ESCROQUERIE AU SUPPORT TECHNIQUE - LES CONSEILS DE L'ADC FRANCE

Categories: Les conseils, Sécurité informatique
Tags: Conseils, Enquête

Un de nos adhérents a vécu une expérience qui mérite d'être explicitée et surtout que vous sachiez quoi faire si cela vous arrive.

Les faits

Il a vu apparaitre un message d'alerte de windows defender l'informant que son ordinateur avait un grave problème de sécurité et qu'il fallait appeler le 04 28 01 06 04.

Là une charmante dame lui explique qu'il a effectivement un problème de sécurité. Il est entré ensuite en contact avec un informaticien

Le travail a consisté à retirer l'antivirus en place. Puis il a été implanté notamment mais pas que des outils utilisés pour veiller à la sécurité et notamment webroot (antivirus) et bleachbit (concurrent de ccleaner).

Pour ce faire, il a accepté d'installer ANYDESK et a laissé la main à la commerciale qui lui a vendu un contrat payable en Espagne.

Il a été utilisé également le numéro 09 74 33 81 15

La facture est arrivée dans la foulée. Le règlement a été effectué par carte bancaire. L'IBAN mentionné sur la facture est bien espagnol.

Elle est émise par la société espagnole FINTEC GLOBAL SPEED NETWORK SL

Les mails sont envoyés avec le nom de domaine fintechglobal.net. Il a été déposé le 20/06/2022. Nous publions le whois :

https://www.whois.com/whois/fintechglobal.net

Il a fait l'objet d'une alerte :

https://www.signal-arnaques.com/scam/view/579986

Le contenu du site fintechglobal.net permet de voir ce qui est proposé :

Nous publions la page accueil :

La-page-accueil-du-site-fintechglobal.pdf

La page "nos services" laissent à penser qu'il s'agit d'une société de prestations de services proposées aux entreprises :

La-page-developpement-web-du-site-fintechglobal.pdf

La-page-maintenance-du-site-fintechglobal.pdf

La-page-programmation-du-site-fintechglobal.pdf

La page boutique contient 6 tarifs sans que l'on sache vraiment le contenu de ces offres.

La-page-boutique-du-site-fintechglobal.pdf

L'activité réelle est contenue dans les conditions générales que nous publions ci-dessous :

Les-conditions-generales-du-site-fintechglobal.pdf

Il est proposé trois services. Une seule est évoquées dans la page "services" du site :

- *1-1 Ce contrat définit les termes selon lesquels Fintech Global Speed Network Limited Company "Fintech Global" délivre au "CLIENT" un service de développement.*
- *1-1 Le présent contrat définit les conditions selon lesquelles Fintech Global Speed Network Limited Company " Fintech Global " délivre au " CLIENT " un service de formation à distance également appelé " formation en ligne ou e-learning " comprenant l'accès à des modules de formation et des*

cours animés par un formateur dans un espace électronique sécurisé.

- *1-1 Le présent contrat définit les conditions selon lesquelles Fintech Global Speed Network Limited Company " Fintech Global " délivre au " CLIENT " un service de maintenance appelé " Contrat de maintenance " comprenant : une assistance téléphonique et une prise de contrôle à distance selon la formule choisie par le client ; un certain nombre d'options souscrites par le CLIENT.*

Le consommateur concerné par ce site est donc bien sur concerné par cette partie. Mais il n'est communiqué aucune information sur cette prestation. Nous supposons que les prix dans la boutique sont à minima concernés par cette troisième. Le cout de l'e-learning n'est pas mentionné.

Ces conditions ont quelques particularités. Certains passages sont en anglais. Par ailleurs, il est imposé le tribunal de commerce d'office. Nous publions les articles 14 qui sont reprises dans les 3 parties :

14-1 De convention expresse, le présent contrat sera régi par le droit européen. Les présentes conditions générales ne doivent pas être interprétées comme limitant les droits statutaires du CLIENT et rien ne limite les droits statutaires du CLIENT en tant que consommateur .

