MosaicLoader

Subject: Malware MosaicLoader

Publié par: Lotesdelere

Contribution le : 23/07/2021 13:02:05

MosaicLoader est un malware qui infecte le plus souvent le programme d'installation des logiciels piratés et pour a pour caractéristique de neutraliser Windows Defender en priorité de façon à pouvoir ensuite télécharger et installer d'autres saletés en toute impunité.

Pour neutraliser Windows Defender le malware utilise les listes d'exclusions, il faut donc vérifier que les clés du registre suivantes n'aient pas été altérées:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows DefenderExclusionsPaths

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows DefenderExclusionsExtensions

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows DefenderExclusionsProcesses

On ne soulignera jamais assez également l'utilité d'un bon firewall pour empêcher les téléchargements non désirés.

Source (en anglais): https://thehackernews.com/2021/07/this ... e-hides-itself-among.html

Article en français:
https://www.phonandroid.com/ce-malware ... par-windows-defender.html