Faux support technique, des modes opératoires toujours plus agressifs

Publié le 25 Avr 2024

Temps de lecture : 6 min

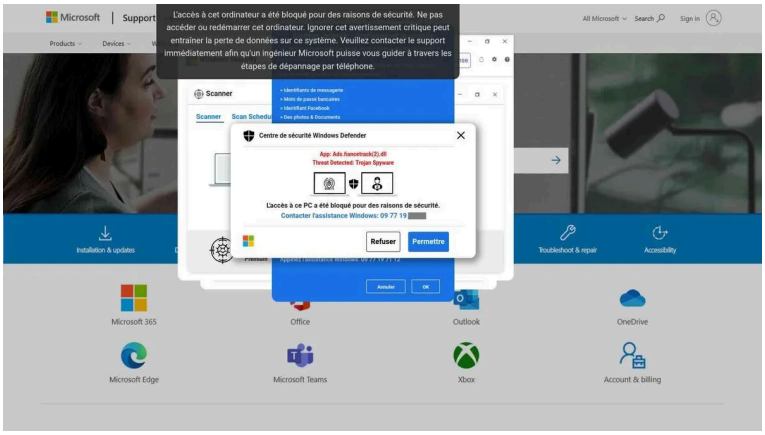
Parmi les grandes tendances de la menace en 2023 recensées dans notre dernier rapport d'activité, l'arnaque au faux support technique ne faiblit pas en intensité et se révèle toujours plus virulente.

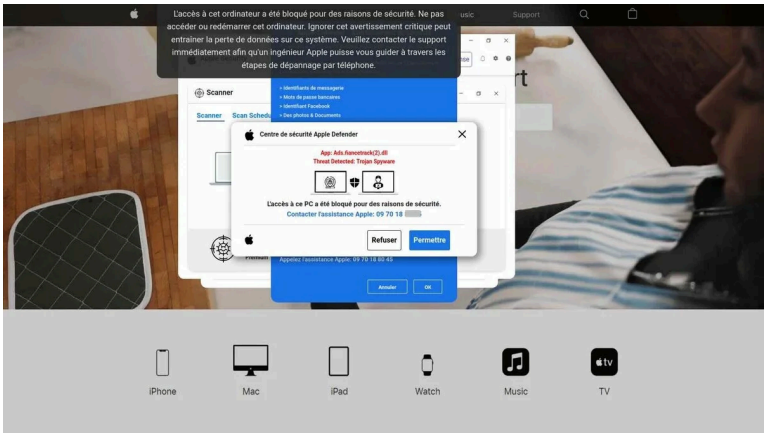
Quels publics sont concernés ?

En 2023, les escroqueries au faux support technique Microsoft ou Apple reprennent la 3e place des principales menaces pour les particuliers et se maintiennent à un niveau très élevé avec 12 000 recherches d'assistance et 140 000 consultations de notre article dédié.

Les entreprises et collectivités, et surtout celles qui ne disposent pas de support informatique, ne sont pas épargnés par cette menace.

Captures d'écran de pages d'alertes d'arnaques au faux support technique (cliquez pour agrandir) :





Quelles évolutions du mode opératoire ?

Les modes de déclenchement d'une alerte anxiogène indiquant une infection virale et demandant d'appeler en urgence un prétendu support technique « gratuit » restent globalement similaires.

Ils reposent principalement sur un hameçonnage par courrier électronique (fausses notifications ou lettres d'informations par exemple) contenant des liens malveillants ou par des pages frauduleuses sponsorisés sur les moteurs de recherche.

Depuis fin 2022 le mode opératoire des opérateurs de faux support technique, qui repose également sur l'**ingénierie sociale**, se révèle beaucoup plus agressif. Aujourd'hui, les escrocs ne se contentent plus de faire payer un dépannage à distance factice.

Les cybercriminels prennent le contrôle des comptes bancaires en ligne de la victime au prétexte que la pseudo-infection virale les aurait affectés. Ils vont ensuite manipuler la victime pour lui faire valider des opérations, soi-disant pour « sécuriser » ses comptes bancaires mais qui en réalité vont avoir pour effet de leur permettre de les piller, à l'instar des modes opératoires d'arnaques au faux conseiller bancaire.

Quels montants de préjudice ?

Les montants constatés de préjudice pour les victimes d'escroquerie au faux support technique, qui jusqu'alors étaient de quelques centaines d'euros, peuvent aujourd'hui atteindre **plusieurs milliers, voire dizaines de milliers d'euros**.

Pour aller plus loin :

- Découvrez les principales tendances de la menaces et les chiffres clés de la plateforme Cybermalveillance.gouv.fr en 2023 dans notre dernier rapport d'activité
- Découvrez le top 10 des cybermenaces les plus fréquentes pour les particuliers
- Découvrez le top 10 des cybermenaces les plus fréquentes pour les entreprises et associations
- Découvrez le top 10 des cybermenaces les plus fréquentes pour les collectivités et administrations

DÉMARRER UN DIAGNOSTIC

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

Entrez votre adresse email

OK

À PROPOS

Qui sommes-nous ?

Presse

DIVERS

Plan du site

Données personnelles

Mentions légales

NOUS SUIVRE

GOUVERNEMENT.FR

ELYSEE.FR

SERVICE PUBLIC

LEGIFRANCE

FRANCE.FR

DATA.GOUV.FR