uno de los mercados underground más importantes en la actualidad donde se vendía acceso a máquinas infectadas ha sido encauzado por el FBI brindándonos información muy interesante sobre los servicios que ofrecían Y cómo operaban esta vez grabando solo pero en la mejor compañía que se puede tener tú querido oyente comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 28 de abril de 2023 este es el episodio número 92 yo soy Martín vigo Y hoy no está conmigo Alexis porros Así que será un episodio entre tú y yo querido oyente los dos solos Charlando sobre ciberseguridad te parece buen plan porque a mí la verdad es que sí empezaré comentando pues como siempre la pregunta del episodio anterior que era la siguiente estarías de acuerdo en que las grandes empresas tecnológicas pudieran contratar a personal que ha trabajado antes para compañías que han ofrecidos servicios de dudosa legalidad a organizaciones gubernamentales teníamos cuatro opciones que os habíamos dado en Twitter que era Somos todos iguales Sí pero no a gobiernos Sí si se los monitoriza y no nunca Y la verdad es que la respuesta son bastante iguales la única que fue menos votada fue la de Sí pero no a gobiernos bastante curioso y bueno lo siguiente como siempre agradecer a todos los que nos apoyáis con el podcast no solo a los que nos dejáis reviews y comentarios y estrellitas y todo y likes y todo eso que de verdad ayuda un montón pero queremos dar las gracias especialmente a nuestros mecenas de patreon que son los que ponen ahí la pasta para que podamos pagar Editores para que podamos pagar lo que nos cuesta el seguir haciendo este podcast y poder seguir dándolos de manera gratuita también no podríamos hacer esto sin nuestros queridos sponsors como es brawler pro una herramienta la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera totalmente gratuita y vas a obtener paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y también una visión completa de tu infraestructura en todas las regiones de aws y tendrás todos los resultados en apenas unos minutos Así que ya sabes empiezo a usar brawler pro y beneficiarte de sus resultados visitando tierra de hackers.com barra brawler prowlerpro y también darle las gracias a monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com monadd.com y mandarles vuestro currículum a tierra de hackers @monat.com con esto ya yo creo que damos paso a la noticia eso sí no sin antes recordaros que V sites Barcelona solo está a un mes y que podéis ya comprar las entradas y os recomendamos que las compráis cuanto antes Por si se agotan y podéis hacerlo en visites punto Barcelona vs Barcelona va a ser una conferencia muy guapa y tierra de hackers yo voy a estar por allí Así que no faltéis Bueno vamos con la noticia qué os parece la noticia que os traigo Hoy va sobre la incautación de los servidores que hosteaban uno de los mercados ilegales underground más importantes de la actualidad hablamos de Genesis Market una web donde podías ir y comprar acceso a miles de hecho millones de ordenadores comprometidos para llevar a cabo tus actividades criminales usandolos como proxys o bueno robar todo el contenido almacenado en el ordenador o vamos lo que se te ocurriera hacer en una vez tienes acceso completo a un ordenador ajeno en lo que el FBI denominó operation Cookie Monster o monstruo de las galletas ha sido necesaria la colaboración de múltiples cuerpos y fuerzas de seguridad del estado de varios países en todo el mundo incluyendo la guardia Civil Española Por cierto y que han sido coordinados por europol si ahora mismo fueras a la web de Genesis

Market verías una imagen así en plan grande con los logos del FBI y demás fuerzas y cuerpos de seguridad del Estado diciendo en grande this Website hasving sized o lo que viene a ser esta web ha sido incautada Pero eso no es todo hay un breve texto que que por eso lo menciono que me gustaría destacar dice lo siguiente los dominios de Genesis Market han sido encautados por el FBI en base a una orden de registro mandada por el estado del distrito americano del distrito de Wisconsin estas incautaciones han sido posibles gracias a la cooperación internacional de agencias policiales en conjunto con el sector privado es decir han tirado de empresas privadas de ciberseguridad para ayudar con la investigación