

# WannaCry : du code nord-coréen... dans un malware américain

Neel Mehta, expert en sécurité chez Google, a retrouvé dans le code de **WannaCry** des similarités avec du code créé par le **Lazarus Group**. Une équipe de pirates nord-coréens. Un lien confirmé par les équipes de Symantec et de Kaspersky Lab.

*« Nous n'avons pas encore été en mesure de confirmer que les outils Lazarus ont déployé WannaCry, a déclaré un porte-parole de Symantec dans un communiqué transmis à CNNTech. Bien que ces connexions existent, elles représentent jusqu'à présent seulement **un lien faible**. Nous continuons à rechercher des connexions plus solides. »*

La prudence reste donc de mise, même si certains ont rapidement conclu que l'affaire WannaCry était l'œuvre du Lazarus Group, qui avait déjà piraté Sony Pictures. Et que cette attaque était donc pilotée par la Corée du Nord.

## Vrai coupable, ou diversion ?

Pour le moment, rien ne permet d'incriminer la Corée du Nord. Du moins pas plus que les États-Unis. Rappelons en effet que ce contre-feu arrivé fort à propos ne doit pas faire oublier le fait que ce malware faisait partie **de la boîte à outils de la NSA**. Un organisme 100 % américain, et à priori sans connexion avec le gouvernement nord-coréen.

Le président russe **Valdimir Poutine** a pour sa part nié toute implication de son gouvernement dans cette attaque, [ironisant](#) sur le fait que cet outil, créé par les services secrets américains, se retourne aujourd'hui contre son créateur.

### À lire aussi :

[La parade n'existe pas pour contrer les futures affaires WannaCry](#)

[WannaCry 2.0 : Renault n'est pas la seule entreprise touchée en France](#)

[WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA](#)