Ransomware : les 3 infos sur l'attaque contre Bouygues Construction

Ironie du calendrier. Alors que le FIC 202O, grand raout de la cybersécurité, fermait ses portes, les serveurs de Bouygues Construction faisait l'objet d'une attaque de type ransomware (rançongiciel) le 30 janvier.
L'information a été officiellement confirmée le lendemain : « Par mesure de précaution, les systèmes d'information ont été arrêtés afin d'éviter toute propagation. » précise le groupe de BTP.

> *Le réseau informatique de @Bouygues_C a été victime d'un acte de cybercriminalité. Tout est mis en œuvre pour un retour à la normale dès que possible. Nous sommes en lien étroit avec nos clients, nos partenaires et les autorités compétentes. https://t.co/3AsUWjpB3a*
>
> *— BouyguesConstruction (@Bouygues_C) January 31, 2020*

Quelle est la nature de l'attaque ?

Selon Zataz, le ransomware s'est propagé depuis les serveurs du groupe au Canada (situés à Toronto et à Vancouver) pour toucher l'ensemble de son sytème d'information.

Le site de référence sur la cybercriminalité affirme avoir identifié le groupe de hackers dénommé Maze comme étant à l'origine de l'attaque. Il s'est aussi fait confirmer une demande de rançon de 10 millions € contre les 200 Go de données dérobées.

Dans le dernier rapport de l'ANSSI « Etat de la menace rançongiciel » , Maze est le nom d'un ransomware distribué en tant que Ransomware-as-a-Service.
« Maze est opéré par au moins un groupe cybercriminel spécialisé dans le Big Game Hunting » indique le rapport. Le nom du groupe baptisé TA2101 est évoqué.

« Si Maze était initialement distribué au travers de sites piégés à l'aide d'exploit kit (Fallout EK, Spelevo EK) et aux couleurs de fausses plateformes d'échange de cryptomonnaie, de nouvelles campagnes d'attaques ont eu lieu à partir de fin octobre 2019 s'appuyant sur des courriels malveillants prétendument issus d'organismes étatiques italiens, allemands ou américains. »

La ville américaine de Pensacola, l'entreprise de sécurité Allied Universal et de Southwire ont également été victimes du même logiciel.

Quelles sont les menaces proférées contre Bouygues Construction ?

Maze menace de rendre publique les données en cas de refus de payer la rançon : « If they don't pay the full dump from their servers will be released to the public. and then they can be sure they will be ruined in lawsuits. »
Selon Darktrace, Maze est à l'origine de ce nouveau type de menace qui a été utilisé la semaine dernière contre la société britannique de transfert d'argent Travelex.

Quel est l'état du système d'information de Bouygues Construction ?

Le groupe affirme que » Les équipements sont progressivement remis en service après avoir été testés. » et que » L'activité opérationnelle des chantiers n'est pas perturbée à ce jour. »

Cependant, un article du Parisien (daté du 30 janvier) évoque des témoignages de salariés du siège social de Guyancourt (Yvelines) prévenus par SMS d'une coupure totale du SI : plus de messagerie, d'accès aux applications, à internet et à la VoIP.

Pour Zataz, qui cite des sources internes à Bouygues Construction, le retour à la normale ne devrait pas intervenir avant 4 à 6 semaines.

Des experts de Microsoft et McAfee sont dépêchés pour soutenir la reprise d'activé et le groupe indique être « en contact étroit avec les autorités compétentes. »
Son statut d'OIV (Opérateur d'importance Vitale) lui permet notamment de pouvoir recourir aux experts de l'ANSSI.

Le groupe de BTP annonce une nouvelle communication sur la situation « en début de semaine ».