AVRIL - JUIN 2019 | N°1

CYBERSECURE

FEDERATION EBEN
ENTREPRISES DU BUREAU ET DU NUMERIQUE

AU SOMMAIRE

A la Une : l'arnaque au faux support technique

ATTENTION AU COUP DE LA PANNE !

La victime est contactée par SMS, e-mail, messagerie instantanée ou voit apparaitre un message sur l'écran de son ordinateur, tablette ou smartphone : on lui signale un problème grave (panne, virus, licence ou logiciel expiré) et on lui demande de rappeler un numéro de support technique d'apparence officielle, sous peine de perdre toutes ses données ou de ne plus pouvoir utiliser son matériel.
Parfois, l'équipement de la victime peut sembler complètement bloqué et même l'être réellement dans des cas plus rares. Une fois le contact établi, les cybercriminels se présentent comme des techniciens et prétendent réparer la machine de leur victime. Après avoir mis en confiance la victime, les escrocs peuvent aller jusqu'à lui demander d'installer un logiciel sur sa machine de façon à en prendre le contrôle à distance.
Cette prestation de dépannage factice est généralement facturée entre 200 et 500 euros. Dans certains cas, lorsque la victime refuse de payer, les criminels n'hésitent pas à la menacer de détruire ses fichiers ou de divulguer les informations personnelles présentes sur sa machine. Craignant de voir ses données disparaître ou divulguées, la victime n'hésite pas à verser la somme demandée.

CAS CONCRET

Trois cybercriminels ont été interpellés dans le département du Rhône et placés en garde à vue le 29 janvier 2019 dans le cadre de ces fraudes massives aux réparations informatiques, a annoncé le parquet de Paris. Présentés à un juge d'instruction, ils ont été mis en examen pour «escroquerie» et «blanchiment en bande organisée» ainsi qu'«introduction frauduleuse de données dans un système de traitement automatisé de données» avant d'être placés sous contrôle judiciaire.

> Le bilan à ce jour est de :
> - 8000 victimes
> - 1,9 millions d'euros déjà saisis par la justice

Ayez les bons réflexes

LES GESTES ÉLÉMENTAIRES

- Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.
- Tenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.
- Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.
- N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.
- N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.
- N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.
- Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.
- Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

*Retrouvez l'ensemble des ces régles et plus encore sur la plateforme www.cybermalveillance.gouv.fr

LE SAVIEZ-VOUS ?

CYBERMALVEILLANCE.GOUV.FR

Cybermalveillance.gouv.fr est le programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. La plateforme en ligne du dispositif vous accompagne et met à votre disposition un kit de sensibilisation qui vise à sensibiliser aux questions de sécurité du numérique, à partager les bonnes pratiques dans les usages personnels, et de manière vertueuse, à améliorer les usages dans le cadre professionnel. Alors, téléchargez dès maintenant votre kit et diffusez-le dans votre entreprise !

28 855 victimes sont venues chercher de l'assistance sur la plateforme www.cybermaveillance.gouv.fr en 2018 dont 24 574 particuliers, 3 650 entreprises et 631 collectivités. Entre le début et la fin de l'année, c'est +500% de personnes qui viennent mensuellement sur la plateforme chercher de l'assistance.

En ce qui concerne les entreprises, les principales menaces identifiées sont les intrusions sur le serveur (16%), les attaques par hameçonnage / phishing (14%), le piratage de compte, le pourriel (spam) et les virus (dont rançongiciel/ransomware) dans 12% des cas. Cyber28 28 855 victimes sont venues chercher de l'assistance sur la plateforme www.cybermaveillance.gouv.fr en 2018 dont 24 574 particuliers, 3 650 entreprises et 631 collectivités. Entre le début et la fin de l'année, c'est +500% de personnes qui viennent mensuellement sur la plateforme chercher de l'assistance.

En ce qui concerne les entreprises, les principales menaces identifiées sont les intrusions sur le serveur (16%), les attaques par hameçonnage / phishing (14%), le piratage de compte, le pourriel (spam) et les virus (dont rançongiciel/ransomware) dans 12% des cas.

ADRESSES UTILES

- www.cybermalveillance.gouv.fr
- ANSSI, www.ssi.gouv.fr
- Cnil, www.cnil.fr/professionnel
- Global Security Mag, www.globalsecuritymag.fr
- no more ransomeware https://www.nomoreransom.org/fr/index.html

Cette lettre d'information vous est offerte par votre prestataire

ESPACE MICRO Informatique et Services

Fédération EBEN
69, rue Ampère
75017 Paris
www.federation-eben.com

Directeur de la publication : Loïc Mignotte
Rédaction : Fédération EBEN, Cybermalveillance.gouv.fr
Photos : Unsplash, Adobe Stock
Maquette : Emmanuelle Bauvais