los ataques automatizan cada vez más llegando a abrirse un mercado de herramientas específicamente diseñadas para comprometer la seguridad de los usuarios en internet al alcance de cualquier criminal y sin prácticamente conocimientos técnicos el grupo cibercriminal chino blacktech se infiltra en empresas estadounidenses y japonesas después de comprometer y modificar rter Cisco de filiales africanas post resaca de conferencias no descansamos y ya tienes un nuevo episodio esperándote comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 13 de octubre de 2023 episodio número 108 yo soy Martín vigo y está conmigo de vuelta en sus aposentos Alexis porros Hola Alexis qué tal Muy bien Martín con muchas ganas de estar aquí contigo y comentar las últimas noticias eh solo voy a comentar algo también que no Es relacionado con las noticias O sí me encantó esa botellita de vino de Rioja que que te regaló uno de los oyentes Sí así que la verdad un detallazo tío me decía que le mencionas como el riojano pero sí me hizo muchísima ilusión un detallazo Así que el año que viene si puedo pues nada vamos con Martín y la disfrutamos los tres juntos O quien que se quiera apuntar ahí la la abrimos y dale claro es lo guapo de ir ahora a conferencias desde que hacemos el podcast que es conocer a todos los oyentes y lo bien que se portan con nosotros solo que faltas tú Alexis a ver si te animas pues eh Nada seguimos para adelante y lo de siempre no para no repetirme eh estamos en las redes sociales más populares donde nos podéis encontrar como tierr deeh hackers o @ tirad hackers también en las plataformas de podcast eh ebox Spotify Google podcast todas esas Apple podcast también tierra de hackers ahí estamos y como digo Siempre más que Bienvenidos a nuestro canal de discord podéis acceder vía tierrade hackers.com barcod Y tenemos muchas conversaciones interesantes sobre qué conferencias nuevas o qué conferen Alguien me puede pasar una lista de conferencias o temas de privacidad que hemos visto en las noticias aparte de todo lo que comentamos eh en en los episodios pero es un sitio donde a veces se quedan temas en el tintero no y ahí pues bueno nos desahogamos un poquito ya sabéis apuntaros a nuestro canal de discord que hay ahí conversaciones muy interesantes en tierra de hakers.com brdc recordaros también que voy a impartir un curso para aprender sobre seguridad en el entorno web orientado a desarrolladores orientado a gente que está empezando en pen testing o simplemente ingenieros de Software que quieren empezar a escribir código más seguro el curso es en inglés y lo voy a impartir de manera presencial en Barcelona el 7 y el 8 de noviembre por las tardes para que sea compatible si estás trabajando Así que ya sabes cybersecurity for web developers y tienes más información en tierradel comom barwe bsur tierr hackers.com websecurity apúntate si quieres aprender y comprender más sobre las vulnerabilidades más habituales en el entorno web también pedirte querido oyente que si nos escuchas en la plataforma ibox han abierto sus votaciones para los mejores podcast y si tú crees que nos merecemos tu voto pues Oye sería un detallazo que nos lo des y para ello puedes ir a tierradel comom bar votar tierrade hackers.com bar votar y así votar por nuestro podcast para ver si ganamos a ser uno de los podcast en tecnología más eh relevantes en esa plataforma sería un detallazo por tu parte y antes de empezar Ya solo nos queda dar las gracias a nuestros mecenas de patreon y a nuestro sponsor monat que es una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast in 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 sabes echadle un a su web monat.com y le podéis mandar vuestro currículum en tierrade hackers @mon at.com y nada comenzamos ya me encontré una investigación de eset que publicaron hace apenas una semanas donde analizan un Bot de Telegram que automatiza una serie de ataques comunes

contra usuarios en internet que la verdad me llamó mucho la atención me llamó la atención por su simpleza y funcionalidad ya que permite prácticamente a a cualquiera llevar a cabo ataques bastante habituales y eficaces sin que el sin que el atacante tenga que saber apenas usar un móvil me gustó esta investigación y decidí traer al podcast porque demuestra una vez más que no se requiere de atacantes sofisticados para que suframos una brecha de seguridad aquello de a mí quién me va a hackear no los chinos pues No a lo mejor lo hace el vecino del cuarto ese que no sabe ni hacer la O con un canuto es algo que comento mucho a gente con la que hablo sobre los peligros de internet y que consideran que ellos pues lo dicho no tienen nada que esconder o que no tendría ningún valor atacarles no comprenden que hoy en día la mayoría de los ataques están hasta cierto punto automatizados que no es un ucraniano en su casa que se levanta un día y decir de de atacar a Manolo no lo que te ataca son scripts de python probando las contraseñas más comunes contra una lista de Correos en las webs más habituales lo que te ataca es un email enviado a millones de personas en pocos segundos lo que te ataca es un SMS recibido en masa por la mayoría de los habitantes de tu país lo que te ataca es código diseñado para atacarte ya luego cuando picas es cuando se pone el Humano a cargo para exprimir ese primer acceso conseguido a tu dispositivo correo electrónico o lo que fuese que ha