WWW.EUREKA24.FR

Category: Placements atypiques
Tag: Enquête

Les autres sites : WWW.SUPPORT247.FR et WWW.SUPPORTDEPC.FR

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'un consommateur ayant vu son ordinateur "bloqué" avec une fenêtre bleue. Il a vu apparaitre un numéro de téléphone apparaitre. Il 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.
Le site www.eureka24 découvert en 2016 continue son activité. Les recherches effectuées précédemment sont confirmées au 19.08.2017.

Nous vous restituons les informations. Les témoignages des consommateurs montre une grande activité dans ce domaine. Il s'agit de problèmes concernant des comportements douteux de vos ordinateurs : écrans bleus, souris qui s'activent toutes seules, des disques durs fonctionnant sans arrêts même quand l'ordinateur est au repos.

Si c'est le cas, vous êtes sans doute victime d'un programme malveillant. Pour les écrans bleus, si vous avez de plus un petit numéro s'affichant pour téléphoner à une hotline et que l'ordinateur ne peut aller plus loin, vous avez sans doute à faire à un 'ransomlogiciel'. Il s'agit d'un pop up qui s'est invité sans votre accord et vous fait croire que l'ordinateur est bloqué. Vous êtes alors invité à contac ter un n° de téléphone pour débloquer la situation.

Cela commence par l'apparition un écran bleu similaire à celui de Windows en cas de gros problème. La différence ? Un n° commençant par 09 77... Le contact avec cette "société" a été difficile. Le consommateur a réussi au deuxième appel à faire supprimer l'écran bleu par son interlocuteur. Ce "technicien" a tenté de convaincre le consommateur d'acheter un logiciel moyennant 400 € pour se débarrasser de son écran bleu. Il a tenté de le renvoyer sur le site

www.eureka24.fr. Devant la ferme opposition de notre consommateur, son correspondant a pu à distance supprimer cet écran bleu non sans avoir pris la main à distance sur son ordinateur !

Devant cette situation, notre service enquête a effectué des recherches sur ce site qui nous a intrigué. Le résultat est communiqué ci-dessous :

1) Les sites Internet :

- eureka24.fr : le whois du site : Domaine eureka24.fr

Il est à noter qu'en 2016, le whois indiquait comme déposant du nom de domaine François SIMON domicilié 3 Rue Marcadet 75018 PARIS. Il s'agit en fait d'un café : Google Map
Par ailleurs, Monsieur SIMON a indiqué un mail identique pour eureka24.fr un deuxième site dénommé support247.fr. Il est aussi concerné par le site www.supportdepc.fr

- Les Conditions Générales de Vente : la visite du site permet de découvrir des conditions générales rédigées en anglais de 17 pages.

Les Conditions Générales de Vente d'Eureka24

Deux informations dans ce maquis juridiques sont intéressantes. Il est cité les articles du code civil de Californie, la deuxième indique une adresse où envoyer toute réclamation en France dans le département 74. Il est proposé en outre 4 formules d'assistance. L'apparence du site semble très professionnelle mais ne présente pas de grand intérêt. Il n'y a qu'un numéro de téléphone. Il n'a pas été possible de trouver dans la page accueil l'adresse du site ou un siret français alors qu'il est indiqué que la société est française.

Les recherches de l'ADC LORRAINE :

a) Le test du service :

Nous avons testé le numéro indiqué. Au premier appel, notre correspondante a raccroché brutalement quand nous avons demandé l'adresse et le siret de l'entreprise... Au deuxième appel, la correspondante nous a indiqué que l'équipe technique était installée à Montréal (Canada) et que le siège social était 105 Rue des Pommiers, 11803 SAINT MARTIN. Ces deux personnes avaient un prénom arabe. En réalité, à cette adresse en haute Savoie et non 11803, on trouve une société de domiciliation qui reçoit et transmet le courrier d'expatriés ou qui propose la domiciliation de sociétés.

La société UBIDOCA

Notre correspondante nous a simplement lu l'adresse mentionnée dans un document émanant soi disant de Microsoft. Il est donc impossible, à partir du site de savoir qui se cache derrière.

b) Les recherches sur Internet :

L'adresse IP permet de découvrir qu'il existe un deuxième site www.daemtaqni.com créé le 17 juin 2016. La page accueil donne le même numéro de téléphone que eureka24.fr avec des mentions en langue arabe. Nous publions celle-ci en arabe et en français :

La page accueil du site www.daemtaqni.com

Le whois de ce site permet de constater que l'adresse IP du site est la même que le site eureka24.fr. Les prestations du site sont identiques à celles d'eureka24.fr. Il n'y a donc pas de doute sur le lien entre les deux sites. Il s'agit d'un site miroir qui permet , en cas de fermeture d'un site frauduleux, de lancer le deuxième immédiatement.

L'écriture arabe sur cette page nous a amené à regarder dans google avec le nom "eureka24". Nous avons constaté l'existence d'un site www.eureka24.tn (Tunisie). Ce site ne propose aucun produit à la vente mais offre des emplois en Tunisie. Les mentions dans le whois ou sur le site ne permettent pas d'identifier la société car toutes les références sont inconnues du site officiel tunisien identifiant les sociétés.

Nous publions la page accueil du site : ASSISTANCE TECHNIQUE EN LIGNE

Pour rappel, le site eureka24.fr mentionne une société française avec 100 salariés. Le descriptif des postes offerts est intéressant :

VOUS ETES EXCEPTIONNEL EN VENTES ? VOUS VOULEZ ETRE RICHE ?

Le whois du site www.eureka24.tn : Domaine eureka24.tn Le whois permet d'établir que le nom de domaine a été déposé par la société eureka24.fr ayant son siège social à Tunis. Nous publions une offre d'emploi. Pour compléter ces informations, le site najdapc.com contient des informations sur eureka24 et daemtaqni.com.

Nous publions sa page accueil : le site www.nadjacpc.com

- Le site supportdepc.fr :

Pour finir cette partie de la recherche, une recherche avec M SIMON comme déposant permet de constater qu'il est aussi concerné par ce site.

- Les forums :

- eureka24.fr : il existe un nombre important de forums expliquant la situation. Nous en publions plusieurs :
- Question sur service technique eureka 24.fr
- Arnaques aux désinfections / support par téléphone

Un forum récent : Appel bizarre de Microsoft Allemagne et Angleterre au sujet de ma licence

- Le site www.support247.fr : le forum montre que le mécanisme est le même : ARNAQUE SUSPECTÉE !!!
- Le site supportdepc.fr : Classe mondiale avec assistance technique instantanée
  Les prix sont en $ et les services proposées en anglais ! Un appel coute 120 $, un nombre illimité 180 $... L'heureux propriétaire de ce site est M. François SIMON déjà cité. Selon domaintools, M. SIMON (s'il existe) est propriétaire de 26 sites au total dont un - www.support247.fr est intéressant. Ce site n'est plus accessible mais il est également cité dans des forums : Description du message

Nous sommes donc en présence d'utilisation d'internet pour convaincre les consommateurs de payer une prestation qui n'existe pas. Elle est gérée depuis la Tunisie.

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 en fin 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