

Qué sucede cuando CC detecta ataques de memoria

En primer lugar, es muy importante señalar que las alteraciones de memoria ocurren por varias razones distintas:

1. Ataques en memoria
2. Interacción entre programas
3. Errores de software
4. Exploits

Por lo tanto, una inyección de proceso o una técnica de alteración de memoria utilizada, incluso entre programas, no es necesariamente una acción maliciosa.

Si un programa que ha sufrido un evento de memoria probablemente malicioso (es decir, el #1 o el #4 mencionados anteriormente) está involucrado en una respuesta automatizada por parte de Cyber Crucible, se produce una actividad de recopilación automatizada.

La parte de la memoria que fue alterada en un programa, así como el estado “anterior”, se guarda en un formato estructurado de Cyber Crucible llamado .ccdifff

Esa porción inyectada o alterada de la memoria se guarda y está disponible para su descarga en el portal web de Cyber Crucible.

¿Por qué no se envía esto automáticamente a Virustotal (etc.) para su análisis?

En algunas circunstancias, el código malicioso utilizado en un ataque contiene variables que son únicas para ese ataque, específicamente para una víctima.

Enviar este código malicioso a un motor de análisis público como Virustotal representaría una divulgación de información no deseada que identifica a la víctima ante la comunidad de seguridad.

¿Por qué sería útil enviar estos datos binarios a Virustotal (etc.)?

Las herramientas de antivirus y EDR basadas en firmas buscan cadenas o bytes de código vistos en ataques anteriores. Incluso si este malware nunca se ha visto antes, es posible que, después de un tiempo, sea conocido por la comunidad de seguridad. Estas herramientas de escaneo generalmente no necesitan que el código esté en un binario con el formato adecuado para señalar una asociación con una pieza de malware conocida.

Revision #1

Created 2026-07-24 01:48:28 UTC by Dennis Underwood

Updated 2026-07-24 01:48:28 UTC by Dennis Underwood