75. Robots Asesinos y Mars Stealer

los mayores fabricantes de robótica a nivel mundial piden en una carta abierta que no se añada armamento a sus robots mientras que en San Francisco la policía ha empezado a hacer Justo eso bajo el amparo de la ley una empresa de ciberseguridad se toma la justicia por su cuenta y abusa de una vulnerabilidad en servidores del malware de robo de datos Marx steeler para quitarle el control a sus operadores y liberar a sus víctimas con una semana de pausa por medio para migrar nuestro podcast ya estamos de vuelta con un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 4 de diciembre de 2022 este es el episodio número 75 yo soy Martín vigo y está conmigo dos semanas después y tras lidiar con varios problemas migrando el podcast Alexis porros Hola Alexis qué tal pues muy buenas Martín aquí andamos como dices a medias entre mcgiver y el inspector Gadget tocando cables en los servidores del podcast para dejarlo fenomenal y seguir publicando episodios para nuestros oyentes Y como siempre agradeceros a vosotros nuestros queridos oyentes el seguimiento que nos hacéis en todos sitios en redes sociales en estando conversando con nosotros en el servidor de discord vía email donde nos enviáis sugerencias y preguntas Incluso en las plataformas de podcast Muchas gracias de verdad y os recordamos que si no lo estáis debería estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita a modo de recordatorio donde estamos en redes sociales Twitter Instagram y Facebook con el handle@tierra de hackers linking YouTube y Twitch como tierra de hackers correos electrónicos no los podéis enviar a podcast arroba tierra de hackers.com y en discord podéis Acceder al servidor a través de tierra de hackers.com barra discord finalmente como siempre agradecer vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que para el episodio anterior fue la siguiente Te parece bien que una entidad gubernamental tenga la capacidad de decidir qué es y qué no es desinformación hasta el punto de tener la capacidad de pedir que se elimine teníamos tres respuestas en este caso la más votada con un 37% fue que no por debido a la libertad de expresión con un 33% no reguladores a políticos y con un 30% tenemos Si es un problema gordo así que ya vemos que dos tercios están en contra y un tercio está a favor Pues sí yo continúo como siempre dando las gracias a nuestros mecenas de patreon la gente los oyentes que nos apoyan en patreon económicamente para poder cubrir un poco los gastos que tenemos con el podcast específicamente quiero mencionar a David Alejandro que se acaba de unir a nuestro grupo de mecenas y se acaba de hacer un hacker social Muchísimas gracias David por apoyarnos te lo agradecemos muchísimo también agradecerle a nuestros sponsors monat aprovecho como siempre ya sabéis para deciros que están buscando a ingenieros y expertos para ayudarles con su misión que es hacer la seguridad más accesible y transparente nosotros lo hacemos a través de un podcast Pero ellos lo hacen a través de herramienta de gestión y visualización de telemetría de datos de seguridad están en silicon Valley pero ya sabéis están buscando gente por todo el mundo con un expertise en temas de ciberseguridad Así que les podéis contactar en el correo tierra de hackers @monat.commod.com y yo creo que empezamos ya con la noticia Para no perder más tiempo y esto es una noticia que os traigo Aunque en realidad la tengo en el tintero hace un par de meses ya de en octubre concretamente cuando vi que Boston dynamics publicaba una carta abierta en su blog si os acordáis Boston dynamics es esta empresa que está detrás de estos vídeos tan espectaculares no de robots haciendo volteretas gimnasia rítmica parkore pues pues esta

carta está afirmada no solo por ellos sino por otros de los mayores fabricantes de robótica del mundo fabricantes como Open roborics agility roborics unitry clears revolex y Annie botics Que bueno que tienen los nombres así son poco originales Pues esta carta abierta estaba dirigida al público en general pero sobre todo a los gobiernos del mundo y qué dice esta carta Pues que estos fabricantes de robots que son Pioneros en el mundo como decía piden que no se añada armamento a estos robots Cómo se te queda el cuerpo repito las principales fabricantes de robots están pidiendo a los gobiernos del mundo que por favor no les pongan pistolas metralletas o explosivos a robots porque es un peligro para la sociedad os Leo un par de párrafos Pero por supuesto os dejo la carta entera enlazada las notas del episodio para que os hagáis una idea de que va esta carta uno de los párrafos dice lo siguiente creemos que Añadir armas a robots que son