INCIDENTE CRÍTICO CROWDSTRIKE

// Better Base, Better Future

METABASE Q

INCIDENTE CRÍTICO CROWDSTRIKE

CONTEXTO

- CrowdStrike presentó un incidente en gran parte de los activos con sistemas operativos Microsoft Windows relacionados con el sensor de Falcon. Según lo analizado por el equipo de Metabase Q, la actualización con fallo corresponde a un archivo "C-00000291*.sys" y no a la última versión del instalador.
- El horario de la versión problemática del archivo .sys corresponde 04:09 UTC. Todos los archivos con la misma nomenclatura ".sys" generado posterior a las 05:27 UTC, son archivos notificados por Crowdstrike como estable.
- La afectación, hasta el momento, no tiene un patrón, por tanto no existe un registro oficial de las versiones afectadas.
- **En Batuta, en el módulo de Librería de Script hemos generado un botón denominado "Incident_CS" que permite identificar aquellos equipos que han sido actualizados, por tanto no representan un riesgo en la operación**
  Ante cualquier duda pueden ponerse en contacto con nosotros por el siguiente medio support@batuta.io
- **Nota: Es importante comentar, que todos los activos encendidos o conectados después del horario del incidente no van a ser afectados**

INCIDENTE CRÍTICO CROWDSTRIKE

DETALLES

- Los síntomas incluyen hosts experimentando un error de comprobación "pantalla azul" relacionado con el sensor de Falcon.
- Este problema no afecta a hosts basados en Mac o Linux.
- No existe oficialmente una mitigación bajando la versión del instalador al N-2

ACCIÓN ACTUAL

- El equipo de ingeniería de CrowdStrike ha identificado un despliegue de contenido relacionado con este problema y ha revertido esos cambios.
- Si los hosts siguen fallando y no pueden permanecer en línea para recibir los cambios de actualización, se pueden seguir los pasos de solución temporal

PASOS PARA LA COLUSIÓN TEMPORAL

- Reinicie el host para darle la oportunidad de descargar el archivo actualizado ".sys" generado por Crowdstrike. Si el host falla nuevamente, entonces:
- Inicie Windows en Modo Seguro o en el Entorno de Recuperación de Windows. El workaround sugerido por CrowdStrike es el siguiente:

INCIDENTE CRÍTICO CROWDSTRIKE

WORKAROUND CROWDSTRIKE

CrowdStrike Engineering has identified a content deployment related to this issue and reverted those changes.
If hosts are still crashing and unable to stay online to receive the Channel File Changes, the following steps can be used to workaround this issue:

- Workaround Steps for individual hosts:
  - Reboot the host to give it an opportunity to download the reverted channel file. If the host crashes again, then:
  - Boot Windows into Safe Mode or the Windows Recovery Environment
  - Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
  - Locate the file matching “C-00000291*.sys”, and delete it.
  - Boot the host normally.
  - Note: Bitlocker-encrypted hosts may require a recovery key.
- Workaround Steps for public cloud or similar environment including virtual:
  - Option 1:
    - Detach the operating system disk volume from the impacted virtual server
    - Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
    - Attach/mount the volume to to a new virtual server
    - Navigate to the %WINDIR%\\System32\drivers\CrowdStrike directory
    - Locate the file matching “C-00000291*.sys”, and delete it.
    - Detach the volume from the new virtual server
    - Reattach the fixed volume to the impacted virtual server
  -

INCIDENTE CRÍTICO CROWDSTRIKE

    - Option 2:
        - Roll back to a snapshot before 0409 UTC.
        - Workaround Steps for Azure via serial
        - Login to Azure console --> Go to Virtual Machines --> Select the VM
        - Upper left on console --> Click : "Connect" --> Click --> Connect --> Click "More ways to Connect" --> Click : "Serial Console"
    - Step 3 : Once SAC has loaded, type in 'cmd' and press enter.
        - type in 'cmd' command
        - type in : ch -si 1
        - Press any key (space bar). Enter Administrator credentials
        - Type the following:
            - bcdedit /set {current} safeboot minimal
            - bcdedit /set {current} safeboot network
        - Restart VM
- Optional: How to confirm the boot state? Run command:
    - wmic COMPUTERSYSTEM GET BootupState
- Latest Updates
    - 2024-07-19 05:30 AM UTC | Tech Alert Published.
    - 2024-07-19 06:30 AM UTC | Updated and added workaround details.
    - 2024-07-19 08:08 AM UTC | Updated

When your security works, your future works.

Buid a better base with Metabase Q

contact@metabaseq.com
+52 55 2211 0920

// Better Base, Better Future

METABASE Q