UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Exposición
Caso CrowdStrike y la caída mundial de Windows

Integrantes:
Gómez Guzmán Anikey Andrea
Leon Gallardo Ian Yael

Materia
Sistemas Operativos

Grupo
6

Profesor
Gunnar Eyal Wolf Iszaevich

Semestre
2025-1

Fecha de entrega
15 de octubre de 2024

Introducción

En años recientes, hemos visto un aumento significativo en la frecuencia y el impacto de los incidentes de ciberseguridad, afectando a empresas, gobiernos y usuarios comunes. La interconexión global de sistemas operativos como Windows los convierte en blancos atractivos para los ciberataques. En este escenario, empresas de seguridad como CrowdStrike juegan un papel esencial en la detección, mitigación y prevención de amenazas de gran escala. No obstante, el reciente colapso mundial del sistema operativo Windows presentó serios desafíos para los proveedores de seguridad y causó una crisis sin precedentes que afectó a millones de personas.

CrowdStrike fue fundada en 2011 por George Kurtz (ex-CTO de McAfee) y se ha convertido en una de las firmas de ciberseguridad más utilizadas del mundo, con más de 29.000 clientes. CrowdStrike tiene su sede en Texas y entre sus hitos destaca la detección del hackeo a sony Pictures el año 2014 o los ciberataques al partido Demócrata entre 2015 y 2016.

CrowdStrike Falcon consiste en una plataforma en la nube que utiliza inteligencia artificial asi como aprendizaje automático para poder detectar y prevenir amenazas cibernéticas en tiempo real. Esta plataforma ofrece a las organizaciones la capacidad de monitorear actividades sospechosas en sus sistemas, detectar posibles ataques y responder de manera rápida y efectiva.

Su función es la de detectar y prevenir posibles ciberataques. Para evitar daños críticos a las empresas con las que trabaja. Una de las compañías que trabaja con CrowdStrike es precisamente Microsoft, quien ha confirmado que la incidencia con sus plataformas es debido a un problema con CrowdStrike.

Este reporte abordará el papel de CrowdStrike en relación con la caída mundial de Windows, explicando los problemas relacionados con este incidente y los desafíos que enfrentaron las principales organizaciones tecnológicas, incluidos Microsoft y CrowdStrike, en la respuesta y mitigación del daño.

Descripción del incidente

El pasado 19 de julio del 2024 a las 4:09 UTC, las computadoras de todo el mundo sufrieron una pérdida por parte de Microsoft, que no solo afectó a usuarios comunes, sino también a bancos, instituciones, organismos y hospitales, además de que esto generó un caos en múltiples aeropuerto, ya que como parte de la operativa rutinaria, CrowdStrike lanzó una actualización de configuración del sensor Falcon para sistemas Windows. Esta actualización de configuración desencadenó un error lógico que provocó el bloqueo del sistema y una pantalla azul (BSOD) en los sistemas afectados con Microsoft Azure.

"La empresa admitió un fallo en una actualización de su plataforma CrowdStrike Falcon, uno de los sistemas de protección de Windows. El impacto solo aplica a computadoras con sistema operativo Microsoft Windows y no a otros sistemas operativos como Mac OS o Linux. Esto se evidencia en la aparición de la clásica pantalla azul de Windows, que

indica que el sistema ha dejado de responder", había explicado a Clarín Matías Sliafertas, CISO de BASE4 Security, empresa de ciberseguridad argentina.

"Al ser un programa de seguridad tiene ciertos permisos especiales dentro de cada computadora y de cada empresa, ya que se encarga de manejar gran parte de la ciberseguridad local y de la red. Es por eso que cuando el mismo sistema que nos protege falla, lo que ocurre es que el programa actúa como si se atacara a sí mismo y, en este caso particular, se eliminó un archivo que es vital para el correcto funcionamiento del sistema. Es exactamente ahí donde radicó el problema", había precisado.

