05/10/2023

Noticias de seguridad de esta semana: su automóvil nuevo es una pesadilla para la privacidad



La semana pasada, WIRED publicó una investigación profunda sobre Trickbot, la prolífica banda rusa de ransomware. Esta semana, las autoridades de EE. UU. y el Reino Unido sancionaron a 11 presuntos miembros de Trickbot y su grupo relacionado, Conti, incluido Maksim Galochkin, también conocido como Bentley, uno de los presuntos miembros cuya identidad en el mundo real confirmamos a través de nuestra investigación. ¿Coincidencia? Tal vez. De cualquier manera, es un gran problema.

Además de las sanciones de EE. UU. y el Reino Unido, el Departamento de Justicia de EE. UU. también reveló acusaciones presentadas en tres tribunales federales de EE. UU. contra Galochkin y otros ocho presuntos miembros de Trickbot por ataques de ransomware contra entidades en Ohio, Tennessee y California. Sin embargo, como todos los acusados □□son ciudadanos rusos, es poco probable que alguna vez sean arrestados o enfrentados a juicio.

Si bien los ciberdelincuentes rusos suelen disfrutar de inmunidad, es posible que no ocurra lo mismo con los piratas informáticos militares del país. El fiscal principal de la Corte Penal Internacional (CPI) dice que la CPI comenzará a presentar cargos por crímenes de guerra cibernética. El fiscal Karim Khan no nombró a Rusia, pero la medida surge tras una petición formal del Centro de Derechos Humanos de la Facultad de Derecho de UC Berkeley pidiendo a la CPI que procese a los piratas informáticos rusos Sandworm por crímenes de guerra. Sandworm, que forma parte de la agencia de inteligencia militar rusa GRU, es responsable de provocar apagones en Ucrania, los únicos casos conocidos de ataques cibernéticos que cortaron una red eléctrica. Sandworm también lanzó el malware NotPetya contra Ucrania, que finalmente se propagó a nivel mundial y causó daños sin precedentes por valor de 10 mil millones de dólares en todo el mundo.

Rusia está lejos de ser el único país que se involucra en tácticas ofensivas de ciberguerra. Los piratas informáticos respaldados por China han atacado repetidamente a EE. UU. y otros países, y es posible que estén recibiendo ayuda para encontrar vulnerabilidades sin parches. Una ley china aprobada en 2022 exige que cualquier empresa de tecnología de redes que opere en el país comparta detalles sobre las vulnerabilidades de sus productos con el gobierno chino dentro de los dos días posteriores a su descubrimiento. La información sobre estas vulnerabilidades puede luego compartirse con los piratas informáticos de China. No está claro cuántas empresas occidentales cumplen con la ley o brindan suficiente información para permitir que los piratas informáticos chinos exploten las fallas de los productos.

Hablando de piratas informáticos chinos, Microsoft finalmente explicó esta semana cómo los piratas informáticos patrocinados por el estado de China lograron robar una clave criptográfica que permitió a los atacantes acceder con éxito a las cuentas de correo

electrónico Outlook de al menos 25 organizaciones, incluidas agencias gubernamentales de EE. UU. Según Microsoft, los piratas informáticos irrumpieron en la cuenta de un ingeniero de la empresa utilizando malware para robar tokens. Luego usaron esa cuenta para acceder a un caché de datos de fallas que contenía accidentalmente la clave de firma que luego robaron y usaron para piratear Outlook. Se suponía que nada de esto sería posible y Microsoft dice que ha corregido varias fallas en sus sistemas que permitieron que se produjera el ataque.

Antes de morir en un misterioso accidente aéreo el mes pasado tras un intento de golpe contra el presidente ruso Vladimir Putin, Yevgeny Prigozhin no era sólo el líder de los mercenarios del Grupo Wagner. También fue el jefe de la tristemente célebre Agencia de Investigación de Internet (IRA), una organización rusa responsable de campañas generalizadas de desinformación. Si bien se informó que el IRA fue cerrado, una nueva investigación muestra que los trolls pro-Prigozhin continúan impulsando su agenda. Muchas de las cuentas que difunden desinformación en X (anteriormente Twitter) han sido prohibidas. ¿Pero desde cuándo eso los ha detenido?