esto es bastante Interesante pero aquí viene lo guapo para saber si ha sido una víctima visita jefaving pound.com o po lite.nl/ecrhack y bueno lo siguiente que dicen es lo que a mí más me ha llamado la atención el último párrafo que dice lo siguiente has estado activo en Genesis Market has estado en contacto con los administradores de Genesis Market mándanos un email estamos interesados FBI mw Genesis arroba FBI punto gob O sea que aquí tenemos al FBI en la web que acaban de incautar poniendo un mensaje que Oye si tú eres uno de los que lo usaba o conocías alguno de los administradores que llevaban esta página web Este mercado de material ilegal te pongas en contacto con ellos Mándales un mail o sea básicamente te están pidiendo que seas un chivato no por un lado pero bueno tiene sentido Porque seguramente quiero pensar que si colaboras pues te eximen no de responsabilidades porque va a ayudar con esta investigación muy interesante también mencionar el tema este de para saber si ha sido una víctima visita jefa Big point.com o polay.n.l/ec para muchos de los oyentes Yo sé que ya conocerán el servicio de inpound pero me parece un momento es perfecto para darlo a conocer a los oyentes que no conocen este servicio jefaving pound que os dejo un enlace en las notas del episodio es un servicio de que creó un investigador con muchísima reputación llamado Troy Hunt y que básicamente recolecta todos los nombres de usuario y contraseña que se van exponiendo por internet pues en mercados underground como este pero lo hace con un propósito positivo no para venderlo No para utilizarlo de manera ilegítima sino para alertar a las víctimas cuando compra o accede o obtiene estas listas de usuarios y contraseñas hackeadas lo que puedes hacer es suscribirte a su servicio y si detecta en la lista de nombres de usuarios y contraseña tu email te mando un mail automáticamente notificándote que tu nombre usuario y contraseña están han aparecido una lista que están públicas en internet y que inmediatamente deberías cambiar la contraseña de hecho muchos gestores de contraseña ya funcionan están digamos conectados directamente para que si utilizas una contraseña la almacenas inmediatamente la detecta y te diga esta no la uses que ya la has usado en el pasado y te la han hackeado por tanto básicamente el FBI lo que ha hecho ha sido compartir la información de todas las víctimas que tenían a la que tenían acceso desde Génesis Market y dársela al servicio a jefaving pound esto es muy interesante porque yo no sabía que el FBI había colaborado alguna vez con con Troy Hunt para esto pero esto está muy bien porque eso quiere decir que ahora si tú tenías configurado este servicio pues te puede alertar ya no solo que tu contraseña haya sido comprometida sino que estaba a la venta en un mercado totalmente abierto a cualquiera para comprar acceso a tu propio ordenador de hecho tanto es así que a veces para que os hagáis una idea las estas listas están protegidas las marcan como High resh digamos que en FIFA Bin pound ciertas listas de números de usuario y contraseñas que cualquiera puede poner un email y ver si ha sido infectado Pero hay otras que se digamos que por alto riesgo ya sea para la privacidad o por la sensibilidad de del servicio comprometido tú no puedes consultar el email de otros solo puedes consultar tu propio email o soy un ejemplo claro el de Ashley Madison esta era una web que ya le hemos hablado en el pasado que era estaba orientada es el tinder para la gente casada estaba orientada para ser infiel a tu pareja Pues bueno hackearon las bases de datos y publicaron nombres de usuario y contraseña

que los nombres de usuario eran emails por tanto yo ahora puedo ir a poner tu email y ver si en FIFA Bin pound estaba presente en esa web y por tanto saber que le está siendo infiel a su pareja Pues esta lista como ejemplo se marcó como hybrisk y por tanto Yo solo puedo verificar que mi propia contraseña si está ahí o no pues esto mismo hicieron pero con Génesis Market menciona que si bien el FBI solo le entregó emails y contraseñas el dataset es decir lo que el FBI obtuvo Al haber incautado los servidores y toda la información de Genesis Markets contienen realidad también números de teléfono direcciones físicas e información completa de tarjetas de crédito O sea