Ransomware : l'épisode Maze était-il prévisible chez Cognizant ?

Une nouvelle victime de marque pour Maze.

Cette fois, le *ransomware* a touché Cognizant.

Le groupe IT américain aux 17 milliards de dollars de chiffre d'affaires l'a confirmé samedi 18 avril 2020. Il a transmis à ses clients une liste d'indicateurs de compromis (IOC) pour les aider à protéger leurs propres systèmes.

Ces IOC comprennent des adresses IP de serveurs et des hashs de fichiers exploités dans de précédents incidents impliquant Maze. Il en circule déjà un grand nombre, la première campagne fondée sur le *ransomware* ayant été détectée il y a près de six mois.

Selon les chercheurs à l'origine du service d'identification de rançongiciels ID Ransomware, l'attaque contre Cognizant n'a rien d'une surprise.

Début février, ils avaient laissé entendre à l'entreprise qu'au moins un de ses collaborateurs avait été victime de *phishing*. Et l'avaient invitée à se renseigner sur la base I Got Phished*.

> *If I remember what we seen/heard/etc about Cognizant, this, if true, not comes as a big surprise...*
> *cc @VK_Intel pic.twitter.com/qr3WuXzdT3*
>
> *— MalwareHunterTeam (@malwrhunterteam) April 18, 2020*

Leur tweet à ce propos (ci-dessus) fait référence à Vitali Kremez. L'intéressé, qui travaille chez Intel, vient de publier une règle YARA destinée à détecter une DLL que Maze a visiblement utilisée pour infecter Cognizant.

> *High alert related to the yet another ransomware attack perpetrated by the Maze group possibly affecting @Cognizant.*
>
> *Reviewing & mitigating against the usual Maze TTPs (including RDP + remote services as an attack vector) is advisable.*
>
> *Pushed #YARA https://t.co/qcUY464fSf pic.twitter.com/z2zHL5apkm*
>
> *— Vitali Kremez (@VK_Intel) April 18, 2020*

** I Got Phished avertit les administrateurs de domaines, par opposition à Have I Been Pwned, qui alerte les individus sur la base de leur e-mail.*

Photo d'illustration © Yu. Samoilov via *Visualhunt / CC BY*