otro lado remotamente o autónomos que cualquier persona los puede comprar y que son capaces de acceder a lugares donde previamente no podían como hogares Y lugares de trabajo eleva las preocupaciones y riesgos de daños a las personas y también tiene una serie de consecuencias éticas y Morales muy grandes la aplicación armamentística de estos modernos robots dañarán también la confianza de la gente en este tipo de tecnologías por estos razones no apoyamos armar nuestros robots Este es otro párrafo nos comprometemos a no Añadir armas a nuestros robots de uso genérico ni crear software para ese propósito para ser claros no tenemos nada en contra de tecnologías ya existentes que gobiernos y agencias gubernamentales utilizan hoy en día para defenderse pues Estos son dos párrafos que destaco yo que Bueno un poco ya entendéis las intenciones de que están intentando hacer estos fabricantes de robótica no como os imagináis cuando vi esta carta me la guardé para preparar una noticia que traeros al podcast Pero como solo era una carta en el momento ahí en octubre Cuando la vi me esperé a que sucediese alguna noticia relevante más para traeros una noticia un poquito más completa no Y ese día ha llegado queridos oyentes en forma de otra noticia que pone los pelos de punta la policía de San Francisco está querida ciudad donde yo vivo utilizará robots para matar a gente remotamente Sí sí esto esto se acaba de votar y aprobar en el parlamento pero vayamos por partes que a veces me gusta un poco soltaros así las cosas no directamente para dejaros un poco volados de la cabeza hace una semana el electronic Frontier foundation o ff que a veces hemos hablado de ellos es que es una organización sin ánimo lucro centrada en los derechos digitales publicaba un post advirtiendo de que en los próximos días se votaría una proposición de ley para permitir a la policía de San Francisco hacer exactamente lo que la Carta abierta que los de los fabricantes que os Acabo de leer pedía no hacer Añadir armas a los robots utilizados ya a día de hoy por la policía concretamente la ley a votar contenía Este párrafo en concreto que define un poco lo que será la ley os lo leo textualmente los robots que aparecen en esta lista no deberán ser utilizados para otro propósito que no sea el entrenamiento o simulaciones detenciones criminales incidentes críticos circunstancias extraordinarias ejecutar órdenes judiciales o para inspeccionar dispositivos sospechosos los robots los robots podrán ser utilizados como una fuerza letal Solo cuando el riesgo de pérdida de Vidas para los ciudadanos o fuerzas policiales sea inminente y sea mejor opción que otras alternativas disponibles para la policía de San Francisco esto es uno de los párrafos de la proposición de ley o sea está escrito Digamos como en modo negativo no en vez de decir se podrá utilizar para esto se dice solo se podrá utilizar para estos casos pero es que ya vemos que esos casos realmente son bastante genéricos por lo menos de la manera que está de redactada y yo ya os digo que como siempre recuerdo que yo no soy un abogado y tenemos que asumir que Martín vigo no tiene ni idea de lo que está diciendo sobre todo cuando hablamos de

leyes Pero bueno el propio electronic Frontier foundation Comenta lo genérico que es Este lenguaje por ejemplo qué es lo que Define una situación extrema o crítica que es lo que justificaría utilizar robots para matar a gente eso se deja criterio de la propia policía de San Francisco para juzgar Son ellos los que van a decir esto es una situación crítica saca el robot para matar al sospechoso claro No está definido específicamente en la propia ley la ley no especifica o define estas situaciones sino que las deja a interpretación y como de lo que hablamos es de usar robots como arma letal pues hombre cuando menos preocupa un poquito No de hecho el ff instaba contactar a los legisladores esto la verdad es que es algo Bastante típico en Estados Unidos para presionar a políticos de tu zona esto yo no lo he visto tanto en España pero en Estados Unidos es bastante común pedir al público Oye Llama a tu a tu gobernador Llama a tu a tu legislador en tu zona en tu ciudad escríbele emails es bastante común allí Pues el ff instaba a contactar para que votasen en contra te daban de hecho el email a donde escribir que era el del propio legislador y te ofrecían un pequeño texto para copiar y pegar si querías y la verdad es que la primera frase de este texto o justificación para votar que no me resultó muy llamativa Y es demoledora dice lo siguiente no deis permiso el departamento policial de Francisco para utilizar robots para matar a gente esta es la primera frase no que están pidiendo