

MacRansom, le premier RaaS dédié aux machines macOS

Un temps épargnés par les grandes vagues de malwares touchant les PC Windows, les **Mac d'Apple** sont maintenant ciblés par les cybercriminels. Et pour cause, puisque macOS devient de plus en plus populaire. Sur les trente derniers jours, StatCounter estime que **18,2 %** des internautes français utilisent macOS. Contre 78,1 % sous Windows ([source](#)).

Une nouvelle vague de malwares débarque sur macOS, alertent les experts en sécurité. Une déferlante comprenant **des ransomwares chiffreurs**. Des outils cryptant les données de l'utilisateur, puis demandant une rançon pour les déverrouiller. Certes, la présence d'un système de sauvegarde efficace et simple d'emploi (Time Machine) permettra de retrouver la plupart de ses données. Mais le risque reste élevé.

Un RaaS pour macOS

Et il devrait s'amplifier avec l'arrivée de l'offre **MacRansom**, [découverte](#) par Fortinet sur le DarkNet. Une solution de **Ransomware as a Service (RaaS)** qui devrait attirer les pirates en herbe, script kiddies et autres pieds nickelés de la cybercriminalité.

Livré sous la forme de RaaS, cet outil est accessible gratuitement, ses auteurs se rémunérant sur un pourcentage des sommes décrochées par les apprentis pirates. Étudié par Fortinet, le malware en question dispose d'un déclencheur programmé, afin de passer sous le radar des antivirus (en restant inactif avant la date fixée par le cybercriminel). Et il chiffre effectivement les données. Après quoi il demande une rançon de 0,25 bitcoin. **Soit environ 700 dollars.**

Si la technicité de ce malware reste limitée face aux offres Windows, les dégâts qu'il pourra occasionner sont bien réels. Méfiance donc.

À lire aussi :

[macOS 10.13 High Sierra, iOS 11, watchOS 4 : les nouveaux OS d'Apple](#)

[McAfee note une explosion du nombre de malwares sous macOS](#)

[Apple livre l'APFS sous iOS et Night Shift sous macOS](#)