Panne et paralysie mondiale : une mise à jour CrowdStrike provoque des bugs en cascade

SPOF !

Vincent Hermann
Le 19 Juillet à 11h46

Sécurité | 5 min

Une gigantesque panne affecte actuellement de nombreuses structures, y compris de grosses entreprises, des aéroports et des hôpitaux. En cause apparemment, une mise à jour des logiciels de cybersécurité de CrowdStrike. Elle provoque des écrans bleus sur les machines équipées de Windows, ainsi que des redémarrages en boucle.

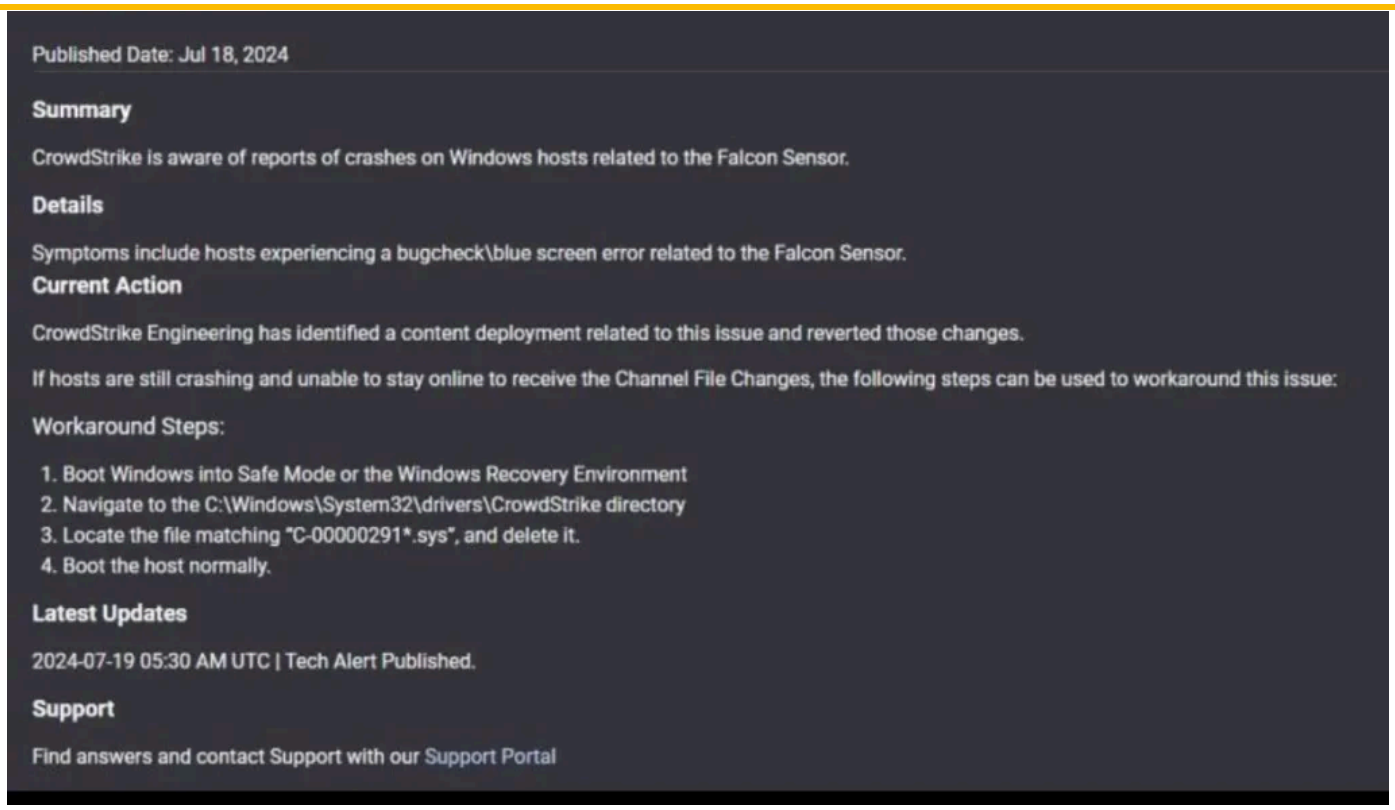
Partout dans le monde, des entreprises et autres structures rapportent être partiellement ou totalement bloquées. Une cyberattaque ? A priori non. Le problème vient d'une mise à jour déployée par CrowdStrike pour son EDR (détection et intervention sur les points de terminaison) Falcon Sensor. Des banques, des aéroports, des hôpitaux, des magasins, des chaines de télévision ou encore des organes de presse sont touchés.

Le symptôme est le même partout : un écran bleu de Windows et un redémarrage du système. Falcon Sensor étant un produit destiné aux entreprises, le grand public n'est pas censé être concerné.

Les exemples sont très nombreux. Parmi les plus retentissants, la bourse de Londres, dont le service de nouvelles « *est actuellement confronté à un problème technique global d'une tierce partie, empêchant la publication de nouvelles sur www.londonstockexchange.com* ». De nombreux aéroports sont touchés, dont ceux de Berlin, Melbourne, Hong-Kong, Prague ou plusieurs en Inde. Aux États-Unis, tous les avions de Delta, United et American Airlines sont cloués au sol.

Citons également les groupes médias ABC aux États-Unis et Sky News au Royaume-Uni, dont les services sont perturbés. Même chose pour les trains au Royaume-Uni.

CrowdStrike indique être au courant de la situation dans une note, qui réclame malheureusement un compte pour la lire.



Sur Reddit, la solution présentée dans la page « cachée » de CrowdStrike est mise en avant. Elle consiste à :

- redémarrer Windows en mode sans échec
- se rendre dans le dosser C:\Windows\System32\drivers\CrowdStrike et à
- y effacer un fichier de type « C-00000291*.sys ».

Après le redémarrage, le problème disparaitrait. Mais, comme indiqué dans de nombreuses réponses sur Reddit : il est presque impossible d'accéder aux machines actuellement. En outre, la solution serait impossible à appliquer sur les machines où BitLocker (solution de chiffrement intégral de Microsoft) est actif.

En France, le CERT vient également de communiquer : « *Le CERT-FR a été informé ce jour d'un incident majeur affectant les systèmes Microsoft Windows disposant de l'EDR CrowdStrike Falcon. Cet incident semble provoquer un écran bleu système entraînant un redémarrage du poste. À ce stade, le CERT-FR n'a pas d'élément indiquant que cet incident est lié à une attaque informatique ». Le Centre ajoute suivre « avec attention les évolutions de cet incident* ». Même son de cloche à l'ANSSI.

La nouvelle pourrait fortement impacter CrowdStrike. Avant même l'incident, l'entreprise voyait son action chuter à cause de divers problèmes de valorisation. Hier, on a également appris que le cabinet d'analyse Redburn Atlantic baissait sa note pour CrowdStrike (et Palo Alto Networks), citant le prix trop élevé de son action et des conditions changeantes sur le marché.

