WWW.SPECIALISTELOGICIEL.COM

Category: Placements atypiques
Tag: Enquête

Les autres sites : WWW.ORDI99.COM et WWW.ORDITRUST.COM

Nous sommes régulièrement sollicités par les consommateurs pour des incidents survenant à nos ordinateurs.

Cela concerne notamment des demandes de règlement pour débloquer un ordinateur. Cette recherche commence avec une demande d'une consommatrice ayant vu son ordinateur "bloqué" avec une fenêtre bleue. Elle a vu apparaitre un numéro de téléphone apparaitre. Elle a alors appelé ce numéro. L'opérateur a pris la main sur l'ordinateur. Moyennant une somme non négligeable, l'appareil est apparemment revenu à son état normal. Nous avions déjà rencontré ce type de problème en 2016 avec une autre société. Nous avons donc effectué des recherches pour savoir qui était derrière ces propositions couteuses.

1) Le site Internet :

Celui-ci n'est pas ouvert. Le propriétaire est anonyme : Domaine spécialiste.org

Le seul élément intéressant est la date de création le 11 juillet 2017.

2) Les documents en notre possession :

La société a envoyé un mail avec une pièce attachées intéressante. Il s'agit de la facture. Il est indiqué que le règlement apparaitra sous le nom de "mydatadefense.com". Le n° de téléphone cité est le 01 86 65 07 98. La société serait installée 10 Rue de Moussy 75004 PARIS.

3) Les recherches de l'ADC LORRAINE :
A) Les recherches en 2017 :
a) La société :

- La facture : la date est dans le format anglais.
- 10 Rue Moussy : il n'existe pas de société informatique à cette adresse. Il s'agit d'un bureau de

poste : Google Map
- Le site www.mydatafense.com : le whois du site est anonyme : Domaine mydatadefense.com

b) Les sites Internet

- WWW.MYDATADEFENSE.COM : il n'y a aucun site accessible avec ce nom. Il n'y a pas non plus de forums ou d'avis sur le site.
- WWW.SPECIALISTELOGICIEL.COM : nous n'avons pas trouvé, comme indiqué, de site mais le nom est apparu dans plusieurs liens de Google : Specialistelogiciel.com Ce site donne deux informations. Il renvoie vers un autre site pour avoir plus d'informations. Nous publions une des pages de ce site : ARNAQUE SUSPECTÉE !!!

Le contenu des témoignages est très intéressant. Ils commencent le 10 aout 2017 :

- Le n° 01 86 65 02 35 ne donne aucun résultat.
- Le n° 01 86 65 07 98 ne donne aucun résultat. Il est mentionné sur la facture reçue par un consommateur.

Le n° 09 74 48 84 83 par contre est très intéressant. Nous publions la première page de Google avec ce numéro : Google

- ORDITRUST :

- Le site Internet : le whois est anonyme. Le site n'est pas non plus accessible : Domaine orditrust.com
- Le n° 09 74 48 84 83 a été utilisé par un autre intervenant dénommé orditrust en janvier/ février 2017. Nous publions les liens :
- ARNAQUE SUSPECTÉE !!!
- orditrust.com

- Le n° 09 75 18 66 62 est cité dans les messages du forum dédié à ORDITRUST : ARNAQUE SUSPECTÉE !!!On le trouve aussi dans un autre forum qui indique comme site www.ordi99.com : ORDI 99 arnaque ou pas

Il est également indiqué que le paiement a eu lieu sur le site www. Mypcassistance.com. Les recherches sur ces deux sites sont rapides. le nom ordi99 utilisé en mars 2017 est en vente. Le site mypcassistance est protégé par l'anonymat.

- Le n° 09 75 18 30 57 est également cité : ARNAQUE SUSPECTÉE !!!
- Le n° 04 81 68 10 14 est également cité. Les messages dans le forum datent de février 2017. Le nom de la société ou du site ne sont pas cités ARNAQUE SUSPECTÉE !!!

- Le site www.orditrust.club :

Il s'agit d'un autre site mais qui se termine par "club"

- Le n° 09 75 18 95 27 est cité : Résultats pour le numéro de téléphone 0975189527

Il est indiqué que le paiement a été fait sur le site www.fixmypc.com. Ce site est basé en Moldavie : Domaine fixmypc.club

La liste des sites hébergés à l'adresse IP nous a intrigué : Adresse IP 178.175.129.115 Les noms parlent beaucoup d'assistance aux PC.

- Les informations contenues dans les forums :

Vous avez pu voir que nous avons mis un grand nombre de forums sur les n° de téléphone utilisées. Nous avons extrait deux messages de ceux-ci sachant que dans plusieurs il est évoqué un règlement à Shangaï.

