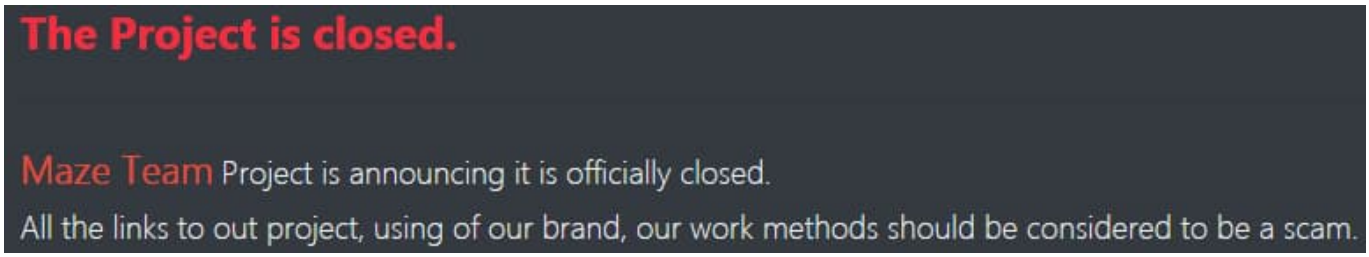
Maze : adieux intrigants pour le ransomware star de l'année 2020

Le « cartel Maze » a-t-il jamais existé ? Uniquement dans l'esprit de ceux qui en ont parlé, à en croire un communiqué récemment publié sur le « site vitrine » du *ransomware*.

Cette déclaration, signée de « l'équipe Maze », va à l'encontre de ce qu'avait pu constater la presse spécialisée. En l'occurrence, un « partage d'expérience et de plate-forme » avec le groupe cybercriminel LockBit. Et une volonté – prétendument affirmée – de coopération avec d'autres.

Au-delà de la question du cartel, le communiqué officialise la **fin de Maze**. « *Tout lien vers notre projet, tout usage de notre marque et de nos méthodes doit être considéré comme une arnaque* », peut-on lire.



« *Jamais nous n'avons eu de partenaires ou de successeurs désignés* », ajoute l'équipe Maze. Et d'inviter les entreprises victimes à se manifester sous un mois si elles souhaitent la dépublication de leurs données.

Maze : une vision du monde

La suite est un pamphlet contre la numérisation du monde. Elle fait écho à l'un des premiers communiqués qu'avait diffusés le groupe Maze. C'était en mars dernier. Le monde moderne y était comparé à une « matrice géante de données personnelles, commerciales et scientifiques ». « *Ceux qui devraient veiller à sa sûreté sont des irresponsables* », nous expliquait-on, entre deux références à Edward Snowden et à Julian Assange.

Le contexte posé, les pirates érigent leurs méfaits sur l'autel d'une entreprise de sensibilisation. Ils prétendent, au passage, avoir eu l'opportunité – volontairement non concrétisée – de couper l'accès à internet dans 35 États (sans qu'on sache desquels il s'agit). « *Un jour, ceux qui franchiront les portes ouvertes* [iront plus loin] », déclarent-ils à ce sujet.

On rappellera qu'eux-mêmes n'ont pas donné de véritables limites à leurs actions. Ils se sont notamment réservé, en cas d'échec des négociations avec les victimes, un plein droit d'usage des données dérobées. Vente, *phishing*, *name & shame*…
Les dernières règles « officielles » donnaient aux victimes trois jours à compter de l'attaque pour amorcer les négociations. En l'absence d'initiative, elles s'exposaient à la mise en ligne partielle de leurs données, avec notification des clients, des partenaires et des régulateurs. Puis à une

publication intégrale après un délai de 10 jours.

« *Nous recherchons les informations sous NDA et tout ce qui peut servir de levier à un procès* », avait expliqué l'équipe Maze au printemps dernier. Elle avait alors décrété des remises sur les rançons, dans le cadre d'une « opération spéciale pandémie ».

Pourquoi Maze s'appelle-t-il Maze ?
« *Nous reviendrons quand le monde se sera transformé* [...] *pour vous montrer vos erreurs et vous sortir du labyrinthe* ». Cette phrase figure dans le communiqué. Elle pourrait justifier le nom du *ransomware*, « labyrinthe » se traduisant, en anglais, par « maze ».

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