que se que se mande a los legisladores la verdad es que es una pasada en ese mundo vivimos ya a alguien más le está viniendo recuerdos de Terminator 2 cuando Sara Connor va por su cuenta no a matar al ingeniero aquel que está desarrollando skynet y lo va a matar precisamente para evitar que lo desarrolle Pues yo creo que con esta noticia nunca hemos estado más cerca es que ya no estamos hablando de la capacidad de armar robots para matar sino de permitirlo los robots ya están ahí y ya tienen esa capacidad ahora ya estamos en la fase de pelearlo a nivel legislativo la verdad es que es de locos De hecho no solo fue el electronic Frontier foundation quien hizo una campaña para conseguir que los miembros del comité votasen en contra el propio fiscal del distrito de San Francisco envió una carta que también os dejo los enlaces del episodio pidiendo lo mismo y os vuelvo a destacar me la leí un solo párrafo de la carta Mañana durante la reunión del comité de supervisores Vais a votar si autorizar o no a la policía de San Francisco a usar los conocidos Como Killer robots el departamento policial de San Francisco ha justificado esta petición en base a la sugerencia de que el uso de robots en vez de agentes ayudará a mejorar la seguridad de la comunidad y los agentes esto es la decisión errónea y utiliza la narrativa del miedo para que puedan crear sus propias normas el comité debería votar en contra de la petición por parte de la policía de utilizar robots para matar a personas la carta es muy interesante y como decía os la deja enlazada y os recomiendo leerla es que entre otras cosas entran Como cada vez la policía en San Francisco y la verdad yo diría en general en Estados Unidos está más militarizada Y estos robots son un paso más hacia la total militarización de este cuerpo que ni es militar ni opera en situaciones de conflicto bélico así que ya veis que son varias los frentes que intentan frenar al comité de darles esta capacidad a la policía de San Francisco Pues bien ya es tarde queridos oyentes la ley fue aprobada a pesar de todo ahora mismo el departamento policial de San Francisco puede utilizar robots controlados remotamente para matar a gente bajo los supuestos que mencioné antes pongamos ahora un poco la nota de sosiego no después de toda esta narrativa tan alarmista por mi parte que siempre queremos dar un poco la otra parte si bien es preocupante que se haya creado justificación legislativa para matar a gente con robots todavía no tenemos terminators por ahí rondando a nivel militar hoy en día ya se mata gente con drones no tripulados por ejemplo que se podría interpretar pues como algo cercano a un robot no digamos Pues un dispositivo electrónico físico con capacidad letal de hecho vi un vídeo la

semana pasada de una empresa dedicada defensa que me dejó los pelos de punta y la estuve buscando y ya no encuentro el tweet es que no tenía que haberlo grabado fallo mío perdonar si no os lo enlazaban las notas pero anunciaban su nuevo mini drone que llevaba una carga explosiva y en el vídeo de demostración Aunque bueno Es renderizado realmente no es un vídeo real se ve como el mini drone se va metiendo por la por una casa vuela por las escaleras al piso de arriba detecta por reconocimiento facial al sospechoso y explota su lado matándolo Esto no es ciencia ficción era un vídeo de un producto que ofrece esta empresa Que de momento está disponible solo para uso militar Y si bien ya se usan drones hace tiempo para combate Este era totalmente autónomo y preconfigurable para entrar en una casa y encontrar automáticamente al objetivo a eliminar y explotar al lado del objetivo o sea Hablamos de un dron autónomo que decide al lado de quien explotar y no que un humano vuele el dron cerca y le da un botón cuando decide el Humano a este es el objetivo Este es otro nivel Y por supuesto abierto a ser hackeado con unas consecuencias mortales y nunca Mejor dicho también pues tenemos robots no que se para desactivar Bombas o inspeccionar vehículos sospechosos que pueden estar abandonados pero Y tenemos esto ya hace tiempo pero son robots muy lentos y controlados remotamente con con un mando a distancia desde la cercanía Con un objetivo muy concreto que simplemente es Deshabilitar Bombas o hacer que exploten no en un en un entorno seguro el problema y volviendo a la Carta abierta de las empresas robóticas es que los robots cada vez son más capaces más autónomos y en general más avanzados Si creamos legislación tan genérica como para decir si puedes usar robots para matar y punto ahí no estamos controlando ni teniendo en cuenta el avance de la tecnología robótica y capacidades de estos robots en fin yo todavía veo el escenario