Communiqué de presse
Paris, le 22 mars 2018

Orange Cyberdefense lance une borne mobile de décontamination des clés USB

- Très utilisées, les clés USB arrivent en 2ème position au classement des cyber menaces les plus dangereuses
- La version mini-borne Malware Cleaner détecte les « badUSB », des menaces indétectables avec les anti-virus classiques
- Malware Cleaner est disponible en France et à l'international

70 %* des salariés font usage de clés USB venues de l'extérieur et la connectent sur le réseau de l'entreprise et 68 %* n'ont pris aucune protection avant de les insérer sur leur PC professionnel[1].

Les clés USB, qu'elles soient neuves ou déjà utilisées, sont des vecteurs importants d'infection des systèmes d'information des entreprises. Elles sont toujours très présentes, notamment dans certains secteurs comme l'industrie, l'éducation et la santé, tant pour le partage de documents que pour des opérations de mises à jour logicielles.

Une nouvelle borne mobile pour développer le réflexe de décontamination
Jusqu'à présent disponible sous forme de kiosques fixes de 70 kg ou en version logicielle installée sur certains PC, la solution Malware Cleaner est désormais disponible en version « mini-borne ». Grâce à cette version moins onéreuse et nomade, les entreprises peuvent généraliser le réflexe de décontamination des clés USB. Mobiles, il est possible de les mettre à disposition à l'accueil, dans des salles de réunions de l'entreprise ou encore partagées entre différents sites en fonction des besoins.

Cinq moteurs de recherche antivirale intégrés pour détecter les menaces
Malware Cleaner a été développée par les experts d'Orange Cyberdefense et notamment ses équipes de « *Ethical Hacking* » (hacking éthique). Simple et rapide d'utilisation, il suffit d'insérer la clé USB pour savoir si elle est infectée. Si c'est le cas, l'utilisateur peut choisir de supprimer le fichier en question ou de le mettre en quarantaine. Il est aussi possible d'éditer un rapport pour avoir plus de précisions sur l'analyse de la clé : détails des fichiers infectés, signatures des attaques détectées, le nom des moteurs antivirus ayant détecté le fichier infecté….

Cette solution utilise simultanément cinq moteurs de recherche antivirale pour optimiser les capacités et la couverture de détection en bénéficiant de la performance et de la complémentarité des cinq anti-virus. Ces derniers sont mis à jour quotidiennement de manière automatique quand la borne est connectée à internet via le réseau ou en 4G. D'ici

[1] source : Ponemon Institute, 2014

la fin de l'année, Malware Cleaner comptera deux anti-virus supplémentaires.
La solution embarque également un moteur de détection des attaques de type badUSB, indétectables par les anti-virus classiques, qui permettent de prendre le contrôle d'un ordinateur.

Malware Cleaner inclut une console d'administration pour gérer les bornes à distance permettant de vérifier le bon fonctionnement et les mises à jour, de disposer de statistiques d'utilisation en temps réel, de connaître le nombre de fichiers infectés ou encore les types d'attaques observées. Toutes ces informations précieuses permettent d'améliorer la sécurité de l'entreprise.

L'industrie, un secteur particulièrement exposé
Dans le secteur de l'industrie, les ordinateurs de pilotage de chaînes de production ne sont pas connectés à internet pour des raisons de sécurité. Les ports USBs de ces machines, sont ainsi régulièrement utilisés pour établir les diagnostiques de maintenance, récupérer les logs SCADA, ou effectuer des mises à jour. Cela les rend particulièrement vulnérables aux attaques via clé USB. Grâce au logiciel « Malware Cleaner » installé sur un PC situé à l'entrée de la zone de production, et à l'ajout d'un protocole de sécurité qui oblige à scanner tous les dispositifs USB dans la borne, la chaîne de production est protégée des attaques via clé USB.

« *Les clés USB constituent un véritable danger pour la sécurité informatique des entreprises. Même si ces attaques sont plus compliquées à mettre en œuvre que des attaques par email par exemple, elles restent redoutables. L'introduction de clés USB au cœur des équipements de l'entreprise permet de propager des codes malicieux, de paralyser des machines, de perdre de données sensibles ou encore de détruire des postes de travail. Un ransomware peut être installé sur un système industriel simplement en insérant une clé USB, sans avoir besoin d'une action de l'utilisateur.»,* précise Alexis Richard, Product Manager chez Orange Cyberdefense.

La solution Malware Cleaner sera en démonstration lors du salon Smart Industries du 27 au 30 mars 2018 (stand 110, Hall 3, Allée G)

Les « règles d'utilisation des clés USB en entreprise » :

- Ne pas brancher une clé USB à un poste de travail dont on ne connait pas la provenance
- Renouveler les clés USB des collaborateurs afin d'éviter la propagation de malwares
- Fournir des clés USB aux collaborateurs pour éviter qu'ils utilisent des clés USB de l'extérieur
- Systématiquement contrôler les clés USB dès lors qu'elles ont été branchées dans un environnement non sécurisé
- Brancher uniquement des clés préalablement décontaminées dans les PC industriels

collectivités en France font confiance à Orange Business Services. A l'international elles sont plus de 3 000 multinationales de renommée mondiale.

Pour plus d'informations, rendez-vous sur www.orange-business.com ou suivez-nous sur LinkedIn, Twitter et nos blogs.
Orange est l'un des principaux opérateurs de télécommunications dans le monde avec un chiffre d'affaires de 41 milliards d'euros en 2017 et près de 273 millions de clients à travers 29 pays au 31 décembre 2017. Orange est cotée sur le NYSE Euronext Paris (symbole ORA) et sur le New York Stock Exchange (symbole ORAN).

Contacts presse :
Orange : Nathalie Chevrier ; 01 44 44 93 93 ; nathalie.chevrier@orange.com
Orange Business Services : Caroline Cellier ; 01 55 54 50 34 ; caroline.cellier@orange.com