Sur X, le CEO de CrowdStrike, George Kurtz, a fini par prendre la parole :

cyberattaque. Le problème a été identifié, isolé et un correctif a été déployé. Nous renvoyons les clients au portail d'assistance pour connaître les dernières mises à jour et continuerons à fournir des mises à jour complètes et continues sur notre site Web. Nous recommandons en outre aux organisations de s'assurer qu'elles communiquent avec les représentants CrowdStrike via les canaux officiels. Notre équipe est pleinement mobilisée pour assurer la sécurité et la stabilité des clients CrowdStrike. »

De nombreuses questions restent cependant ouvertes. Dont la plus évidente : comment une telle mise à jour a-t-elle pu passer les différentes étapes de vérification ?

Quelques heures auparavant, Microsoft avait des problèmes avec Azure et Microsoft 365, mais ils semblent désormais réglés et sans lien apparent avec les soucis du jour. Ces derniers viennent pour rappel d'une mise à jour de chez CrowdStrike, pas d'un problème chez Microsoft.

Signaler une erreur

Commentaires (95) 0

Quelque chose à dire ?

dvr-x Abonné
Aujourd'hui à 12h00 #1

Dire que j'ai failli partir sur du CrowdStrike avant de m'orienter vers SentinelOne

Ce qui me semble bizarre, c'est que si c'est une mise à jour de l'agent (Falcon sensor ?), ca voudrait dire que toutes ces entreprises déploient les nouvelles versions dès leurs publications en automatique, étonnant.

Répondre Réagir

Bonjour,

Je suis comme toi surpris que des déploiements de ce type se fassent de manière totalement automatiques sans jamais passer par des serveurs de pré-prod de ces compagnies (pour les plus grosses d'entre elles).

Est-ce que cela touche uniquement les serveurs dans le Cloud et/ou on-premises ?

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 12h53 #1.2

> **Kaelhan**
> Bonjour,
>
> Je suis comme toi surpris que des déploiements de ce type se fassent de manière totalement…

D'après ce que j'ai pu lire un peu partout, ça touche tout système Windows sur lequel Crowdstrike est déployé et qui a effectué la mise à jour incriminée.

Répondre Réagir

ZeMeilleur Abonné
Aujourd'hui à 13h00 #1.3

> **Freeben666**
> D'après ce que j'ai pu lire un peu partout, ça touche tout système Windows sur lequel Crowdstrike est déployé et qui a effectué la mise à jour incriminée.

Ce n'est pas vraiment dans les bonnes pratiques de déployer une MàJ sur 100% d'un parc le même jour.
Même en prod, en règle générale, tu fais 1%, 10%, 25%... sur plusieurs lots, en évitant de mettre dans le même lot une machine et son backup identifié.
On ne parle pas de tatie Huguette, on parle de gros groupes avec des SI conséquents quand même :/

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 13h03 #1.4

> **ZeMeilleur**
> Ce n'est pas vraiment dans les bonnes pratiques de déployer une MàJ sur 100% d'un parc le même jour.
> Même en prod, en règle générale, tu fais 1%, 10%, 25%... sur plusieurs lots, en évitant de mettre dan…

Tu prêches un convaincu Faut croire que les bonnes pratiques ne sont pas appliquées par tout le monde.

Répondre Réagir

2

erme Abonné
Aujourd'hui à 14h35 #1.5

> **Kaelhan**

de ce que je comprend c'est un peu comme une maj de définition d'antivirus, donc pas très étonnant que ça soit du déploiement, "global et sans test" (mais ça mériterai peut être une réflexion sur le sujet, trouver un compromis entre déployer une nouvelle définition rapidement pour qu'elle soit dispo le plus vite possible sans prendre ce risque de "bug")

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 14h47 #1.6

> **erme**
> de ce que je comprend c'est un peu comme une maj de définition d'antivirus, donc pas très étonnant que ça soit du déploiement, "global et sans test" (mais ça mériterai peut être une réflexion sur le sujet, trouver un compromis entre déployer une nouvelle définition rapidement pour qu'elle…

Falcon de CrowdStrike n'est pas un simple antivirus à l'ancienne avec simplement une base de signature des virus. C'est un EDR (à moins qu'ils le vendent comme un XDR maintenant, MDR, bref).

Il s'infiltre dans pas mal de pans du système, pour surveiller pas mal de choses, et fait de l'analyse heuristique pour détecter de potentielles attaques.

Pour faire tout ça l'outil a besoin d'un accès au noyau de Windows, probablement réalisé au moyen d'un driver qui tourne en kernel-space. Si celui-ci est buggé, c'est le BSOD quasi assuré.

Répondre Réagir

1

::1
Aujourd'hui à 15h55 #1.7

> **erme**
> de ce que je comprend c'est un peu comme une maj de définition d'antivirus, donc pas très étonnant que ça soit du déploiement, "global et sans test" (mais ça mériterai peut être une réflexion sur le sujet, trouver un compromis entre déployer une nouvelle définition rapidement pour qu'elle…

C'est un ingénieur d'une SSII française qui rencontre un ingénieur Microsoft. Il discutent 'Techniques de développement'.

Le premier dit au second 'Moi, ça me coûte un fric et un temps fou de tester mes logiciels avant de les commercialiser'.

L'ingénieur Microsoft lui réponds 'Tu testes tes logiciels toi-même ? T'as pas de clients pour faire ça ?'

Répondre Réagir

5

bilbonsacquet Abonné
Aujourd'hui à 12h01 #2

Et vive les vendredi

C'est assez affolant qu'une telle panne puisse arriver et la solution de passer par le mode sans échec un peu inquié-

EDIT : concernant la panne Azure, c'est visiblement (encore) lié à un changement de configuration qui a fait tout planté :

https://www.bleepingcomputer.com/news/microsoft/major-microsoft-365-outage-caused-by-azure-configuration-change/

Modifié le 19/07/2024 à 12h03

Répondre Réagir

Patatt Abonné
Aujourd'hui à 12h21 #2.1

Y'en a qui vont passer un bon week-end.

Passer en mode sans échec, c'est la galère, sur une flotte de PC, difficile à faire faire par un utilisateur, et le service IT peu pas physiquement allez sur toutes les machines rapidement.

Répondre Réagir

DikVin Abonné
Aujourd'hui à 12h14 #3

Moi qui est connu cette entreprise hier sur un billet sur développez.com ayant comme sujet que les entreprises ne prennent pas le temps d'évaluer les mises à jour de sécurité

https://securite.developpez.com/actu/360418/Les-entreprises-omettent-la-moitie-du-temps-d-evaluer-la-securite-des-principales-mises-a-jour-des-applications-logicielles-car-cela-est-complique-couteux-et-prend-du-temps-d-apres-CrowdStrike/

Répondre Réagir

3 2 15

empty
Aujourd'hui à 12h21 #3.1

Oui, ça m'a fait sourire. Le timing est parfait

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 12h27 #3.2

Ils auraient dû faire parvenir l'info à leurs clients

Répondre Réagir

xlp Abonné
Aujourd'hui à 12h23 #4

BitLocker, je ne connais pas trop.
Toute solution "full disk encryption" doit pouvoir permettre l'accès offline à mes yeux.
Avec VeraCrypt, pas de problème. Avec LUKS on va un cran plus loin, possible de réinstaller l'OS sur le disque chiffré.
Évidemment pour VeraCrypt, pas leur faute. Et encore, je n'ai jamais essayé, c'est peut-être possible (mais ça me semble douteux).