de skynet muy lejos pero también lo veo un pasito más cerca lo dejo con la pregunta del episodio queridos oyentes si vosotros hubiese tenido la capacidad de votar hubierais votado A favor o en contra de que la policía puede utilizar robots armados para matar a personas remotamente y os doy las dos opciones A favor o en contra pues Me he quedado bastante anonadado Martín parece que el futuro ya ha llegado me recuerda a películas de ciencia ficción el tipo chapi o hay robot de Will Smith chapping aunque no tuvo mucho éxito igual no muchos la conocen quería mencionarla porque es digna de mención ya que trata de un futuro muy cercano en el que la policía de Sudáfrica decide comprar robots blindados con el objetivo de reducir el alto índice de criminalidad en johannesburgo y vamos pues son robots a escala humana con pies y brazos que patrullan Sudáfrica como si fueran policías y Bueno hay robots Supongo que todos la conocemos sino de verdad y haberla ahora mismo Bueno después de escuchar acabar el episodio o incluso también Tengo otras dos películas en la mente que me recuerda un poquito Aunque más vanguardistas no tipo Blade Runner con los replicantes no también que mantienen el orden Aunque en un futuro más allá con todo las ciudades tipo Neón y tal no y siempre lluvioso y coches alta tecnología que vuelan y tal o ya más allá la saga de Star Wars que de nuevo Supongo que todos la conocemos y si no muy recomendada con todo esto queridos oyentes hacémonos cuanto antes hay que preparar la resistencia a que bueno el tema tampoco es tan descabellado si lo paramos a pensar detenidamente con los acontecimientos actuales Ya que en algunos países los gobiernos utilizan drones controlados remotamente para lanzar misiles contra objetivos a miles de de distancia no como Estados Unidos por ejemplo o también utilizan robots para desarmar bombas Así que esto sería una mezcla entre los dos casos anteriores comentar que una vez más la guerra Aunque parezca que sea física va a seguir siendo muy importante en el mundo Cibernético ya que los responsables de estos robots tienen que tener cuidado de que personas No autorizadas como

cibercriminales puedan tomar control del robot de forma remota y matar a quien no se debe y ya para cerrar un poquito mis comentarios el siguiente paso que me venía a la cabeza mientras comentabas la noticia Martín y como oportunidad de negocio va a ser que bueno una persona estilo tipo elon musk Crea una empresa de avatares y podamos salir a la calle controlando de forma remota a cuerpos humanos o cuerpos robóticos pero que bueno que nos el contacto con el mundo exterior estando en casita tumbados en el sofá de forma segura al estilo de la película Avatar o la serie de Amazon Prime basada en la obra de William Gibson de periferal o la periferia como se conoce en Latinoamérica todo esto Para estar seguros en casa y evitar que un robot con una mal función de dispare cuando estás caminando por la calle No pues sí Alexis esto de los robots asesinos la verdad es que preocupan dapa muy buen episodio de tierra de hackers Pero bueno que una vez más prefería no tener que quedar de esto a ver cómo evoluciona y un poco lo que mencionaba antes Es verdad que es una pasada Yo cuando vengo a España y veo a agentes de fuerzas y cuerpos de seguridad del Estado pues van vestidos con su uniforme llevan una pistola a lo mejor una porra o así pero que en San Francisco a veces los ves y es difícil distinguirlos de un soldado militar o sea es una pasada allí algunos como como van armados hasta los dientes y tal Y tampoco quiero yo yo nunca he peleado contra el crimen en la calle no quiero que se me malinterprete Pero bueno que sí que que uno se asusta y sé que allí en general pues las armas están más al alcance de todos y puede ser más peligroso que en España pero también el tipo de equipamiento había visto varias noticias en los diarios varios documentales sobre sobre cómo según las fuerzas militares en Estados Unidos van retirando equipamiento en realidad lo que hacen es donárselo a las a la policía de diferentes estados y claro Entonces se va militarizando de esa manera sin tener que gastar dinero pero claro luego es que Y si la función es solo de calle Por así decirlo es una locura ver a veces como Cómo van armados y todo esto pero bueno si se me llama mucho la atención desde luego la diferencia entre pasear por la calle en San Francisco y pasear por la calle en una ciudad española y ver cómo cómo van tanto uniformados como armados las la policía vamos en ambias ciudades una locura en cualquier caso da mucho que pensar que el futuro ya ha llegado como he dicho queridos oyentes y nada ahí está muy buena noticia Martín y