# Tecnologías de ciberseguridad para IC: 'multiscanning' y CDR

Sebastián Carmona
CEO de Micromouse

A esta hora y este momento, el último ciberataque que nos ha sobresaltado ha sido el sufrido por Endesa. Afortunadamente, una buena estrategia y prácticas en materia de ciberseguridad han sido suficiente para repelerlo sin afectar al negocio. Todo lo contrario a lo ocurrido con la filial del Banco Industrial y Comercial de China en Estados Unidos, que durante horas tuvo caídos los sistemas. Han tenido que recurrir al uso de los USB y de mensajeros como alternativa para dar continuidad al negocio. Hay sospechas que el grupo Lockbit está detrás de este ciberataque.

Y es que Lockbit es el principal causante de los ciberataques que acaparan titulares en las últimas fechas. Se sospecha que uno de cada tres tiene su firma, ya sea directamente o a través de sus franquiciados. No en vano, su eficacia es alta debido a su continua actualización (Lockbit 3.0) y a la ingeniería social; todo ello, con el prisma de una organización empresarial con sus objetivos e intereses.

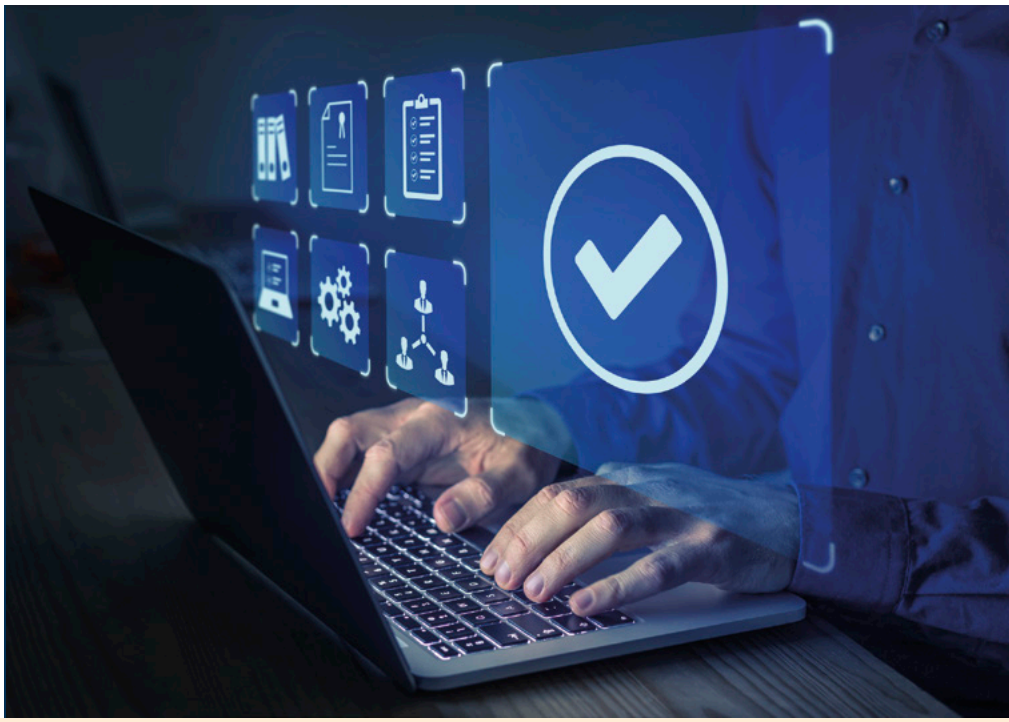
No obstante, ¿es Lockbit imparable? Es muy eficiente, pero una estrategia acertada, buenas prácticas y tecnologías eficaces pueden mitigar sus ataques.

## 'Multiscanning'

Disponer de una combinación de motores *antimalware* para analizar el tráfico de nuestro servidor de correo, nuestro *firewall* o nuestros ficheros (ya estén ubicados en repositorios compartidos o no), dotar de repositorios de datos seguros y, en general, analizar nuestra infraestructura IT hoy es posible: una caja negra "automágicamente" trabajando donde, de forma simultánea y en tipo real, múltiples motores *antimalware* están velando por evitar un ataque.

