Todos conoceréis a **la compañía de seguridad informática ESET**, ya que es una de las más conocidas y líder en el sector de la ciberseguridad. Tiene sede en Bratislava, Eslovaquia, pero en la actualidad cuenta con oficinas en numerosos países. Fue fundada en 1992 y, como bien sabéis todos, uno de sus prodúctos más conocidos y destacados es el famoso software antivirus NOD32. Actualmente su antivirus se encuentra disponible para diversas plataformas, entre ellas GNU/Linux, es por ello que nos ha parecido interesante realizar esta entrevista para conocer un poco más de cerca a ESET…

Concretamente nos ha atendido amablemente **Josep Albors**, el responsable de investigación y concienciación de ESET España. Con él seguimos con nuestra serie de entrevistas a personajes VIPs y empresas del sector tecnológico que iniciamos hace un tiempo. Espero que os estén gustando estas entrevistas y que juntos aprendamos un poco más sobre ellas y sobre los temas que se tratan. Así que sin más esperas, aquí te dejo el contenido:

==========

Isaac: ¿Recomendarías a los usuarios de sistemas UNIX/Linux instalar un antivirus?

Josep Albors: Como usuario de GNU/Linux, macOS y Windows, no veo impedimentos a la hora de instalar una solución de seguridad puesto que apenas afecta al rendimiento del sistema y no solo permite detectar amenazas dirigidas a nuestro sistema. De esta forma, en un ecosistema multiplataforma, seremos capaces de detectar y eliminar amenazas dirigidas a otros sistemas operativos más propensos a sufrirlas y evitarles pasar un mal trago.

Isaac: ¿Veis mejor el panorama de la seguridad en sistemas como GNU/Linux, Solaris, FreeBSD, macOS, etc., que en el caso de Microsoft Windows?

JA: En este punto tendríamos que acotar muy bien a qué nos referimos cuando mencionamos cada uno de estos sistemas. No es lo mismo un GNU/Linux actualizado y bien administrado que un

GNU/Linux obsoleto y con múltiples agujeros de seguridad instalado en un dispositivo IoT que difícilmente recibirá una actualización de seguridad. De la misma forma, no es lo mismo un Windows 10 a nivel usuario que un Windows Server 2016 gestionado por un sysadmin con experiencia.

La situación cambia mucho de un escenario a otro y, si bien Windows ha mejorado bastante su seguridad en los últimos años, a nivel de escritorio sigue siendo el objetivo favorito de los delincuentes (aunque su base de instalaciones también tiene bastante que ver). Por su parte, si bien GNU/Linux apenas tiene amenazas en forma de malware en sistemas de escritorio, en otros entornos donde el sistema viene embebido en dispositivos con capacidades de gestión y seguridad limitadas y que se distribuyen por millones la situación es bastante preocupante.

En lo que respecta a macOS, hemos visto cómo las amenazas dirigidas a esta plataforma han ido creciendo lenta pero imparablemente en los últimos años, por lo que los usuarios de esta plataforma harían bien en considerar la seguridad de sus sistemas como algo esencial.

Isaac: …¿y en el caso de Android e iOS?

JA: A pesar de que estos dos sistemas operativos tienen a UNIX como ancestro en común, la dominancia de Android sobre iOS también ha hecho que los delincuentes se centren en la plataforma de Google. En este punto también afectan las políticas de aprobación y revisión de aplicaciones en las tiendas de aplicaciones oficiales de cada empresa, siendo las de Apple mucho más restrictivas y limitando por tanto el número de aplicaciones maliciosas encontradas con respecto a las que se detectan en Android.

Isaac: ¿Cómo pensáis aportar mayor seguridad para el IoT?

JA: Desde hace un par de versiones las soluciones de ESET cuentan con una herramienta de monitorización de la red doméstica. Esta opción permite analizar el router y otros dispositivos inteligentes en busca de vulnerabilidades conocidas, ofreciendo sugerencias para solucionarlos. Además contamos con una solución gratuita específica para Smart TV y otros dispositivos con Android TV que protegen frente amenazas orientadas a esta plataforma.

Sabemos que la seguridad del Internet de las Cosas es un tema que hay que tener muy en cuenta y estas características incluidas en nuestros productos son solo el principio. Seguimos investigando y desarrollando soluciones que se adapten a las necesidades de este peculiar ecosistema y esperamos contribuir a hacer del IoT un lugar más seguro.