Bueno pues vamos con la siguiente noticia pero antes queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace muy poquito acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de prowler pro y sus Ash el servicio gratuito más completo de seguridad para aws está construido sobre la Popular herramienta Open source brawler y además por el mismo equipo de ingenieros si ya conoces prowler que está disponible en github seguro que vas a aprovechar las bondades que ofrece brawler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de WS y podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar prouer pro de forma totalmente gratuita en prauer.proprow l e r.pro desde ya y bueno una vez dicho esto dentro noticia lo que traigo ahora mismo queridos oyentes es una noticia de malware robo de datos y una empresa que ha contraatacado Y es que una vulnerabilidad en los servidores de Mando y control o command en control como se le conoce en inglés el malware Mars steeler un malware de tipo info styler que roba información confidencial de los sistemas que infecta ha permitido a una empresa Privada de ciberseguridad dejar fuera de combate a los cibercriminales Aunque lo dejo Ahí de momento y antes de seguir con la noticia voy a hacer un breve desvío y voy a hablar de lo que son los info steelers pues info stiller es un tipo de malware que se dedica a infectar sistemas

para robar información como la siguiente credenciales almacenadas en los navegadores web incluidas cuentas de portales de videojuegos servicios de correo electrónico y acceso a redes sociales también detalles de tarjetas bancarias y por supuesto información de carteras de criptomonedas y luego envían todos estos datos al operador del malware según la empresa de ciberseguridad Group i.b el malware de tipo styler es el segundo más popular seguido obviamente del tipo ransomware que es el rey de todos los tipos de malware como estamos viendo en la actualidad y de desde hace algunos años no según esta empresa en los primeros 7 meses de este año los operadores de info steeler infectaron a más de 890.000 dispositivos de usuarios en 111 países y robaron más de 50 millones de contraseñas los cinco países más atacados este año fueron Estados Unidos Brasil India Alemania e Indonesia con entre 91.000 y 35.000 dispositivos infectados dependiendo del país los ciberdelincuentes utilizan principalmente a los infosillers Red Line y Raccoon para obtener contraseñas para cuentas de videojuegos como steam roblox y Epic games credenciales de PayPal que se corresponde con el 25% de los datos robados registros de pago los usuarios y tarjetas bancarias y obviamente como he dicho información de carteras de criptomonedas de hecho redline steeler es el malware de robo de datos más popular en la actualidad siendo utilizado por 23 de los 34 grupos de info steelers que rastrea Group ID y se ofrece en alquiler en la Dark web por unos entre 150 y 200 dólares al mes todos los grupos de cibercriminales identificados coordinan sus ataques a través de grupos de Telegram en ruso según el análisis de los grupos de Telegram Durante los últimos 10 meses de 2021 Los tigres delincuentes recopilaron 27 millones de contraseñas 1,2 millones de archivos de cookies que de forma similar a un nombre de usuario y contraseña Las Cookies permiten el acceso a un servicio online o sistema normalmente a través del navegador web también 56.000 registros de pago que inclu tarjetas bancarias y datos de 35.000 carteras de criptomonedas si nos movemos a este año en los primeros 7 meses los actores de amenazas robaron al menos el doble de datos que en 2021 llegando a robar 50 millones de contraseñas 2 millones de archivos de cookies 103 mil conjuntos de registros de pago y tarjetas bancarias y datos de 113.000 carteras de criptomonedas el valor de Mercado clandestino en la Dark web de solo los registros robados y los detalles de las tarjetas bancarias comprometidas es de alrededor de 5,8 millones de dólares según estimaciones del grupo IB de esta forma el malware de robo de información o info stiller se ha convertido en una de las amenazas digitales más graves de este año y por qué es así porque hay tanto interés en info stiller por parte de los cibercriminales Bueno pues el por el provecho que se le pueden sacar a la información robada los operadores que infectan a sistemas con malware info stiller se benefician de múltiples formas la primera es vendiendo la información robada en la Dark web la segunda es aprovechándose de la información robada ellos mismos para bueno impresionar a sus víctimas robarles el dinero de sus cuentas bancarias y cometer otro tipo de fraude financiero y finalmente ofreciendo el acceso a la