Répondre Réagir

Oui, avec Bitlocker tu peux toujours saisir la clé manuellement au boot, donc je ne comprend pas la partie de l'article qui indique que Bitlocker gênerait le démarrage en mode sans échec

Répondre Réagir

Dj Abonné #4.2
Aujourd'hui à 12h30

> **Freeben666**
> Oui, avec Bitlocker tu peux toujours saisir la clé manuellement au boot, donc je ne comprend pas la partie de l'article qui indique que Bitlocker gênerait le démarrage en mode sans échec

Tu sais pas faire ça a distance non ?
Donc pour une boite, ça implique un tech qui fait la manipulation sur chaque PC de la flotte (et des gens en présentiel)

Répondre Réagir

1

Freeben666 Abonné #4.4
Aujourd'hui à 12h57

> **Dj**
> Tu sais pas faire ça a distance non ?
> Donc pour une boite, ça implique un tech qui fait la manipulation sur chaque PC de la flotte (et des gens en présentiel)

Chaque employé peut saisir sa propre clé (après que le support la lui a communiquée, bien entendu). Mais de toute façon si la raison de saisir la clé est de pouvoir booter en mode sans échec, je vois mal la plupart des users faire ça...

Le plus simple est de ne pas déployer des mises à jour sur des systèmes de prod sans les tester avant...

Répondre Réagir

Kalsth Abonné #4.3
Aujourd'hui à 12h34

> **Freeben666**
> Oui, avec Bitlocker tu peux toujours saisir la clé manuellement au boot, donc je ne comprend pas la partie de l'article qui indique que Bitlocker gênerait le démarrage en mode sans échec

Tout le monde ne connait pas cette clé, surtout en entreprise

Répondre Réagir

Freeben666 Abonné #4.5
Aujourd'hui à 12h58

> **Kalsth**
> Tout le monde ne connait pas cette clé, surtout en entreprise

En entreprise, les utilisateurs ne sont pas censé connaitre (ni même avoir accès) à cette clé. Elle est communiquée par le support uniquement si nécessaire, et après vérification de l'identité de la personne qui la demande.

Et si le support lui-même n'a pas ses clés, c'est qu'ils se sont loupés quelque part.

Répondre Réagir

eglyn Abonné
Aujourd'hui à 13h08 #4.6

> **Freeben666**
> Oui, avec Bitlocker tu peux toujours saisir la clé manuellement au boot, donc je ne comprend pas la partie de l'article qui indique que Bitlocker gênerait le démarrage en mode sans échec

Car les clés sont stockés sur le controleur de domaine généralement, qui est en carafe lui aussi en BSOD

Répondre Réagir

7

darkjack Abonné
Aujourd'hui à 14h35 #4.15

> **eglyn**
> Car les clés sont stockés sur le controleur de domaine généralement, qui est en carafe lui aussi en BSOD

Quand AD a eu la possibilité de stocker les clefs BT, mon collègue a activé l'option et m'a dit trop cool, plus besoin de les sauvegarder.
Un jour, lors d'une recherche de clef BT dans AD, on constaté qu'à partir d'une date inconnue, AD avait arrêté de les stocker, sans changement de l'option le lui demandant... Étant fan de la technique dite ceinture + bretelles, j'avais continué à les sauvegarder en txt, du moins celles que j'avais généré.
Moralité, méfiez vous du backup AD des clefs BT ;)

Répondre Réagir

5

vexal Abonné
Aujourd'hui à 13h16 #4.7

> **Freeben666**
> Oui, avec Bitlocker tu peux toujours saisir la clé manuellement au boot, donc je ne comprend pas la partie de l'article qui indique que Bitlocker gênerait le démarrage en mode sans échec

Quand tu installes le système, il ne te donnes pas la clé. Il faut penser à aller la chercher et l'enregistrer quelque part.

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 13h19 #4.8

> **vexal**
> Quand tu installes le système, il ne te donnes pas la clé. Il faut penser à aller la chercher et l'enregistrer quelque part.

Vérifie, mais par défaut elle est sauvegardée sur ton compte Microsoft. Ou alors ils ont changé comment ils activent Bitlocker.

Répondre Réagir

> **vexal**
> Quand tu installes le système, il ne te donnes pas la clé. Il faut penser à aller la chercher et l'enregistrer quelque part.

La clé utilisée au quotidien est stockée dans le TPM (et peut-être dans le compte Microsoft aussi s'il y en a un), mais il devrait proposer de sauvegarder quelque part une clé de récupération (qui n'est pas forcément celle utilisée au quotidien mais permet d'accéder aux données manuellement) ?

En tout cas il le proposait quand j'avais testé, dans un fichier qu'on garde ensuite où on veut, mais j'ai pas testé de le faire à l'installation.

Répondre Réagir

eglyn Abonné #4.10
Aujourd'hui à 13h32

> **Inodemus**
> La clé utilisée au quotidien est stockée dans le TPM (et peut-être dans le compte Microsoft aussi s'il y en a un), mais il devrait proposer de sauvegarder quelque part une clé de récupération (qui n'est pas forcément celle utilisée au quotidien mais permet d'accéder aux données manuellement) ?…

Il te propose de l'imprimer, soit de la stocker dans un périphérique amovible.
Sauf si tu es sur un réseau entreprise, où elle est directement stockée dans le contrôleur de domaine.

Répondre Réagir

dvr-x Abonné #4.11
Aujourd'hui à 13h54

> **eglyn**
> Il te propose de l'imprimer, soit de la stocker dans un périphérique amovible.
> Sauf si tu es sur un réseau entreprise, où elle est directement stockée dans le contrôleur de domaine.

En particulier, la clef est stocké sur le compte MS, MS propose aussi de l'enregistrer ou l'imprimer.

En entreprise, c'est un faux problème, la clef doit remonter sur le contrôleur de domaine, comme dit plus haut.
Le même contrôleur qui est hautement à risque, donc rarement seul doit surement très bien être backupé. Donc si le seul DC est touché, il faut taper dans les sauvegardes.
Mais vu la taille des groupes concernés, ce serait juste dément de n'avoir qu'un DC et d'y déployer des MAJ d'agent en auto dès leur mise à dispo. Surtout que dans le cas présent, je pense même que certains ont les clés dans Azure AD…

En tous cas ca pourrait bien finir en procès cette affaire.

Modifié le 19/07/2024 à 13h56

Répondre Réagir

eglyn Abonné #4.12
Aujourd'hui à 13h57

> **dvr-x**
> En particulier, la clef est stocké sur le compte MS, MS propose aussi de l'enregistrer ou l'imprimer.
>
> En entreprise, c'est un faux problème, la clef doit remonter sur le contrôleur de domaine, comme di…

Et ben crois le ou pas, tous les DC étaient down, c'est Crowdstrike qui décide les maj, personne n'a la main dessus…

Modifié le 19/07/2024 à 13h57
Répondre Réagir

dvr-x Abonné
Aujourd'hui à 14h19 #4.13

> **eglyn**
> Et ben crois le ou pas, tous les DC étaient down, c'est Crowdstrike qui décide les maj, personne n'a la main dessus...
> ...