- Le forum ci-dessous contient des informations importantes dans le dernier message : ARNAQUE SUSPECTÉE !!!

> *Zak le 23/05/2017 à 05:43*
> *0186265347, 0186262291, 0975183201, 0184880375, 0975183057, 0973728022, 0186265236, 0805082128, 0977551541 ... (popup) .... easysupport Compufly Ltd, 3e étage 5162 Duke St., Halifax, NS B3J 1N7 Canada Téléphone+33 980 090 500 Courriel : info@easysupport.com (https://easysupport.com/fr/contacts/) .....qui vous demande de payer pour éradiquer un virus. C'est un popup qui vous bloque internet, le reste de votre pc fonctionne ! A ce stade rien de grave : vous faites alt-ctrl-sup et vous faites fin de tache sur votre navigateur ; puis vous enregistrer votre travail, vous arrêtez et redémarrez simplement votre ordi !! .....*

* Nous avons trouvé une autre référence sur le Canada :

> *Cat le 30/03/2017 à 11:31*
> *On vient de me contacter sur mon portable (que j'avais donné hier...) d'un autre n°+4915753037911, m''a dit qu'il appelait du Canada pour "finaliser le travail", il voulait apparemment reprendre la main, j'ai refusé et dit que je ne pouvais pas payer 99,99€, m'a répondu qu'il était technicien, que sa sté (orditrust) existait depuis une 10zaine d'années, lui ai dit que j'avais consulté internet (arnaque), m'a dit qu'on pouvait trouver n'importe quoi sur internet, donc lui ai dit, non merci mon ordi fonctionne, conversation terminée, m'a dit que je pouvais appeler quand je voulais... Va-t-il lancer une nouvelle attaque?? (mon antivirus est Avira)*

- Le site https://easysupport.com :

- Le whois du site : il est très pauvre en informations. Par ailleurs, les conditions générales sont en anglais et demandent du travail vu la longueur.
- Les forums : Google donne une idée de la situation : Google

Ils sont également très intéressants : Connaissance de Easysupport

Les explications techniques :

Il reste à découvrir comment cette arnaque est possible. En octobre 2009, la société SYMANTEC a publié un rapport où elle indique avoir identifié 250 sites appelés "facticiels" qui semblent détecter des virus factices d'où le nom "facticiel".
Ces sites proposent de vérifier vos ordinateurs en cas de pépin. Ils en profitent pour installer des virus qui se lancent... permettant ainsi d'arnaquer le consommateur en lui vendant la solution. Cette forme d'arnaque s'est développée en Europe occidentale et aux USA depuis plusieurs années. Les sites que nous venons de découvrir commencent à se créer à partir de février / mars 2015.

Nous reproduisons quelques extraits de cet article qui explique bien le mécanisme :

Pour attirer de nouvelles victimes, les cybercriminels développent des publicités sur Internet ou des sites Web qui génèrent une certaine anxiété chez l'internaute. Avec des messages tels que « si ce message apparaît, votre ordinateur court un risque ou est infecté », ils encouragent l'internaute à scanner son ordinateur ou à acheter le logiciel en question afin d'éliminer toute menace. Ainsi, 93% des installations des 50 faux antivirus les plus répandus ont été effectuées de façon volontaire par les internautes. En juin 2009, Symantec avait détecté plus de 250 antivirus factices.

Coût initial et coût caché pour les internautes :

Le coût initial pour les internautes qui téléchargent ces facticiels varie de 30$ à 100$. Néanmoins, les coûts liés à l'exploitation de leurs données par les cybercriminels sont nettement plus élevés : les informations collectées telles que les numéros de cartes bancaires peuvent être l'objet d'une utilisation frauduleuse, ou bien être revendues sur le marché noir. De plus, certains facticiels installent des codes malveillants qui placent l'utilisateur face à un risque encore plus élevé devant de nouvelles menaces.

Certains antivirus factices demandent par exemple à l'utilisateur de réduire ou de supprimer les paramètres de sécurité de son ordinateur lorsqu'il s'enregistre, voire même l'empêchent d'accéder à des sites légitimes sur la sécurité informatique après leur installation. Par conséquent, l'installation de ces programmes peut abaisser le niveau de sécurité de l'ordinateur alors qu'ils prétendent faire précisément l'inverse.

Des publicités mensongères aux messages anxiogènes pour déclencher l'achat d'un antivirus factice :

Les cybercriminels utilisent différentes méthodes pour inciter les internautes à acheter un antivirus factice ; la plupart d'entre elles repose sur la création immédiate d'une crainte d'être exposé à un risque, ainsi que sur d'autres mécanismes d'ingénierie sociale.
Les annonces proposant ce type de programmes se trouvent sur des sites crédibles et légaux comme des blogs, des forums, des réseaux sociaux ou des sites pour adultes.

Alors que les sites Internet n'ont aucun rapport avec ces activités frauduleuses, leur réputation et leur image peuvent se trouver compromises par la présence d'annonces pour des logiciels de sécurité factices. Les faux antivirus peuvent également apparaitre en tête des résultats des outils de recherche si les cybercriminels ont travaillé sur leur référencement.

Pour augmenter leur chance de « succès », les créateurs de facticiels conçoivent leurs programmes pour que ceux-ci apparaissent comme les plus crédibles possible. Ils prennent en effet l'aspect graphique des vrais logiciels de sécurité conçus par les éditeurs du marché, ou bien porte des noms trompeurs comme SpywareGuard 2008, AntiVirus 2008 ou encore Nortel 2009. Ils sont par ailleurs distribués sur des sites qui jouissent d'une bonne réputation et permettent à l'utilisateur un téléchargement facile. Certains vont même jusqu'à utiliser des moyens de paiement usuels sur Internet et à envoyer à leurs victimes un reçu par email, avec numéro de série et service client.

Il reste à vous donner de bons conseils !

Les bons réflexes :

• Surtout n'obéissez jamais à une alerte sur votre ordinateur qui vous demande de téléphoner à un numéro téléphonique !!! Si votre ordinateur affiche une alerte de virus ou tout autre fenêtre qui bloque votre ordinateur, faites appel à un professionnel près de chez vous,

• Pour isoler votre ordinateur, éteignez-le sur le champ et débranchez-le du réseau Internet en débranchant le câble de l'ordinateur qui le lie à votre box,

• Faites des photos avec votre téléphone portable par exemple et déposez plainte à la police car il s'agit d'une intrusion sur votre ordinateur,

• Vous pouvez avec l'aide d'un professionnel suivre les instructions sur ce site web pour tenter d'identifier le Ransomware : https://id-ransomware.malwarehunterteam.com/

Vous trouverez in fine de cet article des astuces pour éviter de payer.

Les remarques suite à notre enquête

Nous avons enquêté avec l'aide de certaines victimes et nous pouvons déjà vous certifier un certain nombre de choses :

- Inutile de chercher le responsable du site web notamment avec les informations données par la société qui a procédé à l'enregistrement du nom de domaine. Nous nous sommes rendus

compte que les numéros de téléphones et les coordonnées du propriétaire du nom de domaine sont faux. Vous pouvez par contre demander à celui qui a procédé à l'enregistrement du site web à bannir le nom de domaine pour empêcher de nouvelles victimes,
- Les sites en ligne comme https://www.virustotal.com/ ne détectent pas les virus contenus dans les pièces jointes envoyées par courriel. Nous vous recommandons donc toujours de ne pas ouvrir les pièces jointes de destinataires inconnus même si leurs messages semblent légitiment (remises de factures, message important des impôts, de la CPAM…),
- Nous recommandons la plus grande prudence à ceux qui se risqueraient à cliquer sur un lien dans un courriel de destinataire inconnu. Identifiez votre destinataire par les sources officielles à votre disposition : les pages jaunes, les moteurs de recherche, les registres du commerce disponibles via societe.com,
- Enfin, ne contactez jamais une de ces sociétés par les numéros ou sites web fournis si vous n'avez pas la certitude que cette société existe officiellement.

Depuis 2009, la situation s'est aggravée ! Nous avons découvert un site intéressant. Il s'agit de https://stopransonware.fr

Ne ratez pas le site ! Vous allez découvrir une multitude nouveaux pièges… mais outre cet aspect, vous allez aussi y trouver des outils intéressants pour lutter contre une infection de votre ordinateur et de très bons conseils ! Il est à noter que ce site est partenaire de la gendarmerie nationale.

4) Les solutions :

1. En premier lieu, ne jamais appeler ces gens et surtout ne jamais leur, laisser la main sur l'ordinateur.
2. Le lien ci-dessous est vraiment très bien fait. Il vous donne les explications et comment se débarrasser de ce truc.
   Arnaque support téléphonique – PC Support
3. Nous vous conseillons d'installer l'application ccleaner qui est gratuite et très efficace.
4. Pour ne plus être ennuyé, la manip ci-dessous devrait vous redonner la main : controle + alt + suppr
   ARNAQUE SUSPECTÉE !!!
5. Le lien ci-dessous est intéressant. L'internaute a indiqué que l'ordinateur appartenait à son entreprise… Cela a calmé l'ardeur de la personne.
   Vigilence Escroquerie ! Appel téléphonique de Microsoft pour une assistance technique…

Plus que jamais, la prudence est mise sur Internet. Si vous êtes concernés par cette arnaque, contactez nous à l'adresse suivante contact@adcfrance.fr