infraestructura del malware en alquiler para que otros cibercriminales puedan lanzar sus propios ataques en lo que se conoce como inicial Access Brokers o gestores o agentes o corredores como queramos llamarlo de este acceso inicial este último caso de uso es muy común cuando cibercriminales Por una parte no tienen la capacidad de penetrar el perímetro o por otra parte no quieren dedicarle el esfuerzo necesario a ello y directamente compra en el acceso inicial a otros cibercriminales a modo de ejemplo el actor de amenazas responsable del ataque más reciente a Uber compr credenciales comprometidas con el malware infostyler Raccoon para penetrar la red de Uber para distribuir los infoestillers los operadores de malware normalmente dirigen el tráfico a los sitios web de estafa que ellos controlan como cebo que se

hacen pasar por empresas conocidas y convencen a las víctimas para que descarguen archivos maliciosos esto lo hacen utilizando plataformas legítimas para insertar enlaces para que las víctimas accedan a estas webs maliciosas y se puedan descargar el info stiller esto lo hacen a través de enlaces que incluyen en reseñas U opiniones de vídeos de juegos populares en YouTube también lo incluyen en software de minería de criptomonedas ponen estos enlaces también en archivos nft en foros especializados y comunicación directa con artistas de nft y también lo añaden en redes sociales Asociados temas de sorteos y loterías una vez habiendo comentado Qué es un infostiller y el estado actual de amenazas al respecto volvemos al tema del malware Mars steeler el malware Mars Tyler cobró fuerza en marzo de este año tras el desmantelamiento de Raccoon steeler otro malware popular para el robo de datos Y como he dicho es el que permitió acceso al cibercriminal a la red de Uber Así que bastante importante bueno como digo el tema de que Raccoon steeler se dejará de usar Pues condujo a un aumento en las nuevas campañas de Marx steeler incluidos los ataques masivos contra Ucrania en las semanas posteriores a la invasión de Rusia y un esfuerzo a gran escala para infectar a víctimas con anuncios maliciosos en abril de este año los investigadores de seguridad dijeron que encontraron más de 40 servidores que alojaban mando y control de Marx styler este malware Normalmente se distribuye como archivos adjuntos de correo electrónico anuncios maliciosos en páginas o incluso en software descargado a través de sitios que comparten archivos Torrent Así que mucho cuidado con lo que descargáis de las redes Torrent una vez que ha infectado un sistema el malware roba las contraseñas de la víctima y los códigos de doble factor de las extensiones del navegador web así como el contenido de sus carteras de criptomonedas El malware también se puede usar para entregar otras cargas maliciosas tipo ransomware a principios de este año se filtró una copia del malware Marx steeler que permitía cualquier persona crear su propio servidor de Mando y control pero su documentación era incorrecta y guiaba a los posibles malhechores a configurar sus servidores de una manera que exponía los archivos de registro que contenían los datos de usuario robados de los sistemas de las víctimas en algunos casos Incluso el operador se pudo infectar con este malware sin darse cuenta y exponer sus propios datos privados bookward es la empresa de servicios de ciberseguridad con oficinas en el Egipto y Las Vegas Estados Unidos que ha podido tomar el control de los servidores de Marx steeler de las manos de los propios cibercriminales Board dijo que la vulnerabilidad se puede usar para manipular los servidores de Mars stiller para eliminar los datos recopilados de los usuarios infectados finalizar todas las sesiones activas con los sistemas de las víctimas e incluso cambiar la contraseña de administrador del panel web para que los operadores no puedan volver a Iniciar sesión esto significa que el operador pierde el acceso total a todos los datos robados y tendría que atacar y reinfectar a sus víctimas nuevamente a todo esto yo espero que los cibercriminales no tengan una puerta trasera o una contraseña o usuaria adicional si no van a poder volver a retomar el control de los servidores de Mando y control pero bueno parece una hazaña interesante por parte de esta empresa Board esta misma vulnerabilidad también está presente en los servidores del malware hervium otro malware de robo de datos con un modelo de negocio como servicio de alquiler similar al de Marx steeler el malware erbium se vende en uno de los foros de hackers rusos a unos 500 rublos por semana Que son 8 dólares 1500 rublos por mes unos 24 dólares o también 10.000 rublos por año que son 160 dólares el equipo de operadores de erbium también ofrece soporte técnico lo que promete nuevas funcionalidades en el malware en el futuro Board ha descubierto y neutralizado cinco servidores Marx steeler hasta el momento cuatro de los cuales se desconectaron Posteriormente la compañía no está publicando

