Caso CrowdStrike

la caída mundial de Windows

Gómez Guzmán Anikey Andrea
León Gallardo Ian Yael

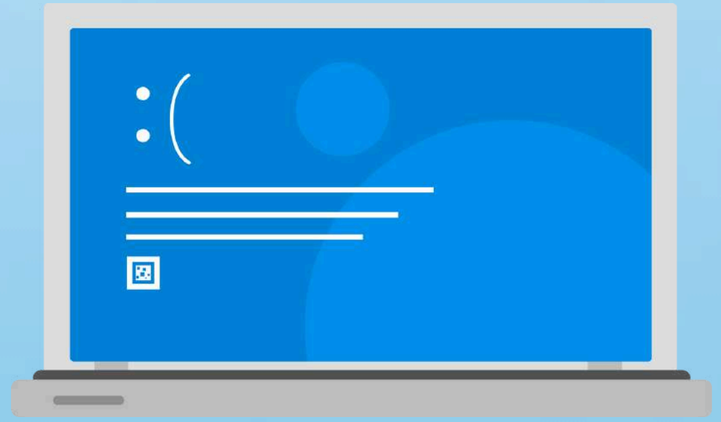
¿Qué sucedio?

Un viernes 19 de julio del 2024 cientos de miles e incluso millones de computadoras empezaron a fallar con el famoso problema de las pantalla Azul de Windows.

El problema se intensifica cuando empieza a afectar a las computadoras de grandes corporativos e instituciones como bancos, aeropuertos, hospitales, fabricas, supermercados, y un sin fin sectores; también afectar a los usuarios finales como nosotros.

Pantalla Azul Windows

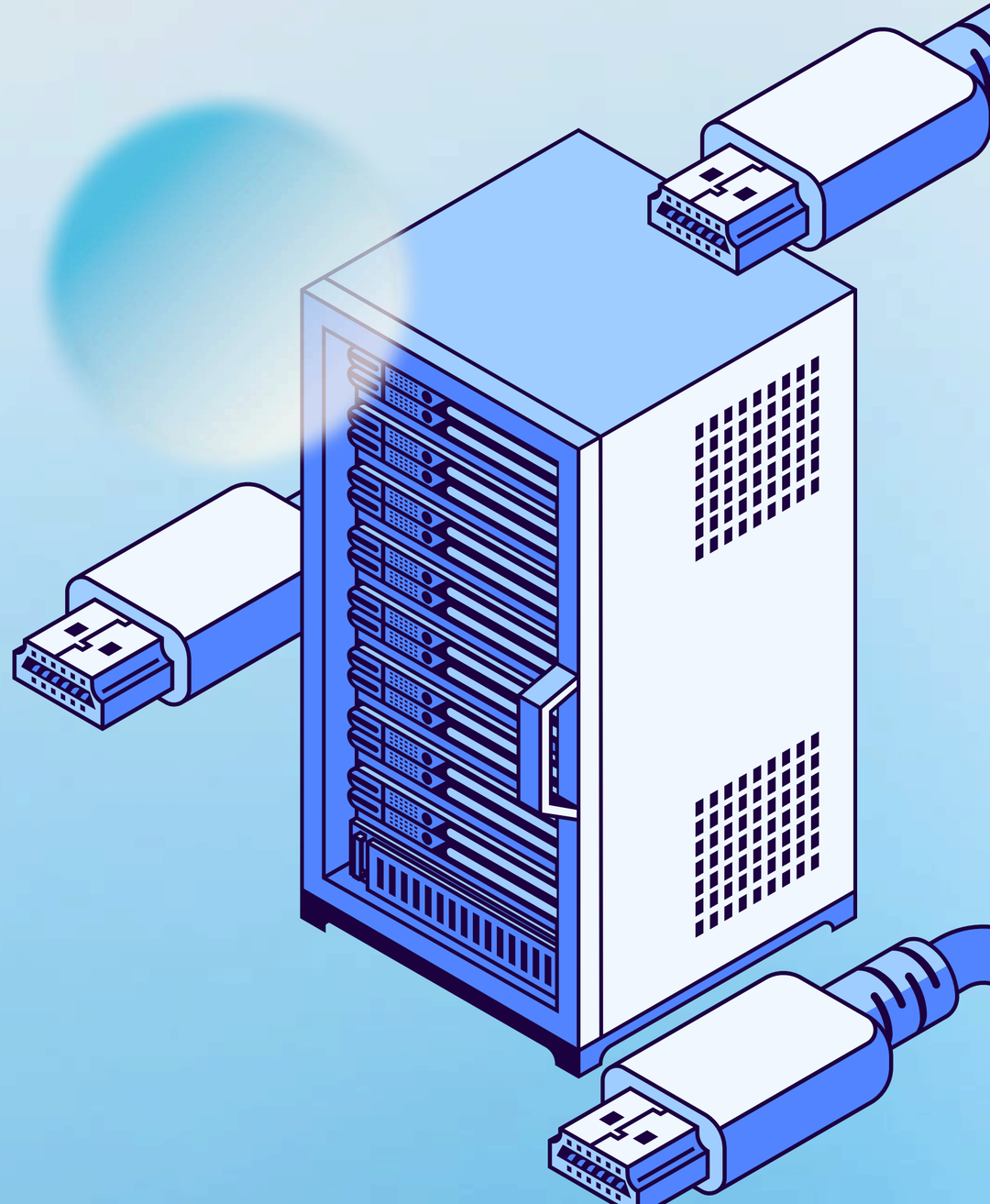
Es una pantalla característica de los sistemas operativos Windows, existe desde hace muchos años, la cual ha ido manchando la reputación de Microsoft y aparece cuando el sistema se bloquea por algún motivo; como problemas con el software o hardware



