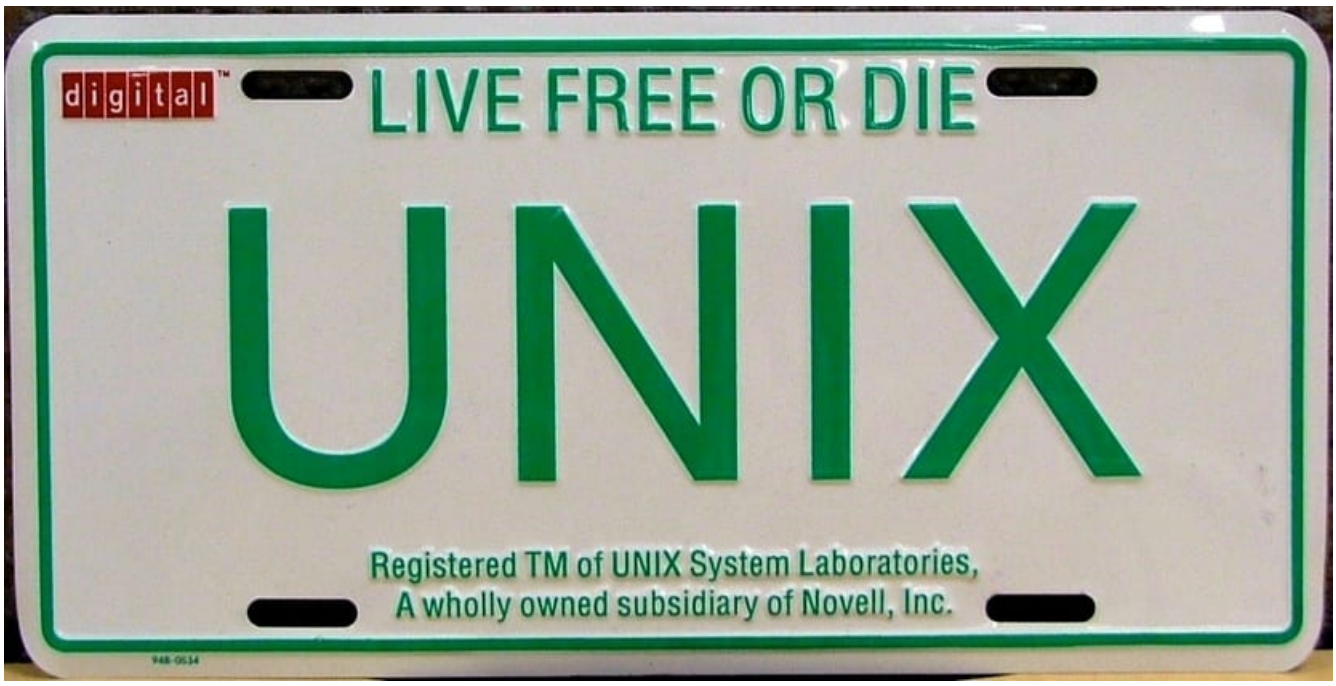
AVAST Software es una empresa bastante conocida en el ambito de la seguridad, ya que es la responsable de uno de los antivirus más conocidos, con una importante cuota de mercado en cuanto a este tipo de productos. Además, también en el mundo del código abierto se la conoce por algunos de sus proyectos y compromisos con esta forma de entender el software. Ejemplo de ello es el repositorio de GitHub que tienen…

La compañía fue constituida en 1990 y desde entonces muchas son las noticias y desarrollos que han copado. Entre sus miembros, se encuentra **el español Luis Corrons**, que es el que ha sido tan amable de responder a nuestro cuestionario en exclusiva para todos los lectores de Isaac. Él desempeña la labor de Security Evangelist de AVAST, como sabéis los «evangelists» están muy de actualidad en el sector tecnológico por la labor que desempeñan. Si queréis conocer un poco más sobre la opinión corporativa de AVAST y Luis, cotinúa leyendo…



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

Luis Corrons: Nosotros siempre recomendamos a los usuarios instalar una solución de seguridad en cada dispositivo posible, y en el caso de los servidores Linux de empresas, ellos deben siempre estar protegidos. Algunos sistemas pueden parecer más seguros que otros, pero hay muchas amenazas multiplataforma, como el phishing, que puede infectar usuarios en cualquier sistema, o engañar a usuarios consiguiendo información sensible, como credenciales de la banca online. En el caso de Linux, es importante la seguridad en servidores compartidos, como los de email, SMB, FTP, y HTTP.

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

L.C.: Otros sistemas operativos no son necesariamente más protegidos que los Pcs, solo que hay menos usuarios no-Windows que usuarios Windows en el mundo. Esto hace que los usuarios no-Windows sean menos deseados como objetivos, porque el target pool es más pequeño.

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

L.C.: Los usuarios de iOS tienen menos riesgo de ser infectados vía apps que descarga, ellos no descargan apps fuera de la tienda oficial Apple App Store y esas apps pasan a través de extensos chequeos de seguridad. Sin embargo, la ingeniería social, una táctica popular usada por cibercriminales que quieren engañar a la gente para que cedan información personal o descargar malware para infectar haciéndose pasar por algo útil o inocente, pueden afectar a los usuarios de todas las plataformas.

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

L.C.: AVAST ofrece Wi-Fi Inspector en versiones gratuitas y de pago, permitiendo a los usuarios realizar escáneres de amenazas de seguridad de la red doméstica. La función alertará al usuario si ellos usan una contraseña débil o por defecto, o si uno de los dispositivos conectados a la red de casa tiene vulnerabilidades. AVAST da a los usuarios tips sobre cómo resolver el problema, que puede incluir, por ejemplo, configuración para fortalecer la contraseña, o actualizaciones del

firmware de los productos.
En la primera mitad de 2019, AVAST también lanzará una nueva plataforma de seguridad Iot, Smart Life, que está basada en tecnología IA para identificar y bloquear amenazas y es entregada a través de un modelo SaaS (Software-as-a-Service) a proveedores de servicios de telecomunicaciones y clientes. Una de nuestra oferta inicial basa en Smart Life es AVAST Smart Home Security, que puede proveer a los clientes protección y visibilidad sobre lo que está pasando en sus redes de casa. Características clave incluyen detección de amenazas de privacidad, botnets, malware así como seguridad para los navegadores y prevención de ataques DdoS (Distributed Denial of Service). La solución está construida en nuestra tecnología IA hecha a medida, y constantemente aprende comportamiento y patrones de uso. Como resultado, posibilita la identificación de hacks vía anomalías en el tráfico con cualquier dispositivo IoT.

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"…

L.C.: Las compañías de antivirus como AVAST, pueden ofrecer herramientas como AVAST Antitrack, que impide que los rastreadores de navegadores creen un perfil de usuario. Más allá de esto, AVAST tiene como objetivo educar a usuarios sobre los riesgos de la privacidad, a través de nuestros canales o medios sociales, como Faceboo, Twitter, blog, donde nosotros regularmente publicamos posts educacionales, así como posts sobre las últimas amenazas.

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

L.C.: Las amenazas dirigidas tanto a los usuarios de PC como a los dispositivos móviles son múltiples, pero principalmente incluyen cryptojacking, ransomware, spyware y troyanos bancarios. Tanto en el móvil como el PC, la mayoría de los programas maliciosos son instalados por usuarios que son engañados por tácticas de ingeniería social. La ingeniería social es una táctica utilizada para engañar a las personas para que realicen ciertas acciones. Los ciberdelincuentes utilizan la ingeniería social para aprovecharse del comportamiento humano, ya que es más fácil engañar a una

persona que piratear un sistema, haciendo que el antivirus, ya sea gratuito o de pago, sea extremadamente importante. En agosto, AVAST impidió que 34,3 millones de ataques infectaran a usuarios de PC en Argentina y 2,2 millones que infectaran a usuarios móviles.

Cryptojacking, es cuando los criminales cibernéticos usan la computadora de las personas para extraer criptomonedas sin permiso. Los delincuentes cibernéticos pueden instalar un software en la computadora de una víctima para minar o usar malware criptográfico basado en el navegador, que se implementa en el código de un sitio web a través de scripts de minería. Cuando un usuario visita un sitio web, el script comienza a minar monedas criptográficas utilizando la potencia informática del visitante. El cryptojacking genera facturas de alta energía para la víctima, un rendimiento deficiente del dispositivo y pérdida de productividad, y tiene un impacto negativo en general en la vida útil de los dispositivos. Como esto se ejecuta basado en el navegador, cualquier tipo de dispositivo que ejecute un navegador puede estar infectado.

El ransomware es un malware que restringe el acceso al sistema o los archivos del dispositivo y exige un rescate para que se elimine la restricción. El ransomware restringe el acceso a todo el sistema o a ciertos archivos al cifrarlos. Los mensajes de rescate a veces parecen provenir de una agencia gubernamental oficial que acusa a las víctimas de cometer un delito cibernético, lo que asusta a muchos a pagar el rescate. El rescate que se exige normalmente solo se paga en las criptomonedas, por lo que el pago no se puede rastrear fácilmente hasta el cibercriminal detrás del ransomware.

Una peligrosa amenaza móvil que está aumentando constantemente son los troyanos bancarios. Los troyanos bancarios son aplicaciones que intentan engañar al usuario para que renuncie a los detalles de su cuenta bancaria simulando ser una aplicación bancaria legítima, por lo general imitando la pantalla de inicio de sesión o proporcionando una pantalla de inicio de sesión genérica con el logotipo del banco correspondiente. AVAST realizó recientemente una encuesta, solicitando a los consumidores que comparen la autenticidad de las interfaces de aplicaciones bancarias oficiales y falsificadas. En España, el 67% identificó las interfaces de banca móvil reales como falsas y el 27% confundió las interfaces de banca móvil falsas con objetos reales. Estos resultados son alarmantes y demuestran que los consumidores pueden fácilmente ser víctimas de troyanos bancarios.

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

L.C.: En algunos casos, solo usando antivirus pueden ayudar a reportar malware. Por ejemplo, hoy, AVAST protege más de 400 millones de usuarios online. Los usuarios gratuitos nos dan acceso a enormes cantidades de datos de seguridad, lo que es realmente clave para el éxito de nuestra tecnología de inteligencia artificial y aprendizaje automático. Nuestra base de usuarios global alimenta nuestro motor de seguridad, que se basa en la IA y el aprendizaje automático, lo que nos proporciona información sin precedentes sobre el ciclo de vida de los ataques ciberńeticos, lo que nos ayuda a mantenernos a la vanguardia y proteger a nuestros usuarios. Además, los usuarios de AVAST pueden enviar archivos y enlaces a sitios web sospechosos directamente a AVAST Thread Labs aquí: https://www.avast.com/es-es/report-malicious-file.php

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…

L.C.: (no han contestado)

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?

L.C.: En este momento, AVAST no ofrece una solución antivirus para Linux para usuarios domésticos.

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?

L.C.: La seguridad Linux debería detectar todos los tipos de malware, incluído aquellos diseñados para Windows, Mac, Linux y multiplataforma.

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

L.C.: En el futuro, los antivirus para dispositivos IoT vendrán en un formato diferente. La masa de dispositivos IoT y sistemas de casas inteligentes son demasiado grandes y diversos como para crear una protección de punto final para todos ellos. Imagina que tienes que instalar una solución de seguridad en todos tus dispositivos inteligentes.

La solución para proteger hogares inteligentes es brindar protección a nivel de red. El router es el centro de la red doméstica inteligente, a la que se conectan todos los dispositivos, y es donde debe comenzar la protección. Como los dispositivos y el tráfico que envían es tan diverso, necesitamos inteligencia artificial para detectar y bloquear amenazas. Los dispositivos IoT y sus actividades y flujos de datos son más predecibles que los de las PC o los móviles, por lo que es muy factible entrenar algoritmos de aprendizaje automático para detectar amenazas. Detrás de cualquier PC, podemos esperar a un ser humano cuyos patrones de comportamiento pueden parecer bastante aleatorios: un usuario puede navegar casualmente por Internet durante un tiempo, y luego comenzar repentinamente a conectarse a un montón de sitios o enviar cientos de correos electrónicos. Sin embargo, si un refrigerador comienza a enviar correos electrónicos, por no mencionar a cientos de miles de ellos, las soluciones de seguridad pueden reconocer que esto es una clara señal de que algo está mal. Y esto hace que sea relativamente sencillo para las soluciones de seguridad establecer una línea de base y detectar anomalías de comportamiento en comparación con esa línea de base.

En Avast, hemos creado una nueva plataforma de seguridad IoT, Smart Life, que se basa en la tecnología AI para identificar y bloquear amenazas y se entrega a través de un modelo de Software como Servicio (SaaS) para proveedores de servicios de telecomunicaciones y clientes. Una de nuestras ofertas iniciales basadas en la plataforma Smart Life es Avast Smart Home Security, que brindará a los consumidores protección y visibilidad de lo que está sucediendo en su red doméstica. Las características clave incluyen la detección de amenazas de privacidad, botnets y malware, así como la navegación segura y la prevención de ataques de Denegación de Servicio Distribuido (DDoS). La solución se basa en nuestra tecnología de inteligencia artificial a medida, y aprende constantemente el comportamiento típico y los patrones de uso. Como resultado, es capaz de identificar hacks a través de anomalías en el tráfico con cualquier dispositivo IoT a medida que ocurren y pueden actuar. Como resultado, por ejemplo, si un termostato inteligente se enciende en un momento inusual y transmite datos en un volumen alto a una ubicación desconocida, podemos actuar al instante para detener el ataque y alertar a la familia sobre la actividad extraña. Y a medida que el espacio de IoT evolucionó, adquirimos conocimientos y, por lo tanto, una mejor capacidad para protegerlo. Después de todo, hay un futuro brillante por delante: donde los dispositivos de IoT realmente pueden brindarnos más comodidad que problemas.

Y con ésta entrevista termina nuestra serie de entrevistas a **compañías de antivirus**, que tendrán un artículo analizando lo que hemos aprendido con el tiempo sobre si debemos o no instalar un antivirus en Linux y sobre lo que nos han comentado en estas entrevistas…Con los datos que he podido sacar de esta entrevista y la de ESET, junto con algunas opiniones que he podido conocer de ingenieros de seguridad de Google o algunos consejos del propio Chema Alonso que he podido leer, el artículo que puede salir es bastante interesante y quizás inesperado para muchos. Como siempre digo, no todo lo que nos dicen es siempre verdad y hay que aprender a filtrar y saber qué podemos dar por válido. Sinceramente pienso que hay bastante desconocimiento entre los usuarios sobre temas de seguridad que espero disipar pronto, al menos en los usuarios de GNU/Linux.