Isaac: ¿Puede una empresa antivirus hacer algo en cuanto a la privacidad? No me refiero solo evitar ataques en un sistema, sino, por ejemplo, evitar que ciertas app recopilen información del usuario, o evitar eso que algunos desarrolladores y empresas están denominando “telemetría bidireccional”…

JA: No es solo que pueda si no que debe ayudar a proteger la privacidad de sus usuarios. En el caso de ESET detectamos las aplicaciones que son claramente maliciosas y, en el caso de ser una aplicación legítima pero que afecta a nuestra privacidad de alguna forma negativa de la que tengamos constancia, avisamos al usuario de que está intentando descargar o instalar una aplicación potencialmente indeseable.

Isaac: ¿A qué otros retos o desafíos os estáis enfrentando últimamente en cuanto a ciberseguridad?

JA: A pesar de que muchos delincuentes son bastante vagos y apenas innovan en la creación de malware, existen unos pocos a los que les gusta ponernos las cosas difíciles. Amenazas como las

que no utilizan ningún archivo malicioso y utilizan herramientas del sistema como PowerShell o aquellas que utilizan terceros de confianza para propagarse y además cuentan con certificados legítimos son una peligrosa amenaza porque hacen que los usuarios bajen la guardia y permiten saltarse algunas medidas de seguridad.

Isaac: ¿Cómo pueden contribuir los usuarios a denunciar o reportar código malicioso?

JA: Se puede contribuir de varias formas, tanto enviando esas muestras a servicios de análisis como Virustotal (que luego las comparte entre las diferentes casas antivirus asociadas) hasta enviárnoslas directamente a nuestros laboratorios por correo electrónico a samples@eset.com.

Isaac: ¿Por qué algunos antivirus se han puesto bajo sospecha y se han descartado para ser instalados en ciertos sistemas gubernamentales? Todos conocemos el caso de una conocida firma de antivirus que ha sido rechazada por Europa. Sé que es porque a los antivirus se les da permisos totales, y eso puede ser un arma de doble filo, pero me gustaría conocer vuestra opinión…

JA: No especulamos sobre lo que hacen otros fabricantes pero ESET, como empresa ubicada en la Unión Europea, cumple con todas las regulaciones vigentes y está totalmente comprometida con la seguridad de sus usuarios. De la misma forma, estamos en contra de la utilización de amenazas aun con supuestas finalidades legales y, por ende, las detectaremos como ya hemos hecho con anterioridad tanto si las desarrollan un grupo de criminales como un gobierno u organismo oficial.

Isaac: ¿Los antivirus para Linux son un simple port de los antivirus para Windows? Es decir, ¿se trata del mismo software portado para poder ser ejecutado en sistemas GNU/Linux?

JA: Las versiones de nuestras soluciones de seguridad para GNU/Linux comparten algunas características con las de Windows y macOS pero han sido desarrolladas desde cero para esta plataforma en concreto. De hecho, las soluciones para servidores GNU/Linux permiten una configuración muy amplia para que los administradores de sistemas los configuren a su gusto.

Isaac: ¿El motor de búsqueda de malware en el caso de la versión para Linux detecta virus para Windows, rootkits, y los llamados multiplataforma (Flash, Java,…)? ¿O algo más?

JA: Efectivamente, el motor de análisis es el mismo tanto para GNU/Linux como para macOS y Windows y, por tanto, permite la detección de malware multiplataforma, incluyendo amenazas para sistemas operativos móviles como Android e iOS.

Isaac: ¿Qué aporta su software antivirus para Linux que no aporta la competencia?

JA: Nuestras soluciones de seguridad cuentan con más de 30 años de experiencia y eso se nota en varios puntos clave. Uno de ellos es la capacidad de detección de amenazas y siendo ESET una empresa líder en el sector permite que nuestros usuarios cuenten con una protección eficaz. Además nuestro motor de análisis es de los más rápidos y de los que menos recursos consume por lo que el impacto en el sistema es mínimo.

Isaac: ¿Crees que en un futuro próximo los antivirus serán sustituidos por otras herramientas de seguridad?

JA: Como empresa que lleva más de 30 años en este sector hemos oído esa pregunta unas cuantas veces. Sinceramente, creemos que los antivirus como tal hace tiempo que evolucionaron a soluciones de seguridad más complejas y preparadas para lidiar con las amenazas más avanzadas. Cómo evolucione cada fabricante es cosa suya pero por parte de ESET seguiremos apostando por

una solución multicapa que les siga poniendo las cosas difíciles a los creadores de malware, siempre teniendo en cuenta la mejor tecnología disponible en cada momento.