En effet, c'est des grands malades alors !!

Mais ca ne change pas qu'ils doivent pouvoir utiliser leurs backup de DC, par contre forcément ca demande un peu de temps... Au final, quoi qu'on en dise, mettre son AD en Hybride MS entra, c'est pas déconnant au final.
Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 14h31 #4.14

> **eglyn**
> Et ben crois le ou pas, tous les DC étaient down, c'est Crowdstrike qui décide les maj, personne n'a la main dessus...
> ...

La question est : qui déploie un outil qui fait des màj auto sans aucun contrôle en prod ? Si j'avais proposé ça à notre admin système, j'aurais été très mal reçu, je peux te le garantir

"Ils ont balancé leur maj sur 100% des machines sur la planètes, c'est juste WTF..."

Je savais pas que CrowdStrike était installé sur les ordinateurs du monde entier !!! Et ils se sont pas encore pris de procès pour position monopolistique ?!

"c'est Crowdstrike qui décide les maj, personne n'a la main dessus..."

A priori les clients avaient la main pour décider de ne pas installer sur leur prod un outil sur lequel ils n'ont aucun contrôle... (je parle des décideurs, pas des admins sys qui vont subir la crise)
Modifié le 19/07/2024 à 15h23
Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 15h22 #4.16

> **eglyn**
> Et ben crois le ou pas, tous les DC étaient down, c'est Crowdstrike qui décide les maj, personne n'a la main dessus...
> ...

Modifié le 19/07/2024 à 15h22
Répondre Réagir

Je vais être le premier à dire que la sécurité c'est primordial, notamment faire rapidement les mises à jour, mais rien ne doit être poussé en prod sans contrôle !

Répondre Réagir

2

eglyn Abonné
Aujourd'hui à 13h07 #5.1

Et un vendredi en plus !!

Répondre Réagir

4

LostSoul Abonné
Aujourd'hui à 15h00 #5.2

Je vais te dire: tout le monde :p Suffit de voir le nombre de boîtes impactées.
Le truc c'est que le Falcon Agent c'est un peu comme un "antivirus" donc c'est CrowdStike qui "pousse" les maj et pas le client qui les "tire". Quand ça marche bien c'est très bien, quand ça foire ... ça foire très bien aussi :p

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 15h16 #5.3

> **LostSoul**
> Je vais te dire: tout le monde :p Suffit de voir le nombre de boîtes impactées.
> Le truc c'est que le Falcon Agent c'est un peu comme un "antivirus" donc c'est CrowdStike qui "pousse" les maj et pas le client qui les "tire". Quand ça marche bien c'est très bien, quand ça foire .....

Pourquoi le fait que ce soit un EDR voudrait forcément dire que le client ne doit avoir aucun contrôle sur le déploiement des mises à jour ? Sur un environnement desktop, pourquoi pas, mais clairement sur des serveurs c'est inacceptable. Surtout qu'à priori là c'est pas juste une mise à jour des signatures de virus et/ou règles de détection heuristique, mais une mise à jour du moteur de l'EDR lui-même (vu qu'un fichier sys est concerné, je dirais le "pilote" qu'ils utilisent pour s'interfacer avec le kernel).

Répondre Réagir

1

empty
Aujourd'hui à 12h24 #6

CrowdStrike : -14% en pré-market à la Bourse
Microsoft : -2%

Microsoft a une part de responsabilité importante dans ce fiasco. La solution manuelle de restauration n'est pas au niveau attendu pour une telle entreprise.

Répondre Réagir

1 1

Répondre Réagir

Thanger Abonné
Aujourd'hui à 12h39 #6.2

> **Freeben666**
> En quoi c'est la faute de MS si les boites n'ont pas de PRA ?

C'est la faute de MS d'avoir un OS qui plante aussi violemment juste parce qu'un outil est défectueux.

Répondre Réagir

3

Freeben666 Abonné
Aujourd'hui à 13h00 #6.4

> **Thanger**
> C'est la faute de MS d'avoir un OS qui plante aussi violemment juste parce qu'un outil est défectueux.

On parle d'un outil qui va toucher au kernel. N'importe quel OS va planter sévèrement si un outil buggé va foutre le bordel dans le noyau. Apparemment tu n'as jamais vu de kernel panic sous Linux, mais je peux te garantir que c'est bien réel.

Répondre Réagir

11

fred42 Abonné
Aujourd'hui à 13h23 #6.6

> **Thanger**
> C'est la faute de MS d'avoir un OS qui plante aussi violemment juste parce qu'un outil est défectueux.

Je ne suis pas certain que ça soit la faute de Microsoft.

L'outil surveille un peu tout ce qui se passe sur les machines :

*Les adresses locales et externes auxquelles l'hôte est connecté
Tous les comptes utilisateur qui se sont connectés sur site et à distance
Un résumé des modifications survenues au niveau des clés ASP, des fichiers exécutables et de l'utilisation des outils d'administration
L'exécution des processus
Des informations récapitulatives et détaillées sur l'activité réseau associée aux processus, notamment les requêtes DNS, les connexions et les ports ouverts
La création de fichiers d'archives, notamment aux formats RAR et ZIP
L'utilisation de supports amovibles*

Pour pouvoir faire ça, il faut des droits importants au niveau de la machine. Comme la solution pour supprimer le problème est de supprimer un fichier .sys, on en conclut qu'ils ont développé un driver Windows faisant cela et que c'est lui qui génère un BSOD. De toute façon, il me semble qu'il n'y a que les drivers qui génèrent des BSOD.
Je ne suis plus/pas trop au courant de ce qui est exigé de la part de Microsoft pour la certification des drivers et c'est peut-être là la faiblesse chez eux, mais un driver de ce type (qui ne gère pas forcément du matériel, c'est un peu complexe à qualifier pour Microsoft ; c'est donc à celui qui le fournit de le qualifier sérieusement.

yl
Aujourd'hui à 14h10

#6.8

> **fred42**
> Je ne suis pas certain que ça soit la faute de Microsoft.
>
> L'outil surveille un peu tout ce qui se passe sur les machines :...

"Je ne suis plus/pas trop au courant de ce qui est exigé de la part de Microsoft pour la certification des drivers...".

Je ne sais pas non plus, mais qqsoit la couverture de test (jamais 100%) simplement avoir prévu un mécanisme de probation (par exemple ne pas avoir une poignée de redémarrages impromptus consécutifs suite à un problème kernel bloquant) qui, s'il n'est pas atteint, va provoquer un retour à l'état antérieur à la dernière mise à jour de manière automatique c'est pas non plus le Pérou! En fait, dans l'embarqué tout le monde fait cela...

Modifié le 19/07/2024 à 14h11

Répondre Réagir

1

empty
Aujourd'hui à 12h40

#6.3

> **Freeben666**
> En quoi c'est la faute de MS si les boites n'ont pas de PRA ?