atacado en esta línea hoy vamos a hablar de ese bote Telegram que os mencionaba bautizado por los investigadores como telecopy como la mayoría sabéis Telegram pone a disposición de los usuarios una Api con la que se puede controlar Telegram con código esto es muy útil porque se pueden programar Bots con los que puedes interactuar a través de Telegram pues como si estuvieras hablando con tu madre por WhatsApp Por así decirlo Le escribes un mensaje el Bot lo lee y hace lo que hayas indicado que hagas Por ejemplo puedes hacerte un Bot que encienda las luces de tu casa y así le escribes por Telegram la orden de enciende las luces y va y las enciende Hay todo tipo de Bots buscando por ejemplo para esta noticia los más populares pues encontré con un Bot Que traduce el idioma que le digas al idioma que le digas lo que le envíes por ejemplo Tú escribes Cómo se dice en chino tal pues te contesta por mensaje como si le escribiese a un amigo que sepa chino y te dice comoo se dice en chino o un Bot al que le puedes escribir para que te recuerde algo en un momento específico del día Oye Recuérdame que le felicite el cumpleaños a mi madre mañana y lo hace te escribe mañana el Bot en sí por Telegram y te dice Oye recuerda esto o un Bot que te permita hacer el seguimiento de paquetes y te irá enviando o sea alertas según se actualice el estado del envío o también un Bot que permite enviarle una nota de audio y que te devuelva el texto de ese mensaje de audio para esos momentos donde no puedes oírlo O sea ya sabéis por dónde voy si sabes programar básicamente tu imaginación es el límite para crear un Bot en Telegram que automatice algún una tarea en concreto y bajo esta premisa Alguien vio un negocio claro un Bot para criminales que automatice las tareas comunes que llevan a cabo esta gente este Bot es capaz de hacer bastantes tareas y vamos a analizarlas una por una todas las tareas están destinadas al fraude robo de dinero de los usuarios de tiendas online en concreto Si bien el Bot soporta mayormente tiendas online de Rusia también tiene soporte para Ebay y curiosamente blablacar un servicio centrado en compartir coches en viajes largos Pues bueno para dividir los gastos entre varios que por cierto es muy popular en España este Bot básicamente te ayuda en las tareas de gestión de anuncios falsos ingeniería social fishing vishing y robo de dinero entremos al detalle generación de páginas web falsas esta funcionalidad permite crear webs que se asemejan a las reales de tal manera que son muy fáciles de confundir con el propósito de que la víctima introduzca pues sus credenciales o los detalles de la tarjeta de crédito o Bueno cualquier otro dato sensible Y por supuesto valioso para el atacante con un comando sencillo Y especificando qué tipo de web quieres falsear este Bot te facilita la web clonada y además la aloja en un servidor por ti y usa uno de los sus

dominios para que no tengas que hacer absolutamente nada y con dominio me refiero a pues dominios muy parecidos al de la propia web real que estás intentando clonar específicamente para soportar a todos los clientes Por decirlo de alguna manera clientes utilizan sub dominios para asignarte tu propia web Y como decía un domin dominio específico en base al tipo de web que has clonado las web soportadas para su clonación están categorizadas incluso por países y efectivamente entre las opciones vemos a España la gente de eset muestra en su informe que como siempre os dejo en las notas del episodio muestra una web de confirmación de pago que es falsa correspondiente a eBay para que por ejemplo después de introducir los datos bancarios en la web falsa la víctima piense que todo ha funcionado correctamente porque está viendo la confirmación de pago a pesar de que insisto es falsa pero sigamos procesamiento de pagos online y cobros una de las tareas más complicadas cuando se trata de robar dinero online es la de recibir pagos Piénsalo Si vas a cobrar dinero fraudulento no te interesa hacerlo a tu cuenta bancaria personal y cobrar en bitcoin aparte de ser s sospechoso para webs como eBay porque pues todo el mundo sabe que eBay no puedes pagar con bitcoin crea también mucha fricción y muchas víctimas pues no sabrían ni Cómo obtener bitcoin a pesar de que las hayas engañado a la hora de pagarte no tienen bitcoin pero tranquilos el Bot acude al rescate como decía todo bien sencillito y automático para que no tengas que hacer absolutamente nada este Bot Está programado para encargarse de recibir los pagos en una cuenta que controlan los propios creadores y son ellos luego quienes lo blanquean por ti y te lo envían a ti en bitcoin para que no pueda ser traceado todo comodidades señores seguramente tengan alguna cuenta bancaria abierta en nombre de una persona falsa o que existe pero no sabe o no lo sabe en países que controlan Pues poco o menos Quiénes son los titulares y bueno tienen verificaciones muy pobres a la hora de abrir cuentas bancarias Ya de ahí compran bitcoin que además Lo pasan por tumblers antes de enviártelo a ti querido estafador lo de tumbler ya os lo hemos explicado en varias veces estos bitcoin mixers donde todo el mundo pone Pues en una hucha común de bitcoin todo su todo su bitcoin que viene de operaciones fraudulentas se mezcla todo te lo reenvían de vuelta y claro ahí se pierde la trazabilidad por supuesto los creadores del Bot se quedan una importante comisión antes