15 jan 2021 -09:25

# Le Centre pour la Cybersécurité Belgique tire les leçons d’une cyberattaque visant les agences gouvernementales américaines, l’affaire SolarWinds

Le Centre pour la Cybersécurité Belgique  a organisé hier son événement Quarterly Cyber Threat Report (QCTR).  Un événement trimestriel où des experts discutent des principales cybermenaces du moment.  L'édition en ligne a intéressé 1300 personnes, de plus de 50 pays différents. C'est un record et un cas unique en Belgique. Il n'est donc pas surprenant que l'affaire SolarWinds soit au programme. Au moment de sa découverte, cette attaque contre les agences gouvernementales américaines a éclipsé tout le reste de l’actualité aux États-Unis et fait encore aujourd'hui l'objet d'une enquête.

## SolarWinds ?

Pour ceux qui ont manqué l’épisode : en décembre 2020, plusieurs agences gouvernementales américaines ont été victimes d'une cyberattaque via la plateforme Orion, un logiciel de SolarWinds. Le produit qui a été compromis est un logiciel permettant de gérer les systèmes à distance. Au total, 18 000 organisations dans le monde ont installé la mise à jour malveillante et de nombreux systèmes ont communiqué avec un serveur de *command and control* géré par les hackers. Plusieurs organisations ont confirmé que ceux-ci avaient pris des mesures supplémentaires sur leur réseau. Il s'agit principalement d'importants départements fédéraux américains tels que le US Treasury Department, la National Telecommunications and Information Administration (NTIA) et les National Institutes of Health (NIH).

Il s’agissait d’une attaque complexe et de grande ampleur.

### Les services publics et entreprises belges sont-ils en danger ?

Ce logiciel est utilisé partout dans le monde, y compris en Belgique. En décembre, Microsoft a pu détecter 40 clients, dont un en Belgique. Le CCB ne connaît pas tous les clients belges et n'a pas encore reçu de signalement d'une victime belge. Toutefois, il est toujours important de surveiller cette menace, de tracer les victimes potentielles et de leur apporter une aide supplémentaire.

### Quelles actions le CCB a-t-il entreprises ?

Dès le début, le CCB a pris cette menace au sérieux.

"Nous sommes constamment en stand-by pour répondre aux questions des victimes potentielles. Le 18/12, nous avons publié un avis technique. Nous avons eu des réunions avec plusieurs centres d'analyse et de partage d'informations (« Information Sharing and Analysis Centres »,ISAC). Les rapports ont été publiés et partagés avec les partenaires par le biais du système d'alerte précoce (« Early Warning System », EWS). Et nous avons organisé un QCTR où des experts de FireEye et Kaspersky notamment ont présenté leurs conclusions pour que l'on puisse en tirer des leçons pour l'avenir."

Miguel De Bruycker
Directeur du Centre de Cybersécurité Belgique

## Et qui est à la source de l’attaque ?

La presse américaine a immédiatement pointé du doigt les hackers d'État russes. Cependant, il est très difficile de connaître la source d'une cyberattaque. À ce jour, nous n'avons aucune certitude quant aux personnes qui ont orchestré l’attaque.

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be