¿Por que sucedió?

Esto no fue debido a un hack o un ataque cibernético, fue por un problema en un software llamado falcón de CrowStrike.

El cual es un sistema antivirus y un sistema de detección de ataques cibernéticos.



¿Pero quién es CrowdStrike?

CrowdStrike es una empresa de ciberseguridad que proporciona servicios de protección contra amenazas cibernéticas, tanto a nivel de endpoint como en la nube. Es conocida por su plataforma Falcon, utilizada para la protección de dispositivos frente a amenazas avanzadas.

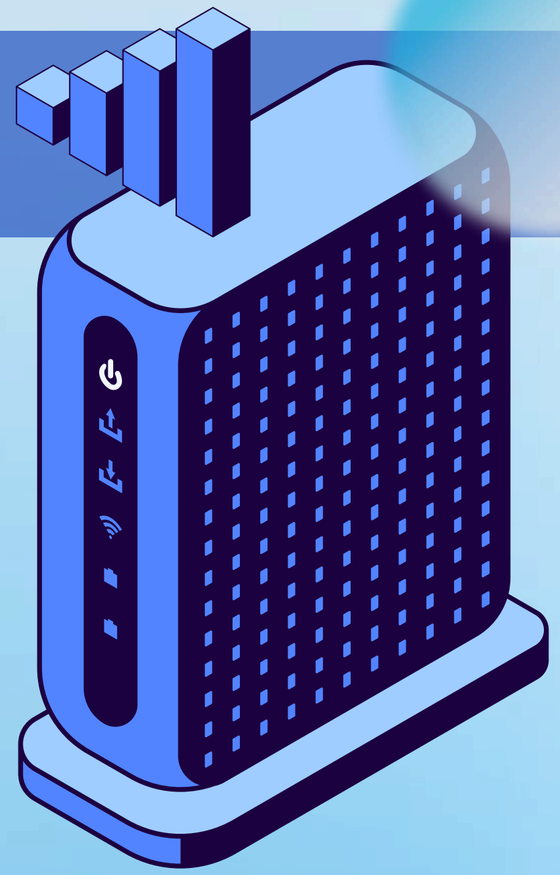
Es una empresa muy importante en el mundo de ciberseguridad, ya que 300 de las 500 más grandes de empresas ocupan sus servicios según Fortune 500; tanto en equipos finales o personales como en servidores