Efectivamente, el análisis simultáneo con múltiples motores *antimalware* es una tecnología avanzada de detección y prevención de amenazas que proporciona resiliencia para soluciones *antimalware* de un solo proveedor. Aumenta las tasas de detección y reduce los tiempos de detección de brotes. Mientras que los sistemas con un único motor *antimalware* pueden detectar entre un 40 y un 80 por ciento de *malware*/virus, la tecnología *multiscanning* es capaz de escanear archivos con más de 30 motores *antimalware* para lograr tasas de detección superiores al 99 por ciento.

Muchos estudios demuestran que a medida que se agregan más motores *antimalware* mejora su tasa de detección.



# Una estrategia de confianza cero es posible, y las tecnologías 'multiscanning' y CDR así lo ratifican

¿Por qué? Porque cada motor individual se especializa en diferentes categorías y es posible que no detecte ciertos tipos de amenazas. A esto hay que añadir que cada motor *antimalware* utiliza algoritmos de detección diferentes y, al combinarlos, se aumenta significativamente la tasa de detección. Por último, y no menos importante, la combinación del trabajo de investigación y generación de patrones de laboratorios de *malware* ubicados en distintas partes del mundo hace que mejore la respuesta a los ataques localizados.

## Desactivando 'malware'

CDR (*Content, Disarm and Reconstruction*) trata cada archivo como una amenaza potencial. Procesa y analiza archivos para eliminar objetos no permitidos y para garantizar que todos sean seguros. Al mismo tiempo, reconstruye el contenido del archivo con plena funcionalidad; de este modo, los usuarios pueden visualizar el vídeo sin descargas de *malware*.

CDR fortifica, asimismo, la prevención de amenazas sin confiar en la detección de las mismas. Asume, por defecto, que todos los archivos son maliciosos y desinfecta y reconstruye cada uno de ellos asegurando su completa usabilidad con contenido seguro. La tecnología es increíblemente efectiva para prevenir amenazas conocidas y desconocidas, incluidos los ataques dirigidos de día cero y las amenazas que están equipadas con tecnología de evasión de *malware*, como *malware* totalmente indetectable, detección VMware, ofuscación y muchos otros.

CDR, asimismo:

- Identifica y escanea los ficheros. Los ficheros se evalúan y verifican a medida que ingresan al sistema de desinfección para garantizar el tipo de archivo y su coherencia, siendo capaz de identificar infinidad de clases. Cada uno de ellos se analiza, además, con la tecnología *multiscanning* para identificar amenazas conocidas y desconocidas. Las extensiones de archivo se examinan para evitar que los archivos aparentemente complejos se presenten como más simples, una señal de alerta para contenido malicioso, poniendo sobre aviso a las organizaciones cuando se detecta cualquier ataque. CDR admite, además, la desinfección de ficheros, como pueden ser PDF, Microsoft Office, HTML o imágenes.

- Desinfecta los ficheros. Los ficheros se reconstruyen en un proceso rápido y seguro. Las distintas capas y elementos que lo componen se separan en componentes discretos, se eliminan los elementos maliciosos y se reconstruyen los metadatos y todas las características del archivo. El nuevo fichero se vuelve a recomponer y liberar, preservando la integridad de su estructura para que los usuarios lo puedan usar de manera segura y sin pérdida de usabilidad.
- Libera los ficheros. Los ficheros recién regenerados ahora se pueden usar de forma segura. Incluso los más complejos siguen siendo utilizables; por ejemplo, las animaciones incrustadas en archivos de PowerPoint permanecen intactas. Finalmente, los ficheros originales se ponen en cuarentena para su copia de seguridad y posterior examen. Al generar ficheros totalmente utilizables de contenido seguro, CDR protege a las organizaciones contra las amenazas más avanzadas y, al mismo tiempo, mantiene la productividad del usuario.

