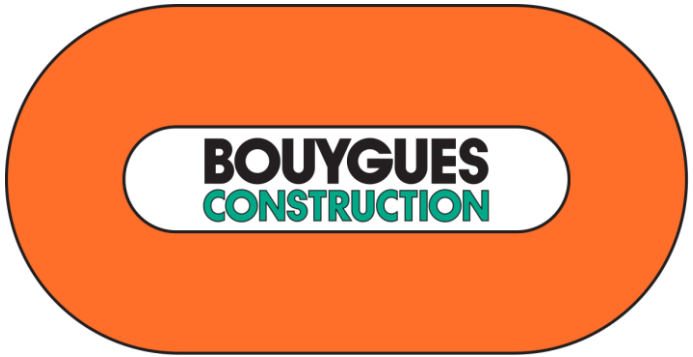
Attaque sur Bouygues Construction

Perret Jérémy
BTS SIO 1
2022-2023
Cybersécurité

Sommaire

Qui ?



- Crée en 1952
- Paris
- 37,59 milliards €
- Présent dans 60 pays

Leader Mondial de la construction

Où ?

Principales zones géographique de bouygue

Lieu de la cyberattaque

En 2001, l'UE a reconnu que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du Canada offrait un niveau de protection adéquat.

Quand ?

30 janvier
2020

Par qui ?

- Maze
- Découvert en mai 2019
- Divulgation sur internet de documents volés à des entreprises

Bouygues Construction
@Bouygues_C

Le réseau informatique @Bouygues_C a été victime d'un acte de cybercriminalité. Nous mettons tout en oeuvre pour revenir à la normale au plus vite.mediaroom.bouygues-construction.com/information-on...

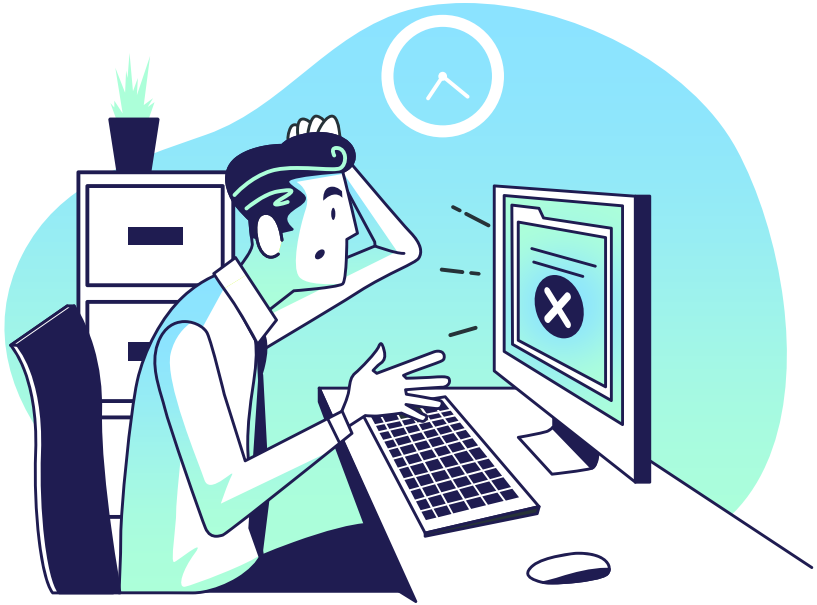
Traduire le Tweet

5:30 PM · 31 janv. 2020 · Twitter for Android

Pourquoi ?

- Chantage
- Perte de crédibilité
- Pertuber les cours de la bourse de Bouygues

Comment ?



- (Phishing)
- S’infiltre sur le réseau via le ransomware Maze
- Répandu sur l’ensemble des réseaux
- Obtiennent des privilèges sur le réseau
- Exfiltrent les données/supprime les copies/chiffre les données

Conséquences ?

- 237 fichiers (700 Téraoctets) subtilisés.
- Rançon de 10 millions
- Arrêts des équipements/serveurs
- Coupure de messagerie/d'accès aux apllications/ à internet/ à la VoIP
- 4 à 6 semaines pour un retour à la normale

Réactions/Solutions

- Plainte déposée pour extorsion en bande organisée
- Rançon non payée
- McAfee/Microsoft mobilisés
- Tous les équipements ont été testés et remis en service
- Prévention envers les employés

Sources

Présentation de Bouygues Construction

- https://www.bouygues.com/bouygues-construction/#:~:text=Pr%C3%A9sent%20dans%2060%20pays%20avec,infrastructures%20et%20de%20l'industrie.

RGPD/LPRPDE

- https://www.boreal-is.com/fr/blog/comparaison-entre-le-rgpd-et-les-autres-lois-sur-la-protection-de-la-vie-privee/
- https://www.deleguescommerciaux.gc.ca/guides/gdpr-eu-rgpd.aspx?lang=fra

Revendications de Maze/Information de Bouygues

- https://mediaroom.bouygues-construction.com/information-on-a-cyberattack/
- https://www.zdnet.fr/actualites/le-groupe-maze-affirme-etre-a-l-origine-du-piratage-de-bouygues-construction-39898575.htm

Attaque de Maze confirmée par l'ANSSI (page 25)

- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

Fin du groupe Maze

- https://www.numerama.com/cyberguerre/661925-rancongiciel-un-des-plus-gros-gangs-disparait-mais-ce-nest-pas-une-bonne-nouvelle.html

Sources

Comment fonctionne le ransomware Maze

- https://www.lefigaro.fr/secteur/high-tech/qu-est-ce-que-maze-ce-rancongiciel-qui-seme-la-terreur-dans-les-entreprises-20200206

Informations concernant l'attaque

- https://www.generation-nt.com/ransomware-bouygues-construction-maze-cyberattaque-actualite-1972725.html
- https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-884699-bouygues-construction-ferme-systemes-informatiques-attaque-ransomware.html
- https://www.lemondeinformatique.fr/actualites/lire-bouygues-construction-paralyse-par-une-cyberattaque-majeure-77926.html
- https://www.silicon.fr/ransomware-3-infos-sur-attaque-bouygues-construction-333632.html
- https://www.weodeo.com/la-securite-informatique/le-back-office-de-bouygues-construction-paralyse-par-une-cyberattaque/

Plainte déposée par Bouygues Construction

- https://www.batiactu.com/edito/cyberattaque-bouygues-construction-a-depose-plainte-58713.php