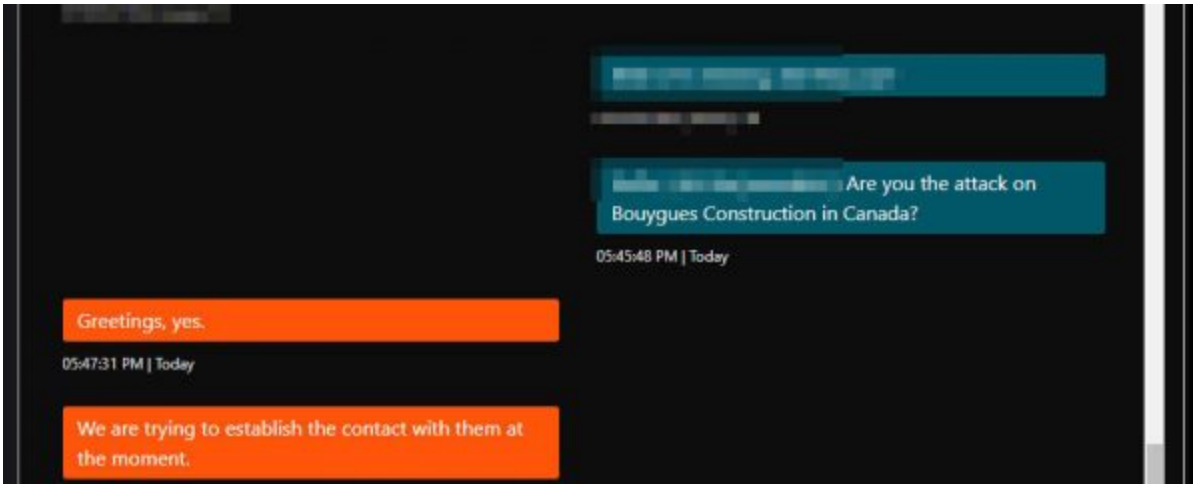
Cyber attaque à l'encontre des serveurs de Bouygues Construction

zataz.com/cyber-attaque-a-lencontre-des-serveurs-de-bouygues-construction/



Posted On 30 Jan 2020
By : Damien Bancal
Comments: 7
Tag: Bouygues construction, ransomware

Toc ! Toc ! Toc ! Qui est là ? C'est Ware… Ransomware ! L'informatique de la société Bouygues construction fermée. Une cyber attaque impacte l'entreprise.

Ambiance électrique dans les locaux de Bouygues construction à Guyancourt, en région parisienne. Le siège social (Bouygues challenger) est en ébullition. Une cyber attaque a touché l'entreprise ce jeudi. Tout serait parti de machines basées en Amérique du Nord.

Selon les informations de ZATAZ, les premières machines ont été infectées du côté de Toronto et Vancouver. L'attaque, selon d'autres sources seraient partis d'Asie.

BYCN_Portail_Depot_Factures

L'attaque semble avoir débuté via un « vers » ransomware. Cela a débuté sur les serveurs au Canada, puis propagation aux serveurs mondiaux de Bouygues construction.

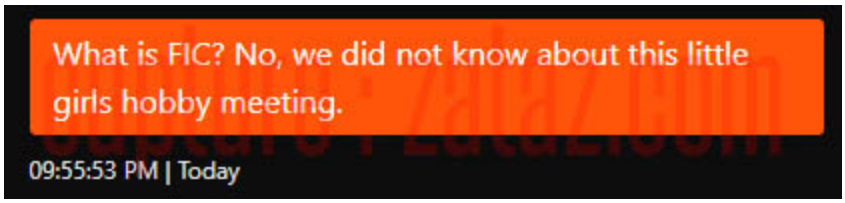
Un cyber problème d'envergure. L'ensemble des serveurs de la société ont été mis à l'arrêt.

Deux éditeurs de logiciels Américains ont été appelés à la rescousse, McAfee et Microsoft.

En contactant différents groupes pirates, j'ai pu retrouver les malveillants. Le groupe Maze. « ***Nous essayons d'établir le contact avec eux en ce moment.*** » indique-t-il !

Le service communication m'a confirmé le problème tout en étant rassurant sur le bon déroulement des chantiers et le fonctionnement normal de l'entreprise. « ***Une crise virale a été détectée sur le réseau informatique de Bouygues Construction le 30 janvier. L'analyse des causes et des impacts est en cours et les actions de sécurisation sont mises en place pour l'interne, pour nos clients et pour nos partenaires. L'activité de l'entreprise se poursuit.*** »

Mise à jour 19h : L'informatique ne devrait pas reprendre son cours normal avant un mois, un mois et demi selon des sources internes.