La actualización defectuosa llevó a problemas graves. Las operaciones de muchas empresas se vieron afectadas, incluidas cancelaciones de vuelos y problemas en servicios financieros, siendo estos dos los sectores más afectados, pero de igual forma afectó empresas, escuelas, administraciones públicas y algunos servicios de emergencia. Microsoft trabajó en conjunto con CrowdStrike y otros proveedores de servicios en la nube para desarrollar soluciones y brindar soporte a los clientes afectados.

Los archivos de configuración que contenía la nueva actualización, se les denomina “Channel files” y estos forman parte de los mecanismos de protección utilizados por el sensor Falcon. Estas actualizaciones son parte normal del funcionamiento del sensor y se producen varias veces al dia en respuesta a nuevas táctica, técnicas y procedimientos descubiertos por la compañía CrowdStrike y no es algo nuevo que se haya implementado, sino algo que se ha mantenido desde que inicio la plataforma Falcon.

"El software de CrowdStrike funciona en la capa de bajo nivel del sistema operativo. Los problemas a este nivel hacen que el sistema operativo no arranque», afirma Lukasz Olejnik, investigador y consultor independiente en ciberseguridad y autor de *Philosophy of Cybersecurity*.

Cuando comenzó el problema los ingenieros encargados de la seguridad y software de ambas empresas, comenzaron a buscar cual era el problema, al principio pensaron que era relacionado con con el lenguaje de programación 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.

La interrupción que se generó a los servicios, pareció deberse, al menos en parte, a una actualización de software por Crowdstrike en los sistemas Microsoft Windows. La firma estadounidense de ciberseguridad dijo a sus clientes la madrugada del viernes que los ingenieros estaban abordando el problema, según un aviso visto por CNN. El problema es específico de Falcon, que está diseñado para proteger archivos guardados en la nube.

Impacto

“Los clientes que tenían sensores Falcon para Windows versión 7.11 y superior en ejecución, que estuvieron en línea entre el viernes 19 de julio de 2024 a las 04:09 UTC y el viernes 19 de julio de 2024 a las 05:27 UTC, pudieron verse afectados. Los sistemas que ejecutaban el sensor Falcon para Windows 7.11 y superior que descargaron la configuración actualizada de las 04:09 UTC a las 05:27 UTC eran susceptibles a un bloqueo del sistema.” Declaró CrowdStrike a través de su página oficial.

A medida que estos problemas empezaron a propagarse, fue evidente que no se limitaban a un error específico o localizado.

Este suceso puso de manifiesto una debilidad en la estructura del ecosistema de Windows, agravada por la fuerte dependencia de este sistema en entornos críticos y la interconexión de dispositivos a nivel mundial.

Se estima que el costo económico del colapso de Windows ascendió a miles de millones de dólares, no solo por las interrupciones directas en el negocio, sino también por la pérdida de productividad, la pérdida de datos y el tiempo necesario para restaurar los sistemas. Ante la fallida actualización de CrowdStrike, esta problemática afectó a 21 mil clientes, según cálculos de Cyberpeace, firma de ciberseguridad, basados en datos de la compañía IDC.

Algunos analistas hablan del "apagón informático" más grande de la historia desde WannaCry, un ransomware que paralizó al mundo en 2017.

Respuesta de Microsoft y CrowdStrike

Ante la gravedad del incidente, Microsoft y CrowdStrike implementaron una serie de acciones para mitigar los daños y restaurar la normalidad en los sistemas afectados.

CrowdStrike respondió rápido corrigiendo la actualización lanzada a las 5:27 UTC del mismo día, así como la empresa confirmó que el problema no había sido causado por un ciberataque, ni un error en la seguridad, sino que había sido causado por un error lógico en la actualización. Además, dio un mensaje comprometiéndose a realizar acciones para identificar cualquier mejora fundamental o de flujo de trabajo para fortalecer el proceso y mantener actualizados a los usuarios acerca de sus hallazgos.

