

Centreon se défend d'être le SolarWinds français

Centreon, un « SolarWinds *bis* » ? Le premier est français ; le second, américain. L'un et l'autre éditent une plate-forme logicielle de supervision informatique. Ils se trouvent aujourd'hui face à la même problématique : leur produit a servi de support à des activités cybercriminelles.

L'[affaire](#) SolarWinds avait éclaté en décembre dernier. Au fil des semaines, le voile s'est levé sur une campagne d'espionnage XXL ciblant essentiellement les États-Unis. Principal vecteur de l'opération : des mises à jour vérolées d'Orion, la plate-forme logicielle de SolarWinds. Elles contenaient une *backdoor*.

Un rapport de l'ANSSI évoque Centreon

L'alerte relative à Centreon est plus récente. Elle découle d'un rapport que l'ANSSI a publié le 15 février. Il [y est question](#) d'une campagne malveillante qui aurait touché la France entre 2017 et 2020. Le levier : des serveurs exécutant la plate-forme logicielle de Centreon.

L'entreprise avait d'abord apporté des clarifications par voie de presse. Dans les grandes lignes, elle affirmait que ses clients n'étaient pas affectés. L'attaque aurait en l'occurrence reposé sur l'édition *open source* de son logiciel, additionnée d'une « modification sauvage ». Plus précisément, un « module [...] développé par un opérateur tiers » et qui vient agir sur une ligne de code « absente des solutions Centreon depuis 2015 ».

Le [communiqué](#) publié par la suite arrondit les angles, mais le fond des propos demeure. Centreon y adjoint une estimation : une quinzaine d'entités ont été ciblées. Toutes exploitaient une version obsolète du logiciel : la 2.5.2, dont la prise en charge est arrivée à terme voilà plus de cinq ans. Son déploiement dans les entités concernées s'est fait, nous explique-t-on, « sans respect de sécurisation des serveurs et des réseaux, notamment des connexions vers l'extérieur ».

Ce démenti a d'autant plus d'importance que le rapport de l'ANSSI suggère des liens avec Sandworm. Un groupe cybercriminel que le gouvernement américain a lié au renseignement militaire russe.

Photo d'illustration © Rawpixel via Adobe Stock