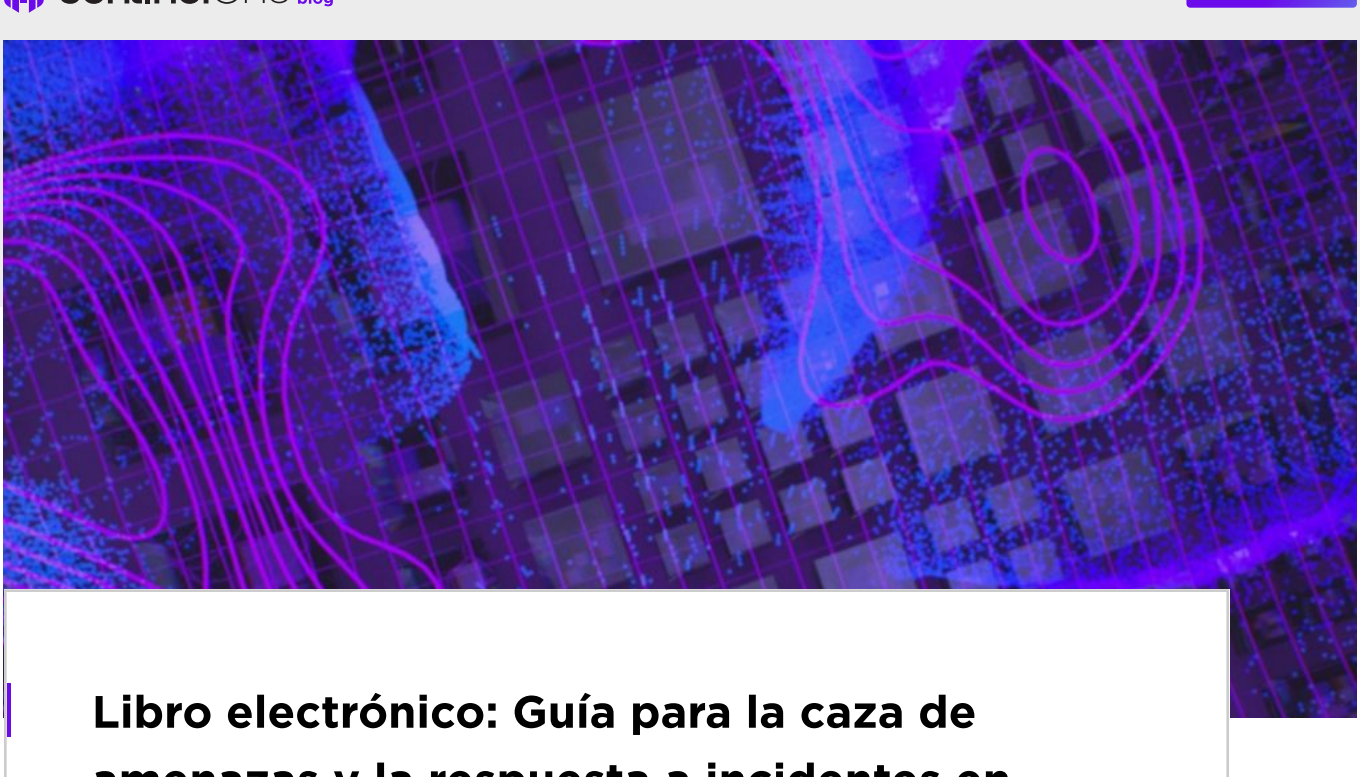
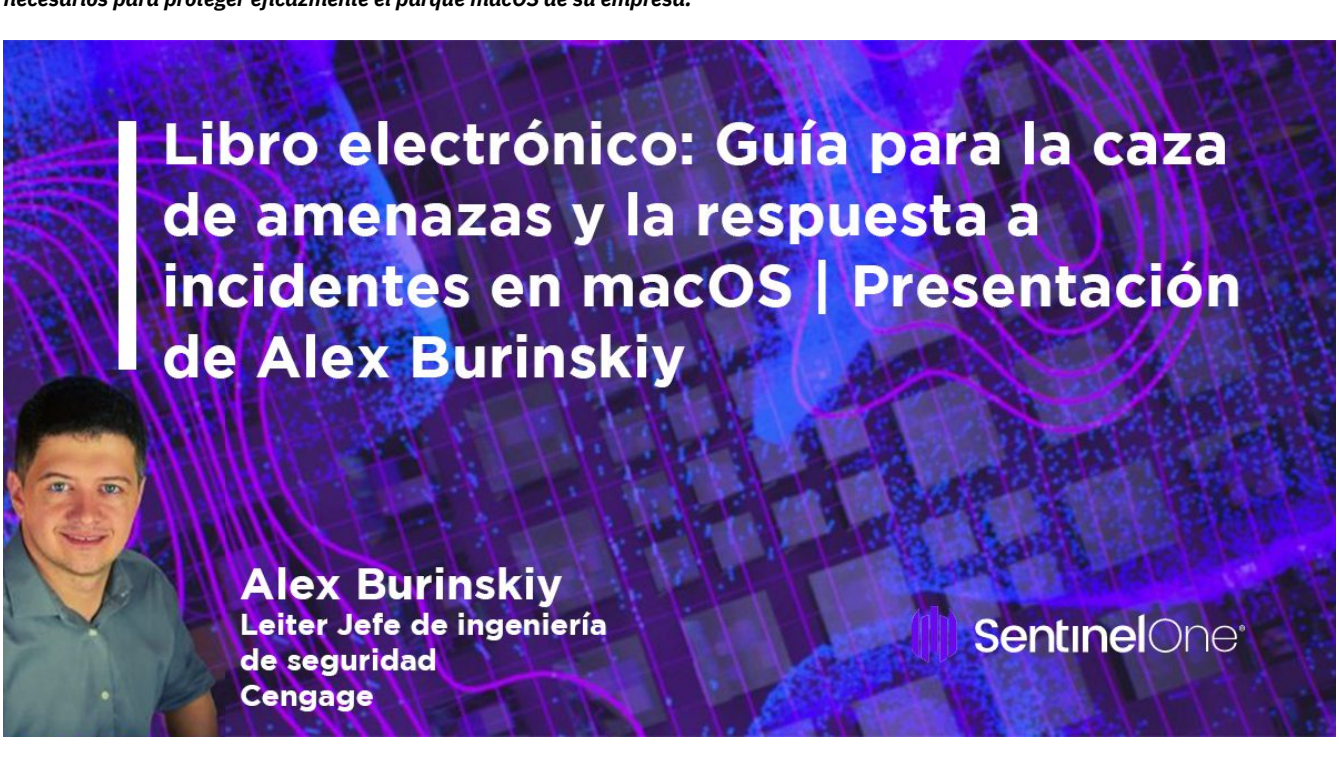