De igual manera CrowdStrike dio instrucciones manuales a sus clientes sobre cómo solucionar la caída y en conjunto estaba trabajando en una nueva actualización que sustituye a la que generó el error. Las instrucciones para solucionar el error, fueron las siguientes:

- ☐ En Window dirigirse a los channel files residen en el siguiente directorio: `C:\Windows\System32\drivers\CrowdStrike\`
- ☐ Identificar el archivo afectado tiene como identificador único 291 y tendrá un nombre de archivo que comienza con “`C-00000291-`” y termina con extensión `.sys`.
- ☐ Eliminar dicho archivo y reiniciar el equipo.

Aunque esto se ponía complicado ya que se pedía un código bitlocker, que si no se cuenta con él, este proceso no se puede realizar, además de que seria tedioso y tardado realizar este procedimiento múltiples veces en locaciones como aeropuertos que cuentan con numerosos equipos.

En cambio Microsoft, trabajó para resolver los problemas que se habían ocasionado por la interrupción y recomendó reiniciar el equipo un aproximado de 15 veces; así como

realizar un informe dando a conocer que las acciones de la empresa habían caído ligeramente en la bolsa de valores de NY.

Consecuencias a corto y largo plazo

A corto plazo:

Como consecuencias a corto plazo se encontraron las ya mencionadas interrupciones a los servicios, ya que los usuarios no podían acceder a sus sistemas, pero solo aquellos que usaran la extensión de Azure (normalmente medianas y grandes empresas), ya que usuarios que usarán Windows en su vida cotidiana, no se vieron afectados, porque CrowdStrike es utilizado predominantemente por grandes organizacione.

En cuestión de horas, múltiples sectores de la economía global empezaron a reportar problemas similares. Muchas organizaciones tecnológicas que utilizan esta plataforma como base para el desarrollo y administración de sus sistemas experimentaron caídas críticas que afectaron centros de datos, sistemas en la nube y aplicaciones empresariales. El sector financiero también sufrió interrupciones, ya que instituciones bancarias, dependientes de Windows para gestionar transacciones y datos sensibles, vieron cómo sus clientes no podían acceder a cuentas ni realizar operaciones. Gobiernos de distintos países reportaron fallos en sus sistemas de administración de servicios públicos y bases de datos, lo que comprometió la prestación de servicios esenciales. En infraestructuras críticas, como salud, transporte y energía, las interrupciones fueron especialmente graves; hospitales enfrentaron dificultades para acceder a historiales médicos electrónicos, y los sistemas de gestión de transporte y energía sufrieron retrasos y fallos operativos.

Las pérdidas no fueron solo causadas por la interrupción de servicios, sino también por la disminución de la productividad, la recuperación de datos y los gastos adicionales para restablecer sistemas comprometidos. Corporaciones y entidades gubernamentales que utilizaban Windows experimentaron interrupciones en sus actividades por períodos de horas o días, ocasionando daños económicos y daños a su imagen. Además de la disminución directa de ganancias, se reflejo la fragilidad de infraestructuras críticas que se apoyan en la conexión y funcionamiento constante de sistemas.

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

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

A largo plazo:

Las consecuencias a mayor plazo fueron notarías, ya que se tuvo que invertir en ciberseguridad por parte de varias empresas y gobiernos, así como revisar las políticas de actualización de software y perchero de vulnerabilidades.

Empresas grandes tuvieron que invertir en sistemas para desarrollar planes que les permitiera seguir operando ante caídas de sistemas.

La recuperación completa de esta falla puede tomar tiempo, ya que se requiere una revisión detallada de todos los sistemas afectados, la implementación de parches y soluciones de seguridad, asi como pruebas para asegurarse de que este problema no se repita. Este tipo de recuperaciones no solo son técnicas, tambien operativas, las empresas deben reevaluar sus políticas de actualización y mantenimiento para evitar que algo similar ocurra en el futuro.

En cuanto a Microsoft y CrowdStrike, tendrán que recuperar la confianza que perdieron por parte de sus usuarios, especialmente en relación con la velocidad de la respuesta y la capacidad para solucionar problemas.