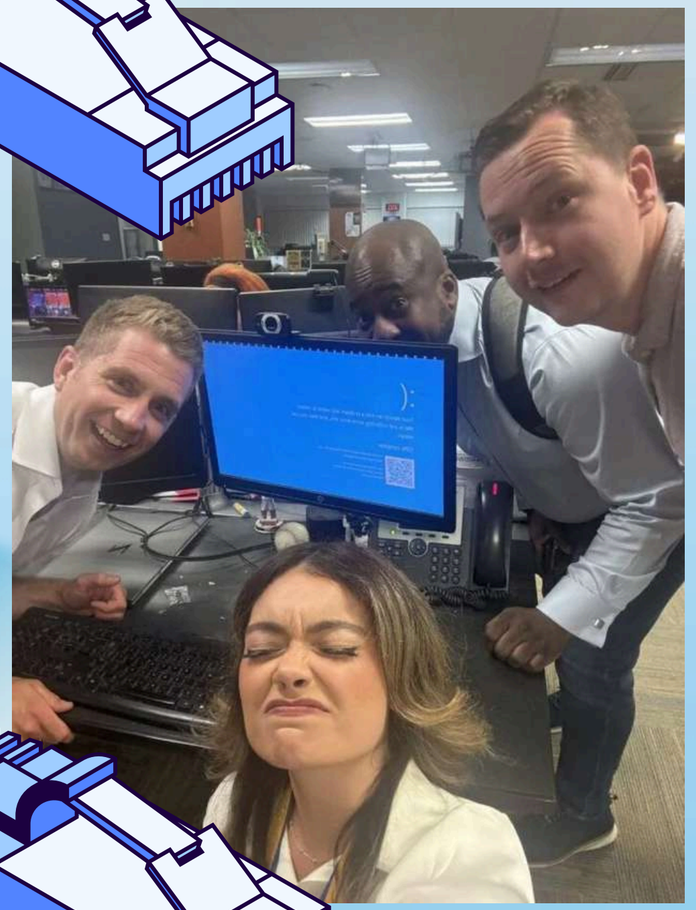
¿Cómo Funciona Falcon?

Falcon es una herramienta, que monitorea constantemente dispositivos para detectar y responder rápidamente ante actividades sospechosas o maliciosas.

Para funcionar, el antivirus necesita acceso al corazón del sistema operativo, el kernel. Esto para poder detectar a tiempo las amenazas antes de que se propaguen por todo el sistema y poder combatirlas.

Por lo que es muy sensible tener acceso al kernel ya que cualquier detalle que se presente puede tener grandes consecuencias.