Libro electrónico: Guía para la caza de amenazas y la respuesta a incidentes en macOS | Presentación de Alex Burinskiy

mayo 28, 2020
by SentinelOne

Ante la mayor presencia de macOS en las empresas, los analistas de seguridad necesitan comprender cómo se comporta el malware que ataca a este sistema operativo y cómo identificar los indicios de actividad maliciosa. Esta guía le proporciona los conocimientos necesarios para proteger eficazmente el parque macOS de su empresa.



En Cengage, disponemos de un gran parque de equipos Mac perteneciente a un conjunto todavía mayor de ordenadores de sobremesa, servidores y otros dispositivos polivalentes, todo ello protegido por la plataforma EPP/EDR de SentinelOne.

Los Mac cuentan con una merecida reputación de robustez, longevidad y fiabilidad. Está extendida también la idea de que los Mac no sufren ninguno de los problemas de seguridad que los usuarios de sistemas Windows conocen bien.

Si bien es innegable que el número de casos de malware que afectan a los equipos Mac es claramente inferior al que sufren los sistemas Windows, hay una cantidad nada desdeñable de puertas traseras maliciosas, troyanos, adware y PUP en circulación listos para aprovechar cualquier oportunidad de infectar a dispositivos desprotegidos o usuarios imprudentes.

En mi experiencia en el entorno empresarial he observado que muchos usuarios de Mac tienen todavía que desarrollar la prudencia que se ha instalado de forma mucho más generalizada en el mundo de los PC Windows. Desde adoptar una actitud precavida sobre los sitios web que visitan o el software que descargan, hasta tomarse el tiempo necesario para reflexionar un instante antes de conceder privilegios de administrador a procesos de instalación que no deberían solicitarlos, los usuarios de Mac deben, por ellos mismos y por sus empleadores, ser conscientes de que el panorama de las amenazas ha sufrido un cambio significativo para macOS en los últimos años. El número de amenazas bloqueadas por SentinelOne en nuestros endpoints ha aumentado considerablemente, y todo indica que esta tendencia va a continuar.

Este nuevo libro electrónico de SentinelOne responde a una pregunta fundamental para toda persona que utilice un sistema macOS y en particular para los encargados de defender estos sistemas en la empresa: ¿dónde buscar pruebas si creemos haber instalado un software malicioso, ser víctima de un ataque de phishing o haber detectado una intrusión en el sistema? ¿Y qué prueba se debe buscar?

¿Sabía que hay un malware para Mac que entra en reposo cuando se abre el Monitor de actividad y puertas traseras que no recurren a LaunchAgents para persistir? Muchos usuarios de Mac, cuando no la mayoría, lo ignoran por completo.

Este libro electrónico es una guía de referencia completa y un tutorial detallado para identificar las pruebas de la presencia de amenazas en macOS, recopilar datos de la actividad asociada a archivos, sistemas y usuarios, y consultar las bases de datos de Mac más complejas y menos conocidas.

Se trata de un recurso muy útil para toda persona interesada en la seguridad de macOS y lo recomiendo encarecidamente a los lectores.

Alex Burinskiy
Jefe de ingeniería de seguridad
Cengage

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- Ataques mediante la cadena de respuestas de correo electrónico | ¿Qué son y cómo puede protegerse?