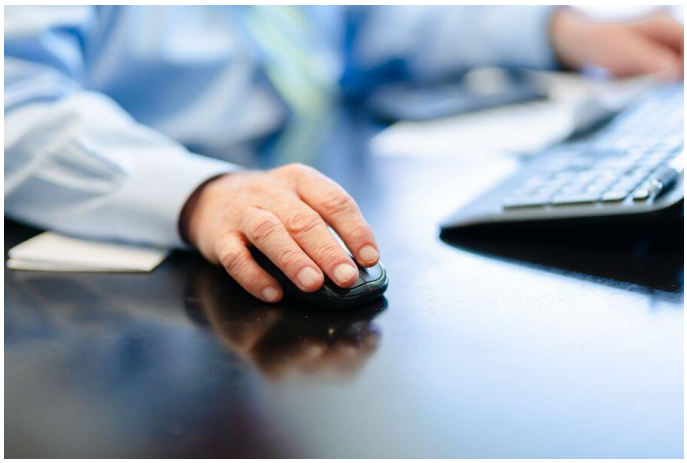
CROWDSTRIKE : POURQUOI LA MISE A JOUR D'UN ANTIVIRUS A PARALYSE LES ENTREPRISES DU MONDE ENTIER ?

De nombreuses entreprises ont été touchées par une panne critique sur des PC et serveurs Windows ce 19 juillet. En cause, une mise à jour défectueuse d'un logiciel de cybersécurité développé par CrowdStrike. Une solution de protection très avancée mais dont le dysfonctionnement a des conséquences très lourdes. Découvrez comment et pourquoi une telle panne a pu se produire.



Avions cloués au sol, chaînes de télévision et banques qui dysfonctionnent, hôpitaux perturbés… Depuis ce 19 juillet au matin, de nombreuses grandes entreprises et administrations tournent au ralenti. Des ordinateurs et serveurs sous Windows sont bloqués sur un "écran bleu" de panne critique dès leur démarrage. La faute à une mise à jour défectueuse du logiciel d'Endpoint Detection and Response (EDR) de la société américaine CrowdStrike, dénommé Falcon.

Pour contrer les malwares, les EDR interviennent à très bas niveau dans le système d'exploitation

Les EDR sont les successeurs des antivirus des années 90, qui détectaient des signatures dans des fichiers exécutables. Si l'antivirus trouvait une correspondance entre le contenu d'un fichier et les signatures de sa base de données, alors celui-ci pouvait être infecté. Un EDR va beaucoup plus loin : il effectue un suivi comportemental, enregistre toutes les activités du système et les stocke dans un journal, et peut intervenir à très bas niveau, jusqu'au noyau du système d'exploitation.

Ces capacités sont devenues nécessaires avec l'arrivée de malwares de plus en plus sophistiqués, qui ont rendu les antivirus obsolètes. Elles sont aussi ce qui a rendu possible cette panne d'envergure mondiale lorsque Falcon Sensor (le composant de l'EDR qui effectue le suivi à très bas niveau) a reçu une mise à jour mal formatée, qui a fait crasher son pilote au démarrage du système d'exploitation.

Les utilisateurs d'EDR autorisent bien souvent les fournisseurs de ces solutions à effectuer des mises à jour automatiques. Ceci évite que les systèmes ne deviennent vulnérables au cas où l'utilisateur rechigne à accepter faire les mises à jour, et permet de garantir la sécurité de très grandes flottes d'appareils (les "endpoints" concernés comprennent aussi bien les serveurs, les ordinateurs professionnels et smartphones que les objets connectés). Cette automatisation est la raison pour laquelle des milliers d'entreprises se sont retrouvées touchées simultanément.

Les mises à jour en fin de semaine, une mauvaise pratique

On notera au passage que CrowdStrike a mal joué du début à la fin. Car en matière de sécurité informatique, effectuer des mises à jour en fin de semaine – et a fortiori le soir – est un choix peu judicieux : mobiliser les équipes IT un vendredi soir ou un week-end est délicat et fait qu'une panne ou d'un incident de sécurité peuvent durer plus longtemps. C'est pour cette raison que Microsoft applique toujours ses mises à jour de sécurité mensuelle le mardi matin.

Qui est CrowdStrike ?

Pourtant, CrowdStrike n'en est pas à son premier rodéo. Appréciée des institutions américaines, la société texane fournit des services de cybersécurité aux entreprises depuis 2011. Son logiciel d'EDR, Falcon, avait été lancé en 2013. Elle dispose d'une importante équipe de chercheurs, mais aussi d'investigateurs qui enquêtent sur les cyberattaques. Elle avait ainsi découvert en 2014 l'implication de la Corée du Nord dans la cyberattaque contre Sony Pictures, et avait aidé le FBI dans l'enquête sur le piratage par la Russie du parti démocrate américain.

Comment cette mise à jour a pu être envoyée aux clients ?

Par chance, seules les machines utilisant Windows ont été touchées, mais ça aurait pu ne pas être le cas. Falcon est aussi disponible pour Mac et Linux, mais la mise à jour en question ne concernait que Windows. Ce n'est d'ailleurs pas la première fois qu'un incident de ce type se produit avec les solutions de CrowdStrike. Une mise à jour problématique avait été publiée il y a quelques semaines pour les distributions Linux Red Hat Enterprise, mais sans grand impact car elle n'avait pas été appliquée automatiquement.

Ce qu'il reste à déterminer aujourd'hui c'est comment une mise à jour à ce point défectueuse a pu être envoyée de cette manière à tous les clients de CrowdStrike. A-t-elle été correctement testée avant son déploiement intégral ? La société devra fournir des explications à ce sujet. George Kurtz, fondateur et PDG de CrowdStrike, qui s'est exprimé sur X (ex-Twitter), n'a pour l'instant pas donné d'explications (ni même présenté d'excuses).

CrowdStrike peut-elle se remettre de cet incident ?

Reste aussi à savoir si CrowdStrike parviendra à se remettre de cet incident. À Wall Street, l'action de la société a plongé de plus de 20% à l'ouverture. Etant donné les problèmes qu'a déjà connu le fournisseur par le passé, ses clients vont-ils lui rester fidèle ? Vont-ils lui demander une indemnisation ?

Le manque à gagner se chiffrera en tout cas en milliards de dollars au total pour cet incident, car si les machines peuvent désormais repartir grâce à des interventions manuelles, la restauration des centaines de milliers de systèmes concernés risque de prendre du temps. Cette panne pourrait donc être l'un des incidents informatiques aux plus longues répercussions de l'histoire.

Source L'Usine Digitale - juillet 2024