Le SPOF qui met en carafe l'OS complet, c'est une responsabilité de Microsoft.
Tout comme l'étaient les BSOD à cause des drivers mal codés en 1998.

L'impréparation des services IT est également en cause oui, et bien évidemment CrowdStrike en 1er lieu.

Répondre Réagir

2 2

Freeben666 Abonné
Aujourd'hui à 13h02

#6.5

> **empty**
> Le SPOF qui met en carafe l'OS complet, c'est une responsabilité de Microsoft.
> Tout comme l'étaient les BSOD à cause des drivers mal codés en 1998.
> ...

Non, le SPOF ici c'est Crowdstrike. Le problème c'est les gars qui déploient des outils qui touchent au noyau, et ensuite n'assure aucun contrôle sur les mises à jour, les poussant allègrement en prod sans contrôle.

Répondre Réagir

fred42 Abonné
Aujourd'hui à 13h25

#6.7

> **Freeben666**
> Non, le SPOF ici c'est Crowdstrike. Le problème c'est les gars qui déploient des outils qui touchent au noyau, et ensuite n'assure aucun contrôle sur les mises à jour, les poussant allègrement en prod sans contrôle.

jour.

Répondre Réagir

aware2 Abonné
Aujourd'hui à 15h34 #6.13

> **fred42**
> Je pense que beaucoup n'avaient pas conscience de ce qu'ils installaient.
>
> Remarque : comme c'est une solution cloud, je ne suis même pas sûr qu'il soit possible de gérer soi…

Alors, d'expérience dans ma boite, comme on a déjà été confronté a des problèmes de compatibilité entre Crowdstrike et certains outils métiers, l'admin a la possibilité de bloquer la maj de l'EDR, de downgrader un client par exemple, de laisser xxx postes clients dans une certaine version, etc.

Répondre Réagir

yl
Aujourd'hui à 14h23 #6.9

> **Freeben666**
> Non, le SPOF ici c'est Crowdstrike. Le problème c'est les gars qui déploient des outils qui touchent au noyau, et ensuite n'assure aucun contrôle sur les mises à jour, les poussant allègrement en prod sans contrôle.

C'est en effet le problème de base, mais les contrôles ne devraient être que la 1ère lame du rasoir. Un mécanisme de probation suite à MAJ assurant au besoin un retour automatique à l'état antérieur devrait être la seconde.

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 14h40 #6.10

> **yl**
> C'est en effet le problème de base, mais les contrôles ne devraient être que la 1ère lame du rasoir.
> Un mécanisme de probation suite à MAJ assurant au besoin un retour automatique à l'état antérieur devrait être la seconde.

Pourquoi ce serait à MS de prévoir ce type de mécanisme ? Si des gens veulent aller bidouiller le noyau, c'est à eux de prendre leurs responsabilités.

Depuis pas mal d'années, les seuls vrais moyen d'avoir des BSOD c'est soit un problème matériel, soit un soft buggé avec accès noyau, souvent des drivers (et encore, de nos jours beaucoup de drivers ne tourne même plus en kernel-space, mais en user-space, et d'ailleurs ça a gueulé quand MS a mis ça en place).

SI sur un système Linux tu vas modifier le système pour charger un module noyau buggé qui cause des kernel panic, il va pas se retirer tout seul non plus. Il va falloir booter en init 1 et virer le module. Et à aucun moment ce ne serait la faute des dev du kernel Linux, juste du dev du module et du gars qui l'a déployé.

Répondre Réagir

Kara(Wo)Man Abonné
Aujourd'hui à 14h46 #6.11

> **empty**

- Les services IT sont le plus souvent dépendants de la direction de leur structure qui peut ne pas financer les infras nécessaires à avoir un PRA, voire un PCA.
- Un PRA n'est pas un PCA ; dans une telle situation, la reprise d'activité est quasi garantie à moyen terme et "quelques heures/jours" ça peut être un risque accepté par la direction.
- Même un bon PRA/PCA peut ne pas suffire dans une telle situation ; typiquement, si la sauvegarde est gérée par une infra MS (avec Veam ou une autre solution), rétablir les sauvegardes peut s'avérer compliqué si le système est dans une salle distante (voire nécessitant un processus avec des accréditations et des contrôles qui peuvent être contraints eux-mêmes pas la situation).
- Normalement, les clés de déchiffrement des serveurs critiques doivent être dans un coffre fort physique ; en pratique, c'est rarement le cas (ou il peut y avoir des soucis d'accès au coffre, surtout en période estivale ou de mid-year)
- Ici, j'ai envie de dire que le responsable est uniquement CrowdStrike. On peut imputer une partie de la responsabilité à MS pour ne pas avoir de mécanisme d'isolement, mais les solutions d'EDR sont parfois implantées dans le système avec des stratégies similaires à des rootkits, donc on est peut-être dans une situation où l'OS n'est pas en mesure de lever correctement les bonnes barrières (et peut-être que le BSOD/reboot est justement la seule barrière qui reste à l'OS pour se protéger et protéger le système)

Répondre Réagir

1

theoldscudo Abonné
Aujourd'hui à 15h32

#6.12

> **Kara(Wo)Man**
> - Les services IT sont le plus souvent dépendants de la direction de leur structure qui peut ne pas financer les infras nécessaires à avoir un PRA, voire un PCA.
> - Un PRA n'est pas un PCA ; dans une telle situation, la reprise d'activité est quasi garantie à moye…

Et même si PRA / PCA, je vois bien d'ici que toutes les machines y compris les env PRA ont le même EDR... on ne va pas payer 2 solutions... donc quand l'EDR fait planter l'OS, ça marche aussi sur les serveurs PRA qui ont mangé la même mise à jour :)

Modifié le 19/07/2024 à 15h32

Répondre Réagir

Kara(Wo)Man Abonné
Aujourd'hui à 18h08

#6.14

> **theoldscudo**
> Et même si PRA / PCA, je vois bien d'ici que toutes les machines y compris les env PRA ont le même EDR... on ne va pas payer 2 solutions... donc quand l'EDR fait planter l'OS, ça marche aussi sur les serveurs PRA qui ont mangé la même mise à jour :)…

Absolument. Après, on peut remettre en question beaucoup de choses en lien avec cette mode des EDR supervisés par des tiers ; que ce soit comme ici avec une stratégie de mise à jour non contrôlée par les clients, mais aussi et surtout sur le fait qu'on laisse une entreprise extérieure avec un accès de supervision à l'ensemble du parc, y compris des services stratégiques. Et que le modèle même de l'EDR décentralisé implique l'envoi de données vers l'extérieur pour faire de l'analyse.
C'est problématique à bien des niveaux (sécurité de l'infra, sécurité des données de l'entreprise, problèmes relatifs à la vie privée des employés...).
Les solutions d'EDR internalisables sont moins courantes (et nécessitent une équipe de supervision connectée de façon permanente, ce que les entreprises ont du mal à assumer).

