Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

	Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

Windows 10 lance automatiquement ses mises à jour, ainsi que tous les utilisateurs que ça importunent le savent. Une bonne opportunité pour les cybercriminels de sévir tranquillement.

C’est ainsi qu’un nouveau ransomware a été découvert par un analyste de chez AVG Technologies.
Un premier exécutable maquille ses propriétés afin de faire croire qu’il provient de Microsoft et qu’il s’agit d’une mise à jour critique.

Une fois ce malware installé, il en télécharge un autre dans le répertoire AppDataLocalTemp, sous le nom WindowsUpdate.exe. Puis il l’exécute.
Pour l’utilisateur, c’est une mise à jour qui s’est déclenchée, tant l’écran de cette seconde partie du malware est bien faite, avec les polices de Microsoft bien imitées.

L’utilisateur n’est pas surpris de voir que son disque dur tourne, tourne… Une ‘expérience utilisateur’ qu’il doit régulièrement supporter…
Sauf que là, le disque tourne parce que le malware en crypte toutes les données. Le méfait accomplit, un autre écran apparaît, moins habituel, avec une invitation à contacter les cybercriminels par mail, pour finalement devoir payer une rançon afin de récupérer les données.
Utilisateurs de Windows 10, la prochaine fois que vous verrez un écran de mise à jour, croisez les doigts !

Article original de fredericmazue

Denis JACOPINI vous recommande le logiciel de sécurité suivant :

Réagissez à cet article

Original de l’article mis en page : Fantom : un nouveau ransomware qui sévit sous Windows 10 | Programmez!