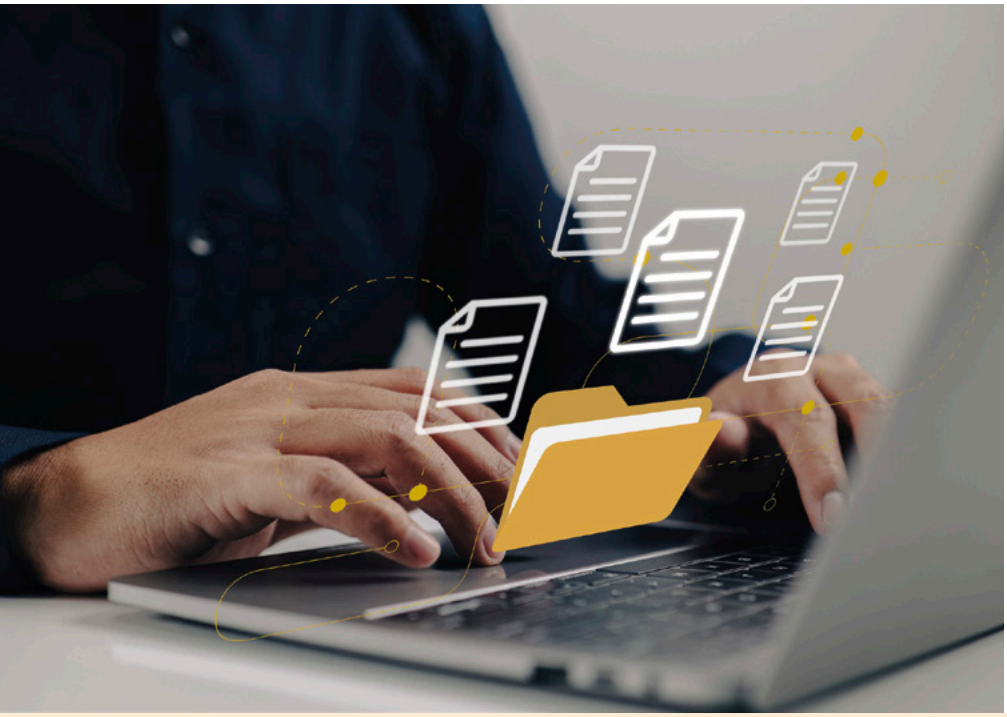
## ¿Por qué CDR?

¿Por qué CDR? Porque el *malware* está creciendo en complejidad y se está volviendo cada vez más exitoso a la hora de evadir los motores *antimalware* y los *sandboxes* tradicionales:

- El *malware* se está volviendo más avanzado y, a menudo, explota vulnerabilidades de software conocidas y desconocidas.
- El *malware* ahora se está generando "compatible *sandbox*" y es cada vez más capaz de evadir los métodos de detección tradicionales.
- La cantidad de tipos de ficheros crece cada día, introduciendo nuevas debilidades potenciales que los actores maliciosos pueden explotar.
- La complejidad de los archivos está aumentando, dando a los ciberdelincuentes más oportunidades para incorporar *scripts* y aprovechar vulnerabilidades.

CDR previene las amenazas sin depender de la detección. Tampoco deja espacio para errores de detección de amenazas y previene muchas de ellas basadas en fichero, incluidas las conocidas, desconocidas, complejas y compatibles *sandbox*. Al desinfectar cada archivo y eliminar cualquier posible amenaza incrustada, CDR "desarma" todas las amenazas basadas en fichero sin la necesidad de detección.

> CDR no deja espacio para errores de detección de amenazas y previene muchas de ellas basadas en fichero



## Tecnologías compatibles

La introducción de una nueva tecnología significa, en muchos casos, un cambio en la infraestructura vinculada a la ciberseguridad de la organización. Estas dos tecnologías sí representan una capa adicional de seguridad y son totalmente compatibles y complementarias con lo ya desplegado. No hay que elegir.

Además, su adaptabilidad a la infraestructura que queremos reforzar hubiera mitigado los ciberataques del Ayuntamiento de Sevilla, que empleó el *email* como vector de ataque a sus sistemas; o de DSB de Dinamarca vía cadena de suministro, cuando fue atacado su proveedor Supeo.

Una estrategia *zero trust* o de confianza cero es posible, y estas tecnologías así lo ratifican.