Répondre Réagir

Le sous-titre 

Répondre Réagir

4

Ey Abonné
Aujourd'hui à 12h28 #8

CrowdStrike c'est juste un antivirus avec des fonctions un poil avancées (genre heuristique sur les paquets réseaux) en fait ?
Ça concerne uniquement les clients ou les Windows servers sont aussi touchés ?

Répondre Réagir

segundo Abonné
Aujourd'hui à 12h37 #8.1

De ce que j'ai pu en lire jusque-là, les clients et les serveurs sont impactés. :/

Répondre Réagir

1

eglyn Abonné
Aujourd'hui à 13h06 #8.2

ça concerne toutes les machines Windows, que ce soit serveur ou workstation

Répondre Réagir

dvr-x Abonné
Aujourd'hui à 14h00 #8.3

> **eglyn**
> ça concerne toutes les machines Windows, que ce soit serveur ou workstation

En même temps, le serveur est un client Windows comme un autre, la différence c'est juste le prix de la licence 
Généralement tu balances juste des stratégies différentes sur Desktop / Laptop / Serveur..

Répondre Réagir

theoldscudo Abonné
Aujourd'hui à 14h22 #8.4

non c'est pas un antivirus, mais un EDR c'est différent.
l'EDR fait de l'analyse comportementale pour remonter des actions suspectes sur un PC (genre ouvrir tous les fichiers excel et remplacer le contenu par autre chose en 3sec), exécuter des scripts en admin allant télécharger du code sur internet etc..

Répondre Réagir

Ey Abonné
Aujourd'hui à 16h07 #8.5

> **theoldscudo**

Justement c'est pas comme les options "heuristique" des antivirus (qui existent depuis plus de 10 ans) ?
Je sais aussi que mon Sophos (pro) par exemple à une partie EDR.
Bref les différences me paraissent pas super claires.

Répondre Réagir

theoldscudo Abonné
Aujourd'hui à 16h34 #8.6

> **Ey**
> Justement c'est pas comme les options "heuristique" des antivirus (qui existent depuis plus de 10 ans) ?
> Je sais aussi que mon Sophos (pro) par exemple à une partie EDR....

Les heuristiques ont plus de 20 ans même :)
Pour l'EDR, c'est probablement une évolution "spécialisée" de cette fonction tout en ajoutant de de nouveaux services.

on tend à séparer les fonctions antivirus et annexes pour mieux vendre plusieurs produits :)

trouvé dans les liens sources de wiki

> Antivirus and Anti-malware: Traditional and next-gen solutions to detect and eliminate malicious software.

> Endpoint Detection and Response (EDR): Tools that provide continuous monitoring and response to advanced threats.

ceci dit il n'y a pas que Crowstrike dans le monde de l'EDR... Qualys, fireeye, même Trend

Répondre Réagir

xillibit Abonné
Aujourd'hui à 16h38 #8.7

> **Ey**
> Justement c'est pas comme les options "heuristique" des antivirus (qui existent depuis plus de 10 ans) ?
> Je sais aussi que mon Sophos (pro) par exemple à une partie EDR....

C'est expliqué ici : https://www.orangecyberdefense.com/fr/solutions/protection-des-mobiles-et-des-endpoints/endpoint-detection-and-response-pourquoi-ledr un EDR réagit avant que le virus arrive sur la machine et peut détecter l'exploitation de commandes en powershell

Répondre Réagir

Freeben666 Abonné
Aujourd'hui à 16h44 #8.8

> **xillibit**
> C'est expliqué ici : https://www.orangecyberdefense.com/fr/solutions/protection-des-mobiles-et-des-endpoints/endpoint-detection-and-response-pourquoi-ledr un EDR réagit avant que le virus arrive sur la machine et peut détecter l'exploitation de commandes en powershell

C'était moins le cas avec les AV "à l'ancienne" qui se contentaient de scanner les fichiers et comparer leurs signature avec une base de données, mais avec la multiplication des méthodes de détection, et les actions de réponse aux détections, les outils interagissent de plus en plus avec le noyau pour récupérer les infos dont ils ont besoin, et effectuer les actions de blocage des menaces.

Répondre Réagir

Ey Abonné
Aujourd'hui à 16h45 #8.9

> **xillibit**
> C'est expliqué ici : https://www.orangecyberdefense.com/fr/solutions/protection-des-mobiles-et-des-endpoints/endpoint-detection-and-response-pourquoi-ledr un EDR réagit avant que le virus arrive sur la machine et peut détecter l'exploitation de commandes en powershell

Merci de vos réponses, je vais checker vos liens ;)

Répondre Réagir

Bill2
Aujourd'hui à 12h28 #9

Moi ce qui mon gonfle, c'est le MS baching alors que MS n'est pas en cause ...
Coucou @sebsauvage https://sebsauvage.net/links/?v1ki1w

Répondre Réagir

6

Thanger Abonné
Aujourd'hui à 12h39 #9.1

Sauf que Windows ne devrait pas planter aussi violemment juste parce qu'un outil est défectueux.
Même si MS n'est pas la cause principale, Windows montre une fragilité là.

Répondre Réagir

2 3

Bill2
Aujourd'hui à 13h18 #9.2

> **Thanger**
> Sauf que Windows ne devrait pas planter aussi violemment juste parce qu'un outil est défectueux.
> Même si MS n'est pas la cause principale, Windows montre une fragilité là.

Ben ... quand l'outil touche au noyau, au bout d'un moment, ça peut plus être contrôlé par MS ...
Comme déjà dit plus haut, c'est pas spécifique à Win, les Kernel Panic sous Linux, ça existe aussi ...

Répondre Réagir

7

yl
Aujourd'hui à 13h52 #9.3

> **Bill2**

Cela arrive sous Linux, mais à part ceux qui développent des modules noyau qui en voit dans la vraie vie, même si chez Microsoft cela est tout de même devenu rare comparé au passé (ils ne pouvaient que faire mieux, ceci dit)?

Tout ce qui remonte upstream (l'immense majorité de ce qui existe) est quand même bien contrôlé et au niveau source car c'est une boite-blanche, pas juste du test comme dans un modèle boite-noire/sources-fermés.

Certes, il est possible de coder et même distribuer (tant qu'on n'utilise pas du EXPORT_SYMBOL_GPL) ses modules noyau fermés pour Linux, mais on a alors un joli "kernel tained" dans le tampon de message au boot et bon courage pour obtenir de l'aide avec cela! Ce sera demerden zizich...

Modifié le 19/07/2024 à 13h52

Répondre Réagir

bilbonsacquet Abonné

Aujourd'hui à 13h56

#9.4

> **Bill2**
> Ben ... quand l'outil touche au noyau, au bout d'un moment, ça peut plus être contrôlé par MS ...
> Comme déjà dit plus haut, c'est pas spécifique à Win, les Kernel Panic sous Linux, ça existe aussi ...

C'est pour ce genre de choses qu'Apple n'autorise plus les modules kernel tiers depuis plusieurs années maintenant, mais autorisent uniquement les extensions en "user land" :

https://support.apple.com/fr-fr/guide/deployment/depa5fb8376f/web

Donc si c'est la faute à Microsoft de continuer à permettre ce genre de choses… Là pour des raisons de sécurité (ou contre la triche pour les jeux vidéos).