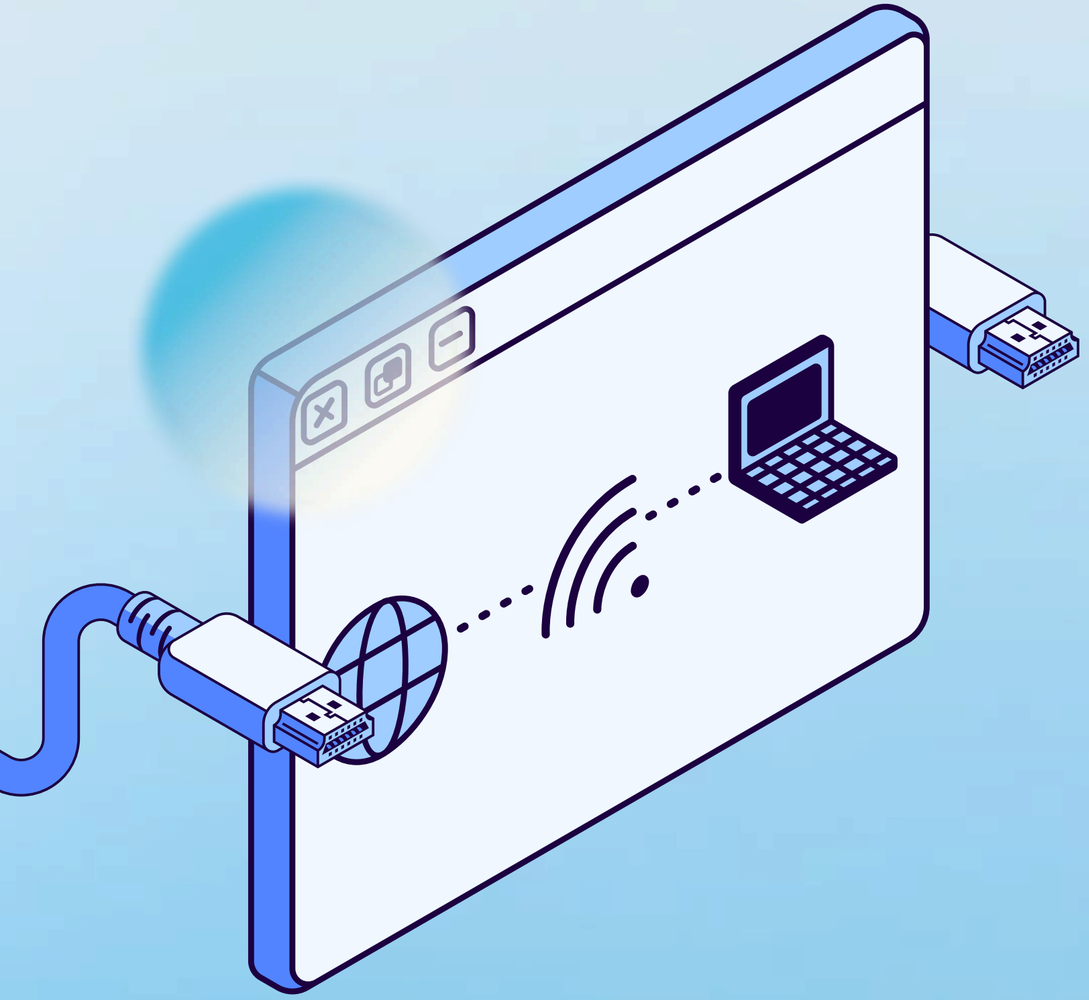


¿Cuál fue el conflicto?

El Antivirus Falcon tuvo una actualización en la madrugada del viernes 19 de Julio a todas las computadoras conectadas y en seguida mando pantallas azules a millones de equipos.

El problema estuvo en un driver del kernel y para solucionar el problema basta con eliminar el archivo.

El conflicto solo estuvo presente por una hora y media, lo que fue suficiente para causar problemas en todo el mundo



¿Por qué se dio el problema?

Al empezar el problema muchos ingenieros en seguridad y software, tanto de la empresa culpable como de otras, empezaron a buscar cual era el error y al principio se pensó que era un problema con el lenguaje de programación usado (C++) y el manejo de la memoria al tener un puntero nulo.

Sin embargo, el ingeniero Tavis Ormandy (ingeniero de Google) descubrió que fue por falta de buenas practicas y no inicializar las variables.

¿Cómo se solucionaba?

Reiniciar el equipo

El equipo de Seguridad de Microsoft propuso la solución de reiniciar el equipo **15 veces** para que pudiera volver a su funcionamiento normal.

Borrar un archivo

El equipo de CrowdStrike proponía que se tenia que entrar en modo seguro o recuperación del sistema operativo, navegar por medio de comandos hasta el driver “C-00000291.sys” que estaba causando el problema y eliminarlo, reiniciar y listo.

Este modo se podía complicar debido que se pide el código bitlocker y si no se cuenta con el, no se puede realizar. Además de que se tenia que hacer computadora por computadora

- CrowdStrike has identified the trigger for this issue as a Windows sensor related content deployment and we have reverted those changes. The content is a channel file located in the %WINDIR%\System32\drivers\CrowdStrike directory.
  - **Channel file “C-00000291*.sys” with timestamp of 2024-07-19 0527 UTC or later is the reverted (good) version.**
  - **Channel file “C-00000291*.sys” with timestamp of 2024-07-19 0409 UTC is the problematic version.**
    - Note: It is normal for multiple “C-00000291*.sys files to be present in the CrowdStrike directory – as long as **one** of the files in the folder has a timestamp of 05:27 UTC or later, that will be the active content.

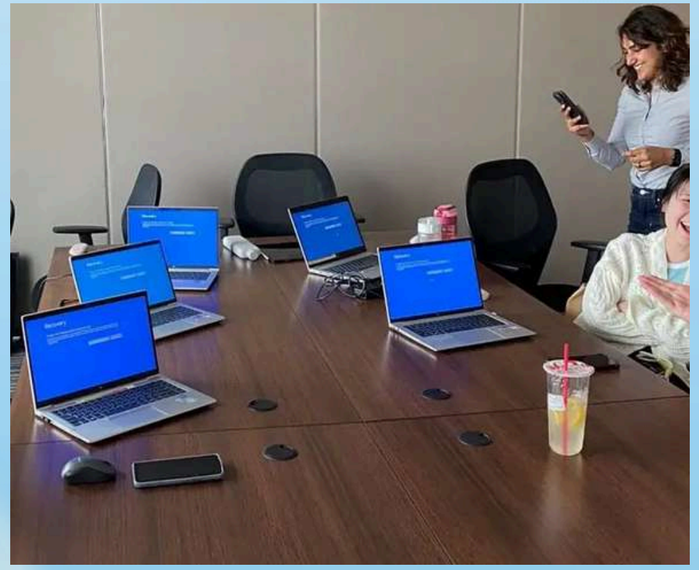
Consecuencias

Para CrowdStrike:
Este problema dejo unas caídas millonarias en las acciones, teniendo que en un fin de semana perdías de 10% de sus acciones.