la vulnerabilidad para no alertar a los operadores Pero dijo que compartiría los detalles de la falla con las autoridades con el objetivo de ayudar a acabar con más operadores de Mars Tyler ya vemos que es un claro caso de contraataque ofensivo y que se ha tomado la ley por su cuenta en el episodio anterior cubrí la noticia de que Australia ha creado un equipo de ataque ofensivo contra cibercriminales sobre todo para combatir el ransomware que se compone de 100 personas trabajando a tiempo completo y también comenté que países como Estados Unidos y el Reino Unido tienen capacidades similares Aunque oficialmente a menores cara Según dicen ellos desde 2017 también comenté que han habido casos de contraataque ofensivo por partes de las fuerzas del orden policías holandeses engañaron al grupo ransomware deadball haciéndoles creer que habían pagado el rescate y pudieron revertir y recuperar la transacción de criptomonedas justo después de haber recibido cada una de las 150 claves de descifrado que pudieron rescatar en otra instancia el departamento de justicia de Estados Unidos recuperó la mayoría de los 4,3 millones de dólares pagados como rescate al grupo darkside por parte de Colonial pipeline en el ataque de ransomware y otro caso fue que el Us Cyber command y el FBI comprometieron los servidores del grupo de ramsomware revivil después del ataque contra casella pero en este caso a diferencia de las situaciones anteriores que acabo de comentar el grupo que contraataca no pertenece a ningún gobierno ni fuerza del orden Es simplemente una empresa de ciberseguridad que se ha tomado la justicia por su mano en esta ocasión desde un punto de vista moral probablemente a la mayoría estemos de acuerdo de que han actuado para bien aunque no somos quién para decidir esto ya que para eso está la ley y dependiendo del país esto puede o no ser un acto delictivo en Sí por ejemplo en Estados Unidos esto sería un acto ilegal en base a la ley de acto de fraude y abuso informático la llamada computer frood en Avis act que Define que comprometer sistemas sin orden judicial Es delito en el pasado han habido casos de empresas privadas o incluso individuos que han realizado maniobras de contraataque contra malware y cibercriminales uno de los casos más famosos es el de Marcus hatskins También conocido como malware Tech que como dice la revista wired fue el hacker que salvó internet entre comillas no para los que no lo recuerdan en mayo de 2017 el ransomware wanna Cry barrió a más de 100 países de una forma muy rápida en todo el mundo bloqueando sistemas críticos como el servicio nacional de salud del Reino Unido la empresa de telecomunicaciones telefónica y otras empresas e instituciones de todo el mundo todo en un tiempo récord una vez infectados con wanna Cry cada sistema se bloqueaba sin permitir el acceso y en su lugar mostraba el típico mensaje de ransomware en el que se exigía el equivalente alrededor de 300 dólares en bitcoins para rescatar los datos cifrados y el acceso de vuelta al sistema a sus 22 años Marcus encontró una vulnerabilidad en el malware wanna Cry que permitió activar el interruptor de apagado o Kill switch como se le denomina en inglés y ralentizar de esta forma la propagación de este ransomware Marcos analizó el binario descubrió que los creadores del ransomware lo habían diseñado para comprobar si una cierta URL conducía a una página web activa Y si ese era el caso el malware se cerraría por lo tanto lo que hizo Marcus fue invertir unos 10 dólares en registrar dicho dominio que está bajar codeado o embebido en el binario levantaron sitio web en ese dominio y de esta forma hacer que la infección a nivel mundial se ralentizara esto permitió ganar tiempo para que administradores de sistemas en todo el mundo pudieran instalar el parche de seguridad que Microsoft había publicado asociado con la vulnerabilidad que wanna Cry explotaba en los sistemas vulnerables y para que empresas de ciberseguridad analizaran El malware con más detalle e incluyeran firmas y definiciones de el comportamiento malicioso en sus sistemas de en Point detección en response para detectar y