Modifié le 19/07/2024 à 13h58

Répondre Réagir

1 1

dvr-x Abonné

Aujourd'hui à 14h15

#9.5

> **bilbonsacquet**
> C'est pour ce genre de choses qu'Apple n'autorise plus les modules kernel tiers depuis plusieurs années maintenant, mais autorisent uniquement les extensions en "user land" :
> ...

Drôle de raisonnement. Si une voiture permet de dépasser des limitations de vitesse, ce n'est pas parce que tu te mets dans un mur à 180km que ce sera de la faute du constructeur.

Alors oui, on peut aussi tout bloquer tout interdire, ca limite les risques.

Et clairement, j'ai du mal à comprendre cette notion de toute de suite comparer à Linux ou Mac OS, comme si ces deux n'avaient pas aussi leurs propres problèmes. Et clairement si Mac OS avait 78% de PDM sur son domaine, Apple découvrirai plein de problématiques et ferait surement des choix différents, qui sait..

Modifié le 19/07/2024 à 15h08

Répondre Réagir

tomdom Abonné

Aujourd'hui à 14h24

#9.7

> parce que tu te mets dans un mur à 180km que ce sera de la faute du constructeur.
> ...

180€, il n'est pas cher le mur ... ou c'est un tout petit mur

Répondre Réagir

dvr-x Abonné
Aujourd'hui à 15h08 #9.12

> **tomdom**
> 180€, il n'est pas cher le mur ... ou c'est un tout petit mur

En effet, merci j'ai corrigé.

Répondre Réagir

yl
Aujourd'hui à 14h33 #9.9

> **dvr-x**
> Drôle de raisonnement. Si une voiture permet de dépasser des limitations de vitesse, ce n'est pas parce que tu te mets dans un mur à 180km que ce sera de la faute du constructeur.
> ...

"un mur à 180€"? Pas cher ton maçon!

Rappel historique:
1) Billy-Bug-Gates au Comdex 1998:

"Si General Motors avait eu la même progression technologique que l'industrie informatique, nous conduirions aujourd'hui des autos coûtant 25 dollars et qui parcourraient 1000 miles avec un seul gallon d'essence."

2) Réplique du PDG d'alors de GM:

"Si General Motors avait développé sa technologie comme Microsoft, les voitures que nous conduirions aujourd'hui auraient les propriétés suivantes :
-Votre voiture aurait un accident sans raison compréhensible 2 fois par jour.
-Chaque fois que les lignes blanches seraient repeintes, il faudrait racheter une nouvelle voiture.
-Occasionnellement, une auto quitterait l'autoroute sans raison connue [1]. Il faudrait simplement l'accepter, redémarrer l'auto et reprendre la route.
-Parfois, lors de manoeuvres particulières, comme par exemple prendre une courbe a gauche, l'auto ferait un simple tout droit puis refuserait de repartir. Pour cela, il faudrait procéder à un échange standard du moteur.
-Les autos ne seraient livrées qu'avec un seul siège, car il faudrait choisir entre "Car95" et "CarNT". Chaque siège supplémentaire devrait être commandé à l'unité.
-Macintosh développerait des voitures fonctionnant à l'énergie solaire, fiable, cinq fois plus rapides et deux fois plus légères. Mais elles ne pourraient emprunter que 5% des routes.
-Les témoins d'huile, de température et de batterie seraient remplacés par un unique témoin "Défaillance Générale". Les sièges exigeraient que chaque passager ait la même taille et le même poids.
-L'airbag demanderait "Êtes-vous sûr ?" avant de s'ouvrir. Occasionnellement la condamnation centralisée de la voiture se bloquerait. Vous ne pourriez alors la rouvrir qu'au moyen d'une astuce, comme par exemple simultanément tirer la poignée de porte, tourner la clé dans la serrure et d'une autre main attraper l'antenne radio.
-General Motors vous forcerait à acheter avec chaque voiture un jeu de cartes routières Deluxe de la société Rand McNally (depuis peu filiale de GM), même lorsque vous ne souhaitez pas ou n'avez pas besoin de ces cartes. Au cas ou vous ne prendriez pas cette option, la voiture roulerait 50% moins vite (au mieux). A cause de cela, GM deviendrait une

-Enfin, il faudrait appuyer sur le bouton "Démarrer" pour stopper le moteur."

Bon, vu ce que deviennent les bagnoles avec Tesla qui fait de véritables dumb-phones sur roues... les temps changent! Ta bagnole te mettra toute seule dans le mur, idéalement sans te laisser une chance (qui peut se jouer en quelques dixièmes de secondes) de reprendre la main.

Répondre Réagir

1 4

dvr-x Abonné
Aujourd'hui à 15h10 #9.13

> **yl**
> "un mur à 180€"? Pas cher ton maçon!
>
> Rappel historique:...

C'est juste un troll qui répond a un autre troll. Mais j'ai bien aimé la réponse quand même ;)

Répondre Réagir

millman42 Abonné
Aujourd'hui à 14h32 #9.8

> **bilbonsacquet**
> C'est pour ce genre de choses qu'Apple n'autorise plus les modules kernel tiers depuis plusieurs années maintenant, mais autorisent uniquement les extensions en "user land" :
> ...

Ce n'est pas comparable, Apple supporte un nombre limité de machines.
La plupart des autres OS (Windows, Linux et autre) sont plus permissifs sur ce que tu peux installer, mais cela implique d'être plus responsable sur ce qu'on installe.

Répondre Réagir

bilbonsacquet Abonné
Aujourd'hui à 14h39 #9.10

> **millman42**
> Ce n'est pas comparable, Apple supporte un nombre limité de machines.
> La plupart des autres OS (Windows, Linux et autre) sont plus permissifs sur ce que tu peux installer, mais cela implique d'être plus responsable sur ce qu'on installe.

Vu la cata d'aujourd'hui, il y a de grandes chances que Microsoft durcisse le ton sur les modules kernel…

Répondre Réagir

Wosgien Abonné
Aujourd'hui à 14h51 #9.11

> **millman42**

C'est clair, ils doivent pouvoir créer une image OS par modèle supporté chez Apple. Ca fera quoi? 100, 200 images?

Répondre Réagir

eliumnick #9.6
Aujourd'hui à 14h20

J'ai entendu l'info sur RFI : "panne informatique mondiale en cause microsoft met à jour un antivirus"

Répondre Réagir

1

swiper Abonné #10
Aujourd'hui à 12h45

C'est là que le déploiement par lot est intéressant pour éviter ces problématiques.
N'empêche que CrowdStrike qui ne test pas ses produits c'est complétement fou !
Les conditions pour que la panne survienne ne semblent pas être si complexes que ça, ce qui rend la situation encore plus dommageable pour l'entreprise de l'EDR.

La communication du PDG me semble vraiment pas super. Préciser que c'est dans une seule mise à jour, sonne comme un "On reste bon puisque ça n'arrive que sur une mise à jour".