que imaginaros menudo tesoro hablan de millones de ordenadores comprometidos Y por supuesto que toda esa información estaba a la venta antes de que el FBI interviniera millones de ordenadores Pero hay un detalle más que hace a este mercado underground especial Algo que marca la diferencia respecto a la venta tradicional de combinar combos no de usuarios y contraseñas algo que de verdad eleva Este mercado el Genesis Market a nivel profesional en cuanto al acceso ilegítimo a sistemas ajenos el finger printing concretamente la inclusión de detalles del fingerprinting del ordenador comprometido en conjunto con el nombre de usuario y la contraseña o directamente las cookies hoy en día las webs más importantes como puede ser las redes sociales Gmail bancos etcétera no sólo se basan en el nombre de usuario y contraseña para dejarte acceder a tu cuenta se fijan en las características de tu navegador al máximo detalle para asegurarse que eres realmente tú quien está intentando acceder a la cuenta y no alguien que te ha robado el nombre de usuario y contraseña Esto está muy bien es una medida adicional de seguridad que evita muchísimo fraude porque seamos sinceros está la orden del día el robo de contraseñas o simplemente gente que reutiliza la misma contraseña en todos lados y por tanto son muy fáciles de comprometer otros servicios por tanto los servicios online se han puesto las pilas y han querido dificultar la tarea a los cibercriminales obligándoles no solo a robarte el nombre de usuario y contraseña sino también las características de tu navegador Imagínate que oidor oyente que quieres entrar en un club privado en una discoteca y la contraseña es Ábrete sésamo No la que te digo Siempre tú vas allí dices la contraseña y entras porque la contraseña es el secreto para entrar y si alguien te roba esa contraseña pues podrá entrar haciéndose pasar por ti es decir si yo te escucho decir Ábrete sésamo en la puerta Pues luego voy yo y digo Ábrete sésamo pero imagínate ahora que aparte de tener que decir la contraseña delante de la puerta el portero observa Cómo vas vestido y ve que no estás vestido como suele estar vestido el dueño de la contraseña ha analizado las características de tu vestimenta a mayores de la contraseña que le has proporcionado y a pesar de que le has dado la contraseña adecuada no te deja entrar porque sospecha basándose en tu vestimenta que tú no perteneces a esa exclusiva a ese club exclusivo que tú no eres la persona el dueño de esa contraseña pues esto sería la analogía no es suficiente que un delincuente entre en tu banco con tu nombre de usuario y contraseña has de hacerlo con el navegador parecido al tuyo configurando la zona horaria a la misma que tiene la víctima la configuración de la resolución de la pantalla a la misma que tiene la víctima tener los mismos plugins instalados en el navegador que la víctima ya te haces a la idea No pues bien Génesis Market vendía también esta información Génesis Márquez No solo vendía el Ábrete sésamo sino también la ropa que tienes que ponerte para entrar en el club privado Dicho de otro modo Génesis Market te daba la contraseña y la información del finger printing de la víctima para que cuando accedieras a su banco correo electrónico o redes sociales estos servicios no sospechasen pero Espérate que esto Esto es muy profesional porque Pensarás que tener que configurar todos los detalles en tu navegador sería una pesadilla no tener que cambiar la configuración de tu de tu navegador para que fuese igual al del navegador de la víctima Génesis Market tenía un plugin para el navegador que automáticamente ajustaba todos los detalles de tu navegador para que se pareciese al de la