14-2 En cas d'échec d'une procédure amiable, tout litige découlant des présentes conditions est de la compétence exclusive du Tribunal de Commerce du lieu d'établissement du fournisseur.

Nous sommes perplexes tant c'est contradictoire. Par ailleurs, la société est espagnole. On saisirait quel tribunal de commerce ?

Il convient de rappeler que le droit de consommation écarte d'office le tribunal de commerce. C'est le tribunal civil du domicile du consommateur.

Nos recherches

La société a été créée le 22/06/2022. Nous publions sa fiche d'identité :

https://librebor.me/en/borme/empresa/fintech-global-speed-network/

Le gérant est aussi le responsable de la société YOUR INTERNET PROFESSIONAL SERVICES

Elle a été créée le 29/06/2021. Nous publions sa fiche d'identité :

https://librebor.me/en/borme/empresa/your-internet-professional-services/

A notre grande surprise, aucune des deux entreprises n'a de site internet. Le domaine d'intervention semblait pourtant justifier des sites.

Mais cette situation permet une grande discrétion sur la toile.

Nos conseils

Si vous avez ce message ou un écran avec "erreur fatale" contactez le ....

NE FAITES RIEN sauf débrancher l'appareil !

Vous le rallumez et vous évitez d'aller sur internet car autrement le message d'alerte va ré apparaitre.

Si le message est toujours présent, vous utilisez ccleaner (outil gratuit) pour nettoyer le disque. Cela suffira mais nous vous conseillons de faire aussi une visite de votre appareil avec l'antivirus.

Si vous avez contacté le numéro apparent et que des manipulations ont lieu et notamment l'installation acceptée d'ANYDESK, ne l'utilisez plus pour internet tant que vous ne l'avez pas fait examiné par un spécialiste. Il faudra vérifier ce que la personne a ou n'a pas installé et vérifier ce qui a été supprimé.

Vous pouvez le faire mais cela demande des connaissances informatiques.

Nous déconseillons de laisser installer ANYDESK ou tout logiciel équivalent si vous ne connaissez pas la personne qui vous le demande.

Il faudra aussi changer tous les mots de passe si vous avez un fichier qui les contient sur votre disque dur.

Si le mot de passe de votre compte bancaire est dans ce fichier, il faut IMMEDIATEMENT le changer et prévenir votre banque de la situation pour qu'elle bloque toute opération non autorisée par vos soins.

Vérifiez aussi si on n'a pas ajouté des bénéficiaires dans les virements autorisées.

Les mots de passe de votre messagerie étant changés, vous devez aussi faire un mail à tous les correspondants pour les avertir que tout va bien suite à un incident informatique.

Nous publions quelques articles qui vous donnent des informations. Nous avons déjà mis en ligne un article sur le sujet.

https://adcfrance.fr/securite-informatique/erreur-ap7mq79-le-faux-blocage-de-lordinateur/

https://support.microsoft.com/fr-fr/windows/prot%C3%A9gez-vous-contre-les-escroqueries-au-support-technique-2ebf91bd-f94c-2a8a-e541-f5c800d18435

https://blog.forumforthefuture.be/fr/article/prise-du-controle-de-votre-ordinateur-a-distance-que-faire-les-bons-reflexes-/14885

https://www.malekal.com/piratage-controle-ordinateur-distance/

https://www.avg.com/fr/signal/how-are-computers-hacked

Conclusion

Cette situation est très déplaisante. Le consommateur panique et appelle vite le numéro apparu sur l'écran. Là il sera entre les mains de personnes expertes qui vont le rassurer et régler le problème moyennant finances...

Si cela vous arrive, suivez nos conseils.

Vous pouvez nous contacter à l'adresse contact@adcfrance.fr

Une action judiciaire est possible vu la méthode utilisée qui est une intrusion non sollicitée dans un système informatique...