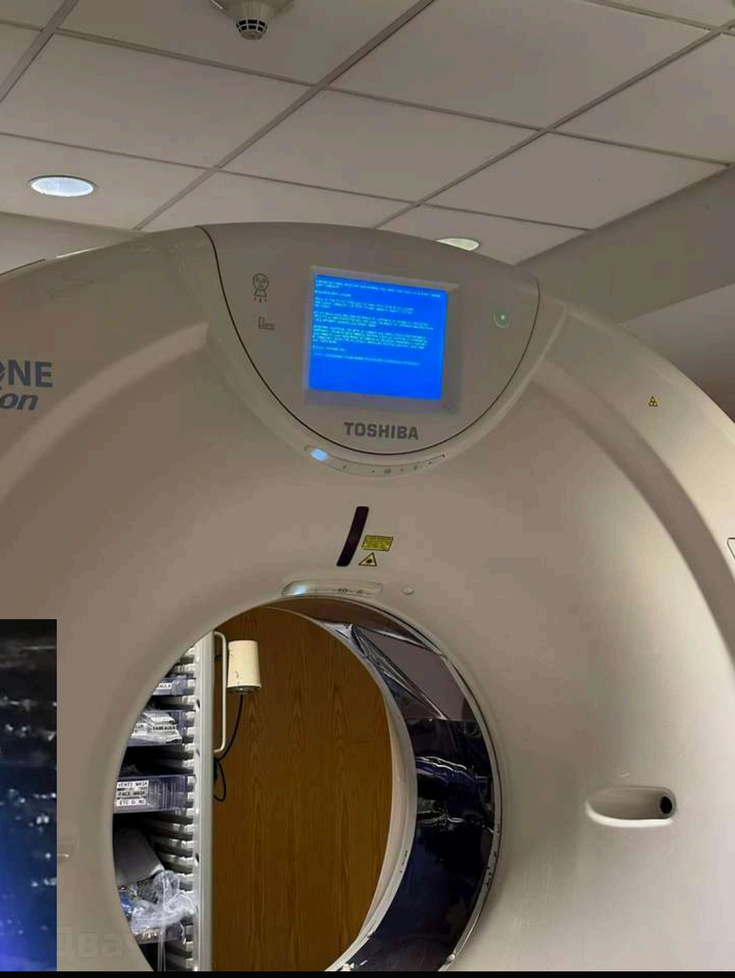
En Aeropuertos:
En este caso los sistemas de los aeropuertos de muchas zonas del mundo dejaron de funcionar y se tuvo que recurrir a escribir como se hacia antes los boletos, se tuvieron que retrasar y cancelar vuelos

