Bouygues Construction : Maze est-il le plus dangereux des ransomware ?

Voilà bientôt une semaine que Bouygues Construction a annoncé avoir été victime d'une « attaque virale de type *ransomware* ».

Vendredi 31 janvier, le groupe français avait fait état de cet incident qu'il disait avoir détecté la veille. Il affirmait avoir mis son système d'information à l'arrêt pour éviter toute propagation.

Le dernier communiqué, daté du 5 février, ne va pas beaucoup plus loin. Message principal : la restauration du SI se poursuit, avec des mesures spécifiques pour assurer la continuité des activités. On n'en sait toutefois pas plus sur l'avancée des négociations autour de la rançon de 10 millions d'euros qui aurait été réclamée à Bouygues Construction.

À la même date, l'ANSSI a actualisé le rapport « État de la menace rançongiciel » qu'elle avait publié à l'occasion du FIC. Elle a enrichi l'annexe relative au *ransomware* qui a touché Bouygues Construction.

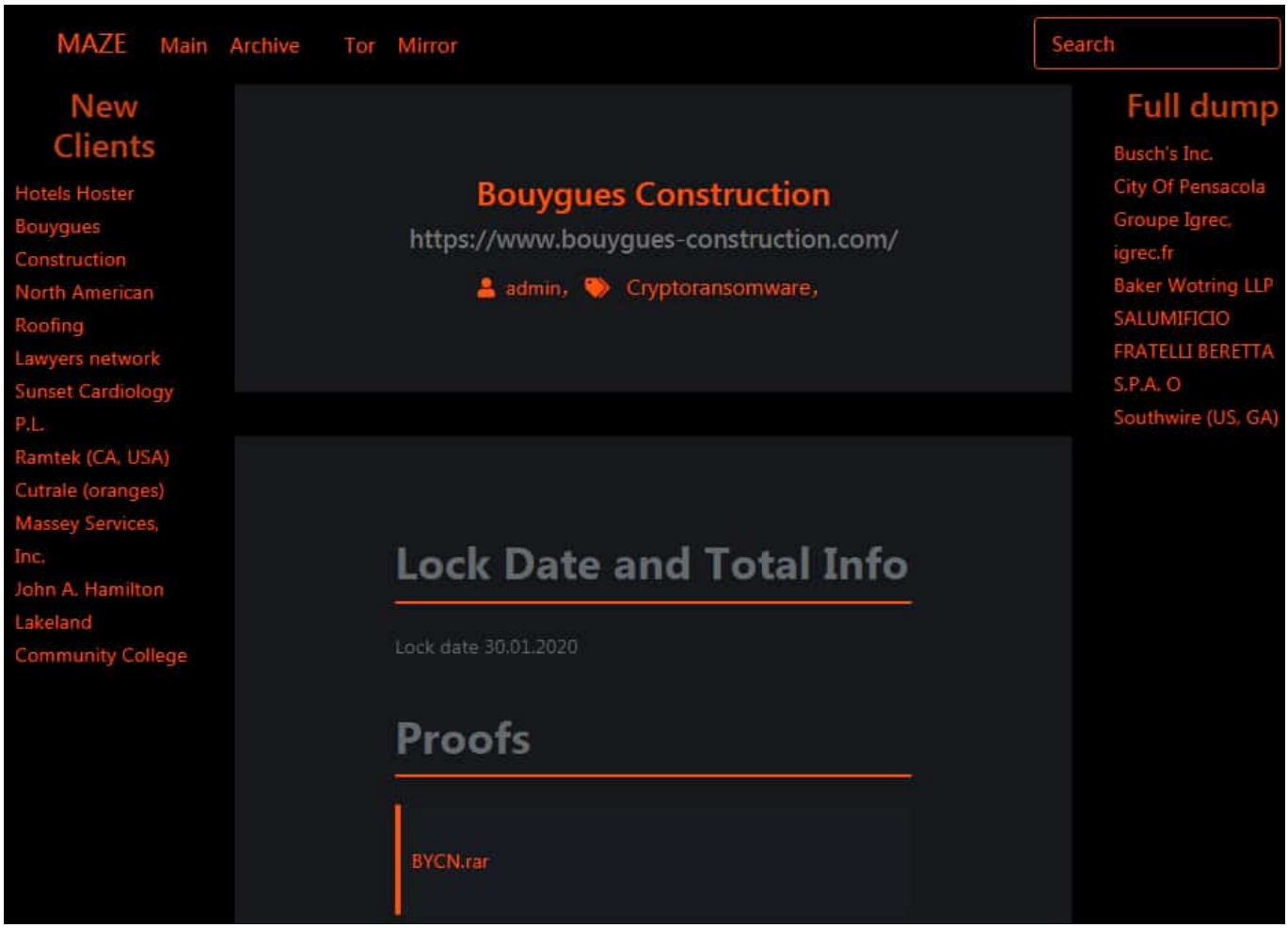
Ce *ransomware*, c'est Maze (variante de ChaCha, ainsi nommé car il utilise l'algorithme cryptographique ChaCha20). Un chercheur de Malwarebytes l'avait découvert en mai 2019*.

> *#FalloutEK dropping Maze ransomware.*
> *IOCs:*
> *– FalloutEK IP,45.76.149[.]204*
> *– Payload, e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684*
> *pic.twitter.com/wiELMUcTU0*
>
> *— Jérôme Segura (@jeromesegura) May 29, 2019*

Chantage au *ransomware*

À l'instar de Snatch, REvil/Sodikonobi ou Zeppelin, Maze est de ces rançongiciels qui ne chiffrent pas tout de suite les données. Ils les exfiltrent d'abord, engendrant un moyen de pression supplémentaire sur les victimes*.

L'un des groupes qui exploite Maze – Proofpoint l'identifie sous le nom de TA2101 – met cette technique en œuvre. Il publie, sur un site Internet mis en ligne à la mi-décembre, une partie des données dérobées aux organisations qui refusent de payer la rançon.



Maze a aussi la particularité d'adapter la somme demandée au profil de la victime.

Le fabricant de câbles américain Southwire, touché en décembre, s'est vu réclamer 850 bitcoins, soit environ 6 millions de dollars au cours d'alors. Allied Universal, frappé à la même époque, a été prié de verser l'équivalent de 2,3 millions de dollars.

« Ces forts montants, combinés au risque de divulgation de données internes, en font le rançongiciel ayant le plus fort impact potentiel sur les entreprises et institutions, résume l'ANSSI. *Celles-ci peuvent effectivement se retrouver à supporter l'impact de la divulgation de données clients* [...]*, mais également de données de recherche, commerciales ou encore classifiées.* »

Bouygues Construction figure sur le site Internet en question. Une archive de 1,2 Go est fournie en guise de preuve, mais elle est protégée par un mot de passe.

Une autre entreprise française (une PME spécialisée dans la trésorerie clients) est sur la liste. Silicon.fr a pu télécharger les quelques documents associés. Par eux, un fichier de clients et des identifiants d'accès aux portails de fournisseurs (Engie, Henkel, SNCF, Solvay).

** Maze était initialement distribué au travers de sites piégés. Au cours de l'automne, on a vu émerger des campagnes de* phishing*.*

*Photo d'illustration © trendingtopics*via*Visual Hunt / CC BY*