víctima no tienes que hacerlo a mano disfrazaba tu Chrome tu Internet Explorer tu firefox de tal manera que fuera indistinguible del navegador que usaba la víctima para acceder a sus cuentas incluyendo Las Cookies de sesión para que incluso ni hiciera falta saber nombres de usuario contraseñas súper Pro esto Y es que lo creas o no es muy difícil tener un finger printing único esto lo saben muy bien en la industria de la publicidad online que nos rastrean a través del finger printing de nuestros navegadores tú puedes pensar que tienes una configuración lo más típica posible en Windows en el navegador Chrome y poco más no como deben de tener millones y millones y millones de personas lo que pasa es que hay muchísimos más detalles a los que pueda acceder una página web como Google o Facebook tu zona horaria la resolución de tu pantalla el idioma de tu ordenador las versiones específicas de tu navegador el tipo de fuentes que tienes instaladas y un larguísimo etcétera si quieres ver lo único que eres en el mundo y Qué características son las que te están haciendo único te dejo un enlace muy bueno a una web que analiza tu navegador y te da un informe todo esto de manera gratuita en la web es my unique.org y ir allí con vuestro navegador y ya veréis yo fui con el mío y evidentemente yo que tengo tantos plugins de privacidad y todo esto pues era único entre millones y millones de personas también os dejo un enlace a un paper interesantísimo sobre lo que se conoce como impass o impersonation assassorbes que es exactamente lo que estaba haciendo Génesis Market facilitarte al máximo modificar tu finger printing para hacerte pasar por otra persona y no os creáis que el acceso a un ordenador ajeno era muy caro de hecho como todo supermercado muchas veces tenían ofertas en la web con unos 30 euros ya podías comprar acceso a un ordenador 30 euros De nada imagínate el daño que puedes hacer cuando estás en el ordenador de otra persona con acceso absoluto o en su correo electrónico o en su banco el malware que utilizaban venía empaquetado de varias formas me encontré haciendo un poco más de búsqueda sobre esta noticia un análisis súper detallado de la empresa sector Seven análisis del malware y las extensiones del navegador usadas que os dejo las notas del episodio de hecho utilizaban también extensiones de navegadores plugins maliciosos para ir robando todo el fingerpring del navegador de la víctima O sea no sólo teníamos el plugin de navegador que utilizaban los que los clientes de Genesis Market sino plugins de navegador maliciosos que eran con los que infectaban los navegadores de las víctimas o sea súper Pro esto pues sector Seven analizó una muestra que obtuvieron de una víctima que bueno Esto me llamó bastante la atención curiosamente intentaba instalar un antivirus de pago sin pagar y Para ello se bajó el típico crack de internet para que fuera gratis que en realidad era el malware de Genesis Market y lo que hacía era desinstalar el antivirus que acaba de instalar e instalarle un programa malicioso tenéis todos los detalles en el reporte pero algo que me llamó la atención es que el programa malicioso venía con dos imágenes en bebidas digamos dentro del ejecutable que no se usaban para nada Y qué imágenes pensáis que son pues una de Lebron James el famoso jugador de baloncesto y otra de la bandera del arcoíris usada por la comunidad lgtb muy Random esto Supongo que yo que sé los creadores del malware y querían hacer entender que Lebron James es gay o algo así no sé pero esas dos imágenes mencionan el reporte que están dentro del ejecutable del malware pero no se utilizan para absolutamente nada bueno queridos oyentes este ya sabéis que es un episodio más corto de lo normal porque estoy yo solo pero o quiero terminar con la pregunta de este episodio a ver una pregunta que a lo mejor te haces a ti mismo un poquito de doxing Pero bueno no tienes por qué haber utilizado un mercado para comprar cosas ilegales Pero la pregunta es has comprado alguna vez en uno de los mercados underground que se pueden encontrar por internet Así que házmelo saber si sí o si no en Twitter @tierra de hackers y hasta aquí Hemos llegado Qué te ha parecido este episodio de tú a tú querido oyente Solo estoy yo hablando de estas cosillas que tanto nos gustan si te ha gustado por favor Te agradecería un montón que te suscribas al podcast si no lo

Estás todavía que hemos visto por ahí por Apple podcast que hay mucha gente que nos escucha miles de personas pero no están suscritos que nos deje reviews que los compartes con tu compañeros lo que te pedimos siempre porque con eso conseguimos crecer Con eso conseguimos más visibilidad y con eso conseguimos que podamos seguir adelante dedicándole las horas que esto lleva y trayéndote toda la actualidad Muchas gracias y nos vemos y nos escuchamos en el próximo episodio Adiós adiós si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers