Photo de Igor Omilaev sur Unsplash

Panne CrowdStrike : comment une simple mise à jour a-t-elle entrainé une telle pagaille ?

« C'est le stagiaire qui… »

Vincent Hermann
Le 19 Juillet à 17h59

Sécurité | 6 min

L'incident survenu chez CrowdStrike a entrainé un plantage d'un très grand nombre d'ordinateurs Windows. Comment en est-on arrivés là ? Il s'agit très probablement de la convergence de plusieurs facteurs techniques, que nous allons exposer.

Dans notre article, nous relations comment une mise à jour du logiciel Falcon Sensor de CrowdStrike avait provoqué une épidémie d'écrans bleus à travers le monde. La panne engendrée a touché de nombreux aéroports et autres structures.

Comme le déploiement d'une telle mise à jour a-t-elle été possible ? Et comment la mise à jour d'un produit de sécurité peut-elle aboutir à un plantage complet du système ?

Sous Windows, comme sur n'importe quel autre système d'exploitation, il existe des niveaux de privilèges, basés sur un système d'anneaux concentriques (les fameux rings). Le ring 0 constitue l'espace noyau (ou kernel). Les privilèges y sont maximaux, de même que les performances. Dans son infrastructure, Microsoft a simplifié les autres niveaux depuis longtemps et n'en laisse aujourd'hui qu'un autre : le ring 3, l'espace utilisateur.

Dans les vieilles versions de Windows, de nombreux pilotes étaient en espace noyau. Aujourd'hui, le paysage a changé. L'évolution du framework de développement des pilotes a repoussé un nombre croissant de catégories vers le ring 3. Sous les actuels Windows 10 et 11, les pilotes en espace noyau sont beaucoup plus rares. Le cas le plus connu est le pilote graphique, pour des questions de performances.

L'autre exception est pour les logiciels de sécurité. On parle ici des antivirus et plus généralement des suites de sécurité. Ce type de produit surveille un certain nombre de processus. Pour le faire, ils utilisent le plus souvent un pilote en espace noyau, lui octroyant les privilèges nécessaires à une telle surveillance.

clignotement soudain de l'écran sous Windows, le système vous avertissant qu'une panne du pilote graphique a été détectée. Le message indique que le pilote a été relancé. Parfois, le système n'y parvient pas et un écran bleu se produit.

Comme l'explique l'ingénieur Aurélien Chalot chez Orange Cyberdéfense, le fonctionnement est le même pour les EDR (Endpoint Detection and Response), auxquelles appartiennent les suites de sécurité. La proximité du pilote avec le noyau lui octroie privilèges et performances. Mais, en cas de plantage, c'est le noyau lui-même qui risque de partir avec l'eau du bain.

Falcon Sensor de CrowdStrike possède bien un pilote en espace noyau, csagent.sys. C'est un agent responsable du cœur des fonctionnalités de surveillance. Il est alimenté très régulièrement par des fichiers de définition. Ceux-ci permettent de mettre à jour les capacités de détection des malwares de l'agent en lui donnant les moyens de les repérer par leur empreinte.

Falcon Sensor, comme tous les autres solutions de sécurité, reçoit donc plusieurs types de mises à jour. Certaines concernent l'agent, d'autres, beaucoup plus fréquentes, les définitions. Or, c'est un fichier de définition qui a provoqué la vaste panne. Comment est-ce possible ?

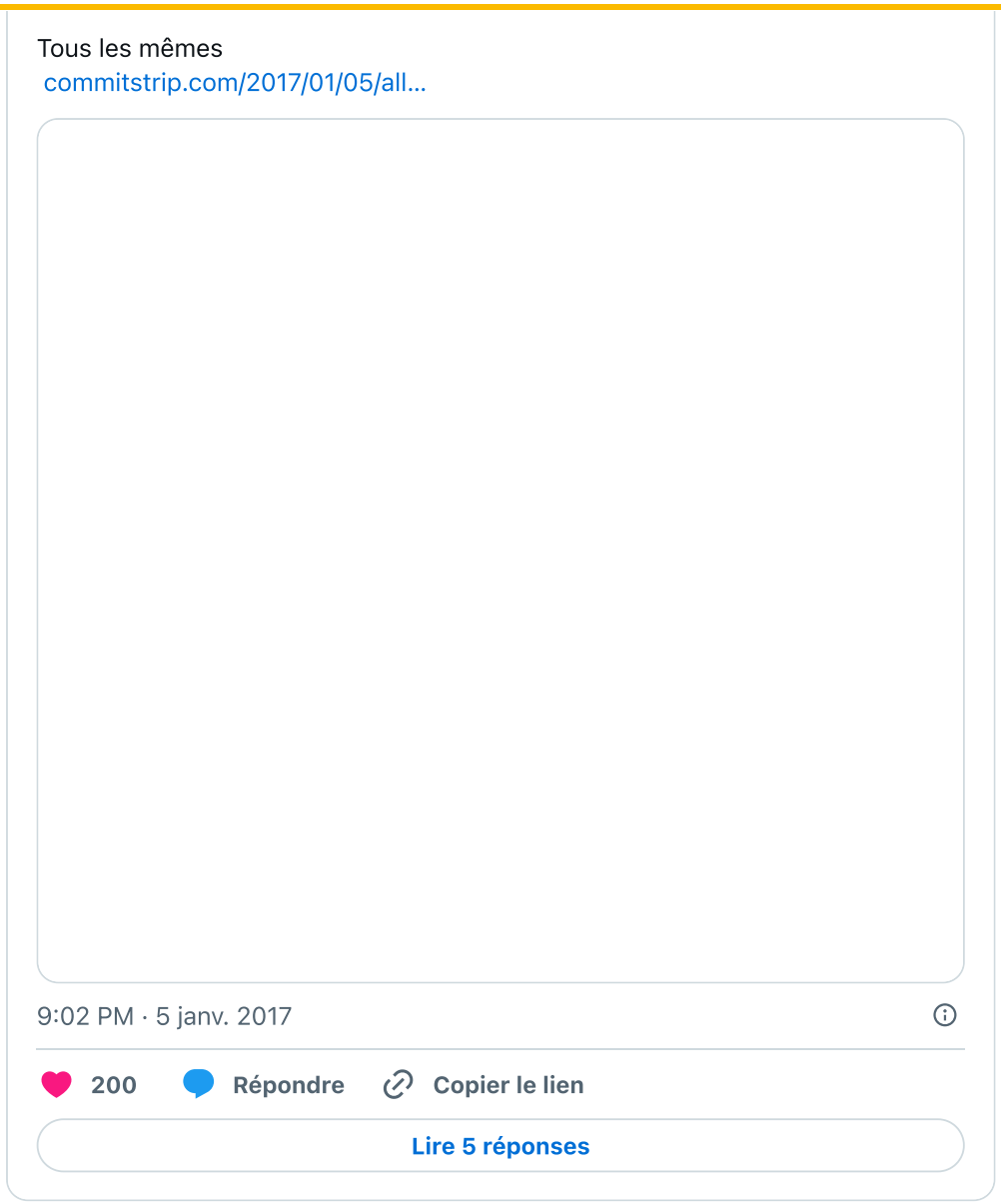
Selon l'expert en cybersécurité Kevin Beaumont, qui a récupéré des fichiers incriminés, tout vient d'un problème de formatage. Le fichier de définition, lorsqu'il est interprété par le pilote, entraine un plantage de ce dernier qui, à son tour, entraine le noyau Windows avec lui.

Pour lui, une chose est sûre : « *Il s'agira de l'incident "cyber" le plus important de tous les temps en termes d'impact, c'est juste un spoiler, tant la récupération est difficile* ».

Plus on en apprend sur les raisons techniques de l'incident, plus la question de la validation s'impose : comment une telle mise à jour a pu passer les tests de qualité (QA) et être validée pour déploiement ?

Car il faut constater l'ampleur de la panne. Au vu du nombre de machines concernées (au strict minimum des dizaines de milliers, partout dans le monde), on peut se demander comment un problème aussi important n'a pas été détecté durant la phase de test. À moins que celle-ci ait été particulièrement légère, voire inexistante.

C'est la question que se pose notamment l'ingénieur Maiko Bossuyt (MaikoB sur X). Il n'est pas le seul, le sujet revient régulièrement sur les réseaux sociaux. CrowdStrike n'a pour le moment rien dit.



La question de la réparation, en revanche, pose toujours un gros problème. Microsoft, sur sa page de statut pour Azure, indique avoir reçu des retours de clients sur le plantage CrowdStrike qui touchait des machines virtuelles Windows ou Windows Server.

Dans le cas des machines virtuelles, les tâches peuvent être automatisées. Selon des clients, redémarrer les machines plusieurs fois (jusqu'à quinze !) donne de bons résultats.

Selon Maiko Bossuyt, avec qui nous nous sommes entretenus, l'explication est simple : le BSOD n'est pas forcément immédiat. Avec un peu de chance, Windows a le temps de se charger et Falcon Sensor de trouver la dernière mise à jour, qui corrige le tir. S'il parvient à la récupérer et l'installer, la machine est tirée d'affaire. « *Ça se joue vraiment à quelques secondes* », ajoute-t-il. L'opération est donc loin de réussir dans tous les cas

La réparation prend beaucoup plus de temps, car il faut intervenir physiquement sur chaque ordinateur et se déplacer dans les datacenters pour les serveurs Windows sans accès IPMI (ou autre). Dans le cadre d'organisations possédant des milliers de machines, l'opération risque de virer au cauchemar. Si BitLocker est actif, il faut en plus avoir la clé de restauration de chaque machine sous la main.

Enfin, précisons que ce n'est pas la première fois que le pilote de Falcon Sensor entraine des problèmes, même si aucun de cette ampleur. Sous Windows, on trouve des cas de plantage similaires en décembre dernier. En avril, on relevait des kernel panics sur Linux.

Signaler une erreur

Commentaires (2) 0

Quelque chose à dire ?

linkin623 Abonné
Aujourd'hui à 18h07

#1

Notre serveur d'identification est tombé, ben heureusement qu'on a le Support sur une plateforme cloud pour répondre aux clients. Par contre faire quoi que soit avec les outils internes c'était mort tout ce matin.

Crowdstrike est au début d'un sacré bordel...

Répondre Réagir

wanou2 Abonné
Aujourd'hui à 18h17

#2

Sur des applications critiques les fichiers de définition passent sans contrôle à priori ?

Répondre Réagir

2