Mise à jour 22h : Les pirates m'ont expliqué réclamer 10 millions d'euros ! « ***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.*** » Ils auraient volé pour 200Go de données. Des preuves m'ont été communiquées. Les pirates réclament… 10 millions d'euros. Cette attaque s'est déroulée au moment de la tenue du Forum International de la Cybersécurité 2020, à Lille (Nord de la France). Un étonnant parallèle ! Ils vont me préciser ne pas connaître le FIC avec leurs… mots : « ***What is FIC? No, we did not know about this little girls hobby meeting.***«

Au sujet de l'auteur

Damien Bancal - Fondateur de ZATAZ.COM / DataSecurityBreach.fr Travaille sur les sujets High-tech/Cybercriminalité/Cybersécurité depuis 1989. Gendarme commandant réserviste Cyberdéfense Hauts-de-France. Ce blog est personnel. En savoir plus : https://www.damienbancal.fr

Articles connexes

1

Marketing de la Malveillance : exemple avec Stormous

Posted On 23 Avr 2022
, By Damien Bancal

0

Les ransomwares considérés comme la principale menace pour le secteur financier

Posted On 10 Mar 2022
, By Damien Bancal

3

Ransomware : nouvelle arrestation chez les pirates

Posted On 06 Oct 2021
, By Damien Bancal

0

Apple a-t-il payé le silence d'un groupe de pirates informatiques ?

Posted On 29 Avr 2021
, By Damien Bancal

1

L'enseigne GUESS en prise avec des pirates. Les données du patron dans les mains des voyous 2.0

Posted On 14 Mar 2021
, By Damien Bancal

6

Ransomware : un opérateur de Ryuk et Avaddon raconte

Posted On 22 Fév 2021
, By Damien Bancal

2

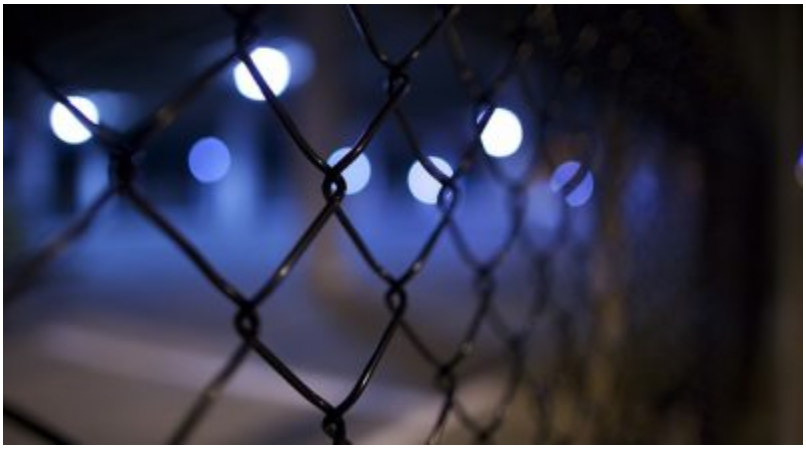
Le groupe BVA en prise avec des pirates informatiques

Posted On 17 Fév 2021
, By Damien Bancal

3

Ransomware : janvier 2021

Posted On 23 Jan 2021
, By Damien Bancal



0

120 prisons impactées par un ransowmare

Posted On 09 Nov 2020
, By Damien Bancal

0

Ransomware : payer ? Moi jamais ! … ou presque.

Posted On 30 Sep 2020
, By Damien Bancal

0

Piratage de données de la société Bridgestone

Posted On 18 Sep 2020
, By Damien Bancal

1

La société Bisnode rançonnée ? Des dizaines d'entreprises Françaises affichées !

Posted On 01 Sep 2020
, By Damien Bancal

3

Plus de 30 groupes de ransomwares en action

Posted On 27 Août 2020
, By Damien Bancal

3

Le groupe Volkswagen touché par un ransomware… et une fuite de données

Posted On 26 Août 2020
, By Damien Bancal

2

Conti : 43e groupe opérateur de ransomware

Posted On 26 Août 2020
, By Damien Bancal

Ransomware : les attaques contre la France en forte progression

Posted On 19 Juil 2020
, By Damien Bancal

0

MMA et CPM dans la tourmente du chantage numérique

Posted On 18 Juil 2020
, By Damien Bancal

1

Les pirates du groupe Nifilim prennent en otage des données du groupe Orange

Posted On 16 Juil 2020
, By Damien Bancal

0

Comptables, avocats et DRH cibles privilégiées des ransomwares

Posted On 14 Juil 2020
, By Damien Bancal

0

Prise d'otage de l'autorité régionale de transport de l'État du Texas

Posted On 03 Juil 2020
, By Damien Bancal

7 Comments

Laisser un commentaire

*

*

Ce site utilise Akismet pour réduire les indésirables. En savoir plus sur comment les données de vos commentaires sont utilisées.