Répondre Réagir

1

eglyn Abonné #11
Aujourd'hui à 13h05

C'était la surprise du matin chez nous, et évidemment pas possible de faire une automation, donc mode sans echec / suppression fichier alakon à la main sur chaque serveur...

Et on est content de pas avoir Crowdstrike sur nos PC, uniquement sur les serveurs...

Bon, on va devoir changer d'EDR en tout cas, ils vont pas survivre à cela

Modifié le 19/07/2024 à 13h05

Répondre Réagir

eglyn Abonné #12
Aujourd'hui à 13h13

ils le disent sur leur site en tout cas, il fallait juste inclure leur EDR dans la liste

Répondre Réagir

10

HumpfHumpf Abonné
Aujourd'hui à 13h55 #12.1

Et ils ont pourtant des bonnes pratiques pour la gestion des patches

Répondre Réagir

::1
Aujourd'hui à 15h50 #12.2

ça s'appelle faire un perfect

Répondre Réagir

lexiii Abonné
Aujourd'hui à 13h20 #13

Ce KO mondial met en lumière que l'on mets tout nos oeufs dans le même panier. Si on avait plus de diversité de système, le KO serait moins impactant.

On voit les limites d'un réseau homogène. C'est tout ou rien. On diversifie ou on utilise le meêm produit pour tout

Répondre Réagir

MisterDams Abonné
Aujourd'hui à 14h05 #13.1

Homogène faut pas abuser, y'a aussi tout un tas de services qui continuent leur vie. Ceux sous Linux, ceux qui utilisent d'autres solutions de sécurité... Et globalement, on a de plus en plus de déploiements par vagues justement pour éviter ça (Android, Windows, Tesla, etc.).

Sans minimiser le raté monumental de CrowdStrike sur ce coup, qui doit bien faire payer cher sa solution, dans le cas d'une protection ~~antivirus~~ EDR, on peut aussi considérer qu'un déploiement rapide est parfois nécessaire. Une fois que t'as identifié une menace, difficile de se dire qu'on va attendre 3 mois pour déployer sur l'ensemble des postes protégés !
Évidemment, ça n'empêche pas que le truc doit être testé avant.

Modifié le 19/07/2024 à 14h50

Nioniotte
Aujourd'hui à 13h55
#14

Nous on est bloqué depuis ce matin au boulot. Déjà qu'il y a quelques semaines, CrowdStrike provoquait des monstres ralentissement sur les PC et qu'il fallait surtout pas redémarrer le PC sinon c'était pire...

Répondre Réagir

SebGF Abonné
Aujourd'hui à 14h05
#15

Au moins, c'est un EDR efficace ! Une machine tankée est une machine sécurisée.

Répondre Réagir

18

dvr-x Abonné
Aujourd'hui à 15h12
#15.1

Répondre Réagir

iFrancois Abonné
Aujourd'hui à 14h24
#16

Ca me rappelle le Bitdefender Epic Fail of 2010 tout ça

Répondre Réagir

LostSoul Abonné
Aujourd'hui à 14h57
#17

Une bonne heure pour "patcher" les serveurs ce matin Vive l'IT
Et oui, on se demande comment un truc pareil a pu passer ...

Répondre Réagir

fdorin Abonné
Aujourd'hui à 14h59
#18

Pour celles et ceux qui pensent que Windows c'est de la merde et ne devrait pas planter sans vraiment savoir comment Crowdstrike s'immisce dans le système, je vous invite à voir ce qui se passe sous Linux :
- https://access.redhat.com/solutions/7068083
- https://forums.rockylinux.org/t/crowdstrike-freezing-rockylinux-after-9-4-upgrade/14041

Bref, Linux, c'est aussi de la merde codé avec les pieds ^^

(ce troll est sponsorisé par Trolldi, le jour où le troll est permis \o/)

Répondre Réagir

cayan Abonné
Aujourd'hui à 15h57
#18.1

Faudra expliquer ça à Mr Mélenprout ...

« Microsoft équipe des armes françaises et le ministère de la Défense. Tout va bien ? Vous comprenez enfin ce que veut dire indépendance nationale et souveraineté ? », s'est par exemple insurgé Jean-Luc Mélenprout sur X

Répondre Réagir

fdorin Abonné
Aujourd'hui à 16h02
#18.2

> **cayan**
> Faudra expliquer ça à Mr Mélenprout ...
>
> « Microsoft équipe des armes françaises et le ministère de la Défense. Tout va bien ? Vous…

Nan mais si les politiques si connaissaient :
1) ça se saurait
2) on n'aurait jamais eu le pare feu OpenOffice

[edit]
Pour être sérieux 2min (promis, pas plus) :
- une solution souveraine n'aurait pas empêché ce type d'incident de survenir
- un problème survenant n'aurait alors touché que la France, pas le reste du monde.

Le côté souverain n'aurait protégé de rien du tout ici

Modifié le 19/07/2024 à 16h05
Répondre Réagir
3

FrancoisA Abonné
Aujourd'hui à 18h15
#18.4

> **cayan**
> Faudra expliquer ça à Mr Mélenprout ...
>
> « Microsoft équipe des armes françaises et le ministère de la Défense. Tout va bien ? Vous…

Ca c'est parce que personne au Ministère des Armées n'a lu la licence de Windows.
La licence de Windows interdit l'usage de Windows pour commander une arme.

Et quand on sait que des systèmes de défense du porte avion Charles de Gaulle sont contrôlé par des ordinateur sous Windows, ca laisse rêveur.

- Chef, y a un missile qui se dirige vers nous.
- M'embête pas je dois redémarrer Windows après une mise à jour .....

Scène fictive. Toute ressemblance .....

Modifié le 19/07/2024 à 18h16
Répondre Réagir

Winderly Abonné
Aujourd'hui à 16h43
#18.3

Répondre Réagir

Xanatos Abonné
Aujourd'hui à 15h16
#19

Vendredi miam !
Lu sur leur site https://www.crowdstrike.com/fr-fr/

> 62 minutes suffisent pour mettre votre entreprise à terre.

Même pas des Russes, je suis déçu
Et un petit pour la route:
https://framapiaf.org/@bronco/112812608310071326

Répondre Réagir

aware2 Abonné
Aujourd'hui à 15h29
#20

I was Here !

Vécu de l'intérieur ce matin vers 06h30. Je bosse dans une chaine TV. Quand la régie finale m'a appelé et que je vais vu le carnage Mon état mental oscillait entre et car je ne pouvais strictement rien faire

Répondre Réagir

1

taralafifi
Aujourd'hui à 15h33
#21

C'est un IA qui a contrôlé et poussé l'update vérolée ?

Répondre Réagir

::1
Aujourd'hui à 15h56
#22

c'est un ingénieur d'une SSII française qui rencontre un ingénieur Microsoft. Il discutent 'Techniques de développement'.

Le premier dit au second 'Moi, ça me coûte un fric et un temps fou de tester mes logiciels avant de les commercialiser'.

L'ingénieur Microsoft lui réponds 'Tu testes tes logiciels toi-même ? T'as pas de clients pour faire ça ?'

Répondre Réagir

95