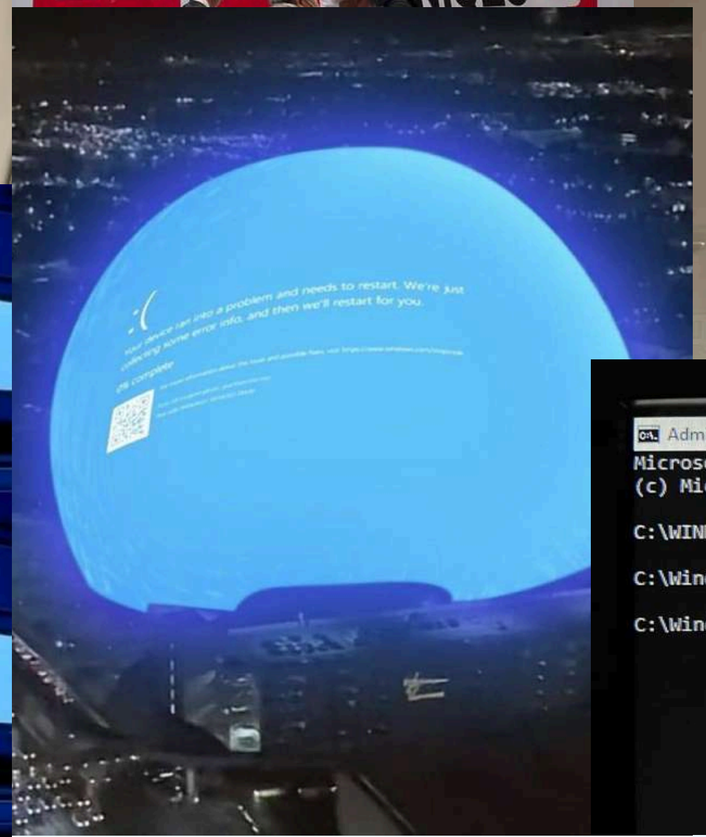
Consecuencias

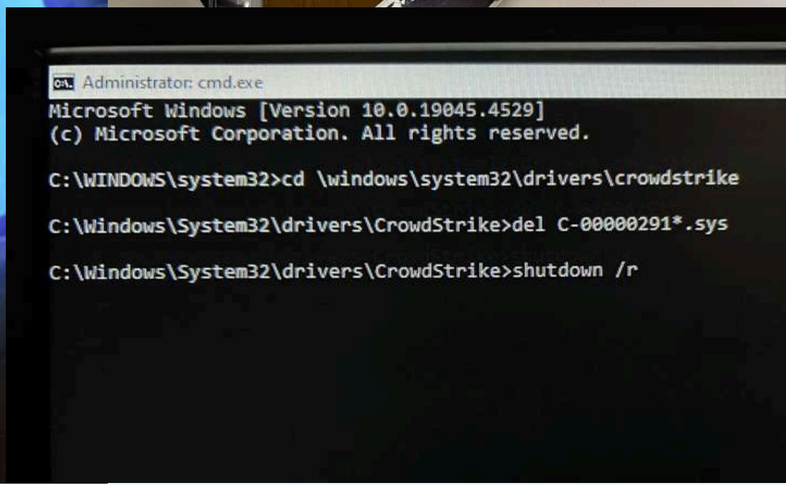
En tiendas:
Se tuvo que recurrir a solo aceptar pagos en efectivo debido a que los sistemas de cobro estaban deshabilitados, afectando a los comercios.



En corporativos:
Las actividades se pararon en la mayoría de sectores corporativos hasta por medio día porque los usuarios o servidores estaban inactivos.







George Kurtz ✓
@George_Kurtz

Follow

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This is not a security incident or cyberattack. The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates and will continue to provide complete and continuous updates on our website. We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels. Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

4:45 AM · Jul 19, 2024 · **10M** Views

Problemas Adyacentes

Durante el problema los ciberdelincuentes hicieron presencia para el sector empresarial por medo de phishing, haciéndose pasar por el soporte de Crowstrike y poder sacar algún provecho de la situación.

También la presión aumento para las empresas de ciberseguridad, ya que se hizo visible que si no se maneja correctamente la seguridad de en los sistemas, puedes tener consecuencias gigantes.

```
crowdstrike.phpartners[.]org
crowdstrike0day[.]com
crowdstrikebluescreen[.]com
crowdstrike-bsod[.]com
crowdstrikeupdate[.]com
crowdstrikebsod[.]com
www.crowdstrike0day[.]com
www.fix-crowdstrike-bsod[.]com
crowdstrikeoutage[.]info
www.microsoftcrowdstrike[.]com
crowdstrikeodayl[.]com
crowdstrike[.]buzz
www.crowdstriketoken[.]com
www.crowdstrikefix[.]com
fix-crowdstrike-apocalypse[.]com
microsoftcrowdstrike[.]com
crowdstrikedoomsday[.]com
crowdstrikedown[.]com
whatiscrowdstrike[.]com
crowdstrike-helpdesk[.]com
crowdstrikefix[.]com
fix-crowdstrike-bsod[.]com
crowdstrikedown[.]site
crowdstuck[.]org
crowdfalcon-immed-update[.]com
crowdstriketoken[.]com
crowdstrikeclaim[.]com
crowdstrikeblueteam[.]com
crowdstrikefix[.]zip
crowdstrikereport[.]com
```

¿Se pudo evitar?

Actualizaciones Automaticas

Un sistema tan delicado y critico no se le recomiendan tener actualizaciones automáticas.

Y gracias a esto se dio el famoso “Delmonting” que es cuando un programador despliega una actualización en un viernes y se va por la tarde inconsciente de que podría pasar algo mal

Probar exhaustivas

No se realizaron las pruebas exhaustivas que pueden durar varios dias al programa y no mandarla como se hizo, de golpe a todos los usuarios. Sino paulatinamente para poder tener tiempo de revertir los cambios.

Gracias
Por su atención

Gómez Guzmán Anikey Andrea
León Gallardo Ian Yael