Lecciones aprendidas

Este colapso nos brindó lecciones para que las organizaciones no se vean afectadas por problemas similares a futuro, como la importancia de adoptar enfoques más preventivos y coordinados:

1. **Actualizaciones escalonadas:** implementar actualizaciones de manera gradual, poder mitigar el riesgo de fallos masivos al ir evaluando el desempeño de los equipos y sistemas en lugar de actualizaciones automáticas. Surgió el conocido fenómeno del "Delmonting", en el cual un desarrollador lanza una actualización un viernes y se va por la tarde sin considerar posibles problemas.
2. **Control de calidad riguroso:** junto con el punto anterior es importante realizar pruebas exhaustivas para implementar actualizaciones para evitar errores críticos.
3. **Planes de recuperación:** es importante desarrollar y practicar planes de recuperación y contingencia antes de desastres para minimizar el impacto.
4. **Reducción de acoplamiento:** diversificar sistemas y proveedores para evitar dependencia excesiva en un solo servicio con la finalidad de poder seguir activos en caso de que se presente una falla.

Este fallo demuestra la interconexión entre muchos sistemas y como la falla de uno puedo desencadenar un efecto dominó.

La empresa CrowdStrike y otras empresas de ciberseguridad están progresando hacia la inteligencia artificial (IA) y el aprendizaje automático (machine learning) para identificar comportamientos inusuales y prevenir amenazas futuras. Estas tecnologías posibilitan la identificación anticipada al analizar enormes volúmenes de información en tiempo real con el fin de reconocer anomalías en el tráfico de red o en el funcionamiento de los sistemas.

Conclusiones

La crisis global de Windows reveló no solo fallos en sistemas comúnmente usados, sino también la importancia de respuestas ágiles, actualizaciones regulares y soluciones eficaces.

Aunque el bloqueo de 8,5 millones de computadoras pueda parecer un número pequeño en comparación con los miles de millones de equipos en funcionamiento diario en el mundo, lo preocupante es que este fallo afectó lugares logísticos clave como aeropuertos, estaciones de tren y empresas. Como resultado, la sensación de colapso se incrementó, dado que, aunque solo fue el 1 por ciento de los dispositivos con Windows, la repercusión de este fallo afectó a millones de personas debido a la caída de numerosos servicios.

Esto también pone de manifiesto uno de los aspectos negativos del mundo globalizado actual, ya que, a pesar de que la igualdad de progreso en áreas como la tecnología o la expansión de las empresas ha aumentado, estos problemas también afectan a nivel mundial.

Referencias

- Clarín. (2023, julio 20). *CrowdStrike: Revelan la causa del error que provocó la caída mundial de Microsoft*. Clarín. https://www.clarin.com/tecnologia/crowdstrike-revelan-causa-error-provoco-caida-mundial-microsoft_0_gFYImuIC3Y.html

- CNN en Español. (2024, julio 19). *¿Qué pasó con la caída mundial de Microsoft? CrowdStrike y las implicaciones globales*. CNN en Español. Publimetro. (2024, agosto 19). La caida de Microsoft y las lecciones aprendidas. Publimetro. https://www.publimetro.com.mx/queretaro/2024/08/19/la-caida-de-microsoft-y-las-lecciones-aprendidas/
- AS. (2024). ¿Qué provocó la caida de Microsoft y originó el colapso mundial de CrowdStrike? AS. https://as.com/meristation/betech/que-provoco-la-caida-de-microsoft-y-origino-el-colapso-mundial-de-crowdstrike-n/
- NMás. (2024). NMás. Esto paso: CrowStrike por que fue ka falla informatics microsoft que causo una caida mundial https://www.nmas.com.mx/tecnologia/crowdstrike-por-que-fue-falla-informatica-microsoft-que-causo-caida-mundial/
- Hosting. (2024). . Hosting. Caida mundial de Microsoft. https://www.hosting.com.pe/caida-mundial-microsoft-crowdstrike-trax.php
- Technology Review. (2024). . Technology Review. https://www.technologyreview.es//s/16551/balance-de-la-caida-de-microsoft-muestra-lo-facil-que-es-infligir-un-dano-global

- CrowdStrike. (2024, julio 19). Detalles técnicos sobre la interrupción del 19 de julio. CrowdStrike. https://www.crowdstrike.com/technical-details-on-todays-outage-latam/