detener el malware y de esta forma evitar que wanna Cry causará males mayores vemos que hay una diferencia entre los dos casos primero en el caso de Marx contraatacó de forma activa abusando de una vulnerabilidad en el servidor de Mando y control del malware sin embargo en el caso de wanna Cry Se podría decir que Marcus contraatacó de forma pasiva contra el ransomware ya que no tocó no interactuó directamente con su infraestructura sino que el ransomware fue el que interactuó primero con el sitio web hospedado en El dominio que Marcus había registrado ya vemos que son dos formas distintas de contraataque activo versus pasivo y que a veces Incluso se pueden combinar para tumbar malware y actividades ciberdelictivas recordemos que ambos casos fueron llevados a Cabo por entidades o individuos privados que no pertenecen a ningún gobierno ni fuerza del orden y tampoco tenían ninguna orden judicial por lo tanto de nuevo el debate queda ahí es correcta la acción de bookware contra Mars Tyler en este caso hay que comentar que como Board tuvo acceso a servidores de Mando y control de Marx Y estos servidores contenían los datos robados de sus víctimas Board potencialmente ha podido tener acceso a mucha información confidencial a la que no estaba autorizado recordemos contraseñas de acceso a Portales de videojuegos datos bancarios y de tarjetas de crédito o débito o incluso carteras de criptomonedas No creo que a ninguna de las víctimas le guste que sus datos confidenciales no solo los puedan tener cibercriminales ofreciéndolos estos datos en la Dark web sino que también los pueda haber obtenido una empresa de ciberseguridad sin permiso alguno No autorizada en cualquier caso quiero cerrar la noticia dejándoos con unas medidas que os pueden ayudar a protegeros o responder a una infección de malware de robo de datos o también llamado infostiler Así que lo que podéis hacer es lo siguiente y comentar que esto no es consejo nuevo lo llevamos inculcando en los episodios anteriores Bueno desde el inicio de tierra de hackers y a modo de recordatorio queremos recordar que si estáis infectados lo que podéis hacer es lo siguiente cambiar contraseñas y semillas de doble factor notificar a entidades bancarias cerrar tarjetas de crédito y débito y pedir nuevas monitorizar actividades bancarias suscribirse a servicios de prevención de robo de identidad hacer búsquedas de tu propia información online aplicar parches de seguridad Tan pronto como se publiquen ya sea en portátiles sistemas de sobremesa o móviles instalar un antivirus u otro sistemas de seguridad y vigilar con de ingeniería social ya sea vía email chats mensajes o llamadas o incluso en enlaces de plataformas web estilo YouTube y similares Así que tener mucho cuidado con este tipo de amenaza ya que ya veis que vuestros datos son tan valiosos como el oro muy interesante la noticia Alexis Como siempre muy curioso este tema de los infoestibles teníamos los deira wipers que era simplemente Borrar datos tenemos otros que solo para crear de nayalo of service Y tenemos esto es especializados en robar información lo cual tiene muchísimo sentido cuando hablamos como hemos hecho en muchas ocasiones ocasiones en tierra de hackers del tema de robar propiedad intelectual un vector de ataque muy común sobre todo desde china Así que tiene sentido que se haga este tipo de malware especializado pero sobre todo también el tema de que lo puedas alquilar esto también lo hemos hablado muchas veces lo de ranson buenas a service es que es una pasada que se crean nuevos mercados en todos los sentidos Qué locura pues hasta aquí Hemos llegado en este episodio Gracias por tener paciencia que os hemos dejado una semanita sin episodio pero estábamos lo dicho migrando el podcast Gracias por seguir ahí vuestros comentarios que son una pasada los emails que nos mandáis colaboraciones que nos pedís como siempre Muchísimas gracias recordar compartir el podcast que nos ayuda muchísimo comentarlo en redes no solo en redes sociales pero en las propias plataformas de podcasting porque eso nos hace más relevantes y crecemos en los charts para que

nos descubra más gente es el objetivo Y como siempre pues nos podéis también apoyar si así queréis en patreon patrón puntocom/h de hackers pues muy contento de haber finalizado la migración del podcast a la nueva plataforma y de poder publicar otro episodio más contigo y con los oyentes de nuevo a darles mucho las gracias por su apoyo con esas reseñas y mensajes maravillosos que nos envían y que nos dan la motivación para poder seguir adelante con el podcast y también por supuesto dar las gracias a nuestros patrocinadores y mecenas ya sabéis que todos formáis parte de tierra de hackers y hacéis realidad este podcast lo dicho desde aquí seguimos trabajando duro para poder traeros episodios interesantes pues nos vemos y nos escuchamos en el próximo episodio Adiós adiós Chau hasta la próxima 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