En otro lugar, explicamos cómo los ataques de inyección rápida contra chatbots de IA generativa como ChatGPT aprovechan una falla que es difícil de solucionar. Detallamos lo difícil que es optar por no permitir que Facebook use sus datos para entrenar su IA. Tenemos un resumen de Proton Sentinel, un conjunto de herramientas similares a las que ofrece Google pero con un fuerte énfasis en la privacidad y la seguridad. También publicamos una historia con The Markup sobre la búsqueda de Axon para construir drones armados con Taser. Y obtuvimos información privilegiada sobre una reunión entre los principales espías estadounidenses y grupos de libertades civiles sobre la Sección 702 de la Ley de Inteligencia y Vigilancia Extranjera, que expirará a finales de año.

Pero eso no es todo. Cada semana, reunimos las noticias sobre seguridad y privacidad que nosotros mismos no cubrimos en profundidad. Haga clic en los titulares para leer las historias completas. Y mantente a salvo ahí fuera.

Su coche nuevo es una pesadilla para la privacidad

Las compañías de automóviles están recopilando y vendiendo datos personales extremadamente detallados de conductores que no tienen una forma real de optar por no participar, según un nuevo informe de la Fundación Mozilla. Los investigadores pasaron cientos de horas estudiando 25 políticas de privacidad de las principales marcas de automóviles y descubrieron que ninguna de ellas cumplía con los estándares mínimos de privacidad y seguridad de la fundación.

Según el informe, los automóviles modernos, repletos de sensores hasta el techo, recopilan más información sobre usted que cualquier otro producto en su vida. Saben adónde vas, qué dices y cómo mueves tu cuerpo. La política de privacidad de Nissan, por ejemplo, permite a la empresa recopilar y compartir la actividad sexual de los conductores, datos de diagnóstico de salud e información genética, según el informe.

El ochenta y cuatro por ciento de las marcas estudiadas por los investigadores comparten o venden este tipo de datos personales, y sólo dos de ellas permiten que los conductores eliminen sus datos. Si bien no está claro exactamente a quién comparten o venden datos estas empresas, el informe señala que existe un mercado enorme para los datos de los conductores. Un corredor de datos automotrices llamado High Mobility citado en el informe tiene una asociación con nueve de las marcas de automóviles estudiadas por Mozilla. En su sitio web, anuncia una amplia gama de productos de datos, incluidos datos de ubicación precisos.

Esto no es sólo una pesadilla para la privacidad, sino también para la seguridad. Volkswagen, Toyota y Mercedes-Benz han sufrido recientemente filtraciones o violaciones de datos que afectaron a millones de clientes. Según Mozilla, los automóviles son la peor categoría de productos para la privacidad que jamás hayan analizado.

Actualice su iPhone: Apple corrige los días cero sin clic

Apple acaba de lanzar una actualización de seguridad para iOS después de que investigadores de Citizen Lab descubrieran una vulnerabilidad de cero clic que se utiliza para entregar software espía Pegasus. Citizen Lab, que forma parte de la Universidad de Toronto, llama a la cadena de exploits recién descubierta Blastpass. Los investigadores dicen que es capaz de comprometer los iPhone que ejecutan la última versión de iOS (16.6) sin que el objetivo siquiera toque su dispositivo. Según los investigadores, Blastpass se envía al teléfono de la víctima a través de un iMessage con un archivo adjunto de Apple Wallet que contiene una

imagen maliciosa.

El software espía Pegasus, desarrollado por NSO Group, permite a un atacante leer los mensajes de texto de un objetivo, ver sus fotos y escuchar llamadas. Se ha utilizado para rastrear a periodistas, disidentes políticos y activistas de derechos humanos en todo el mundo.

Fuente: www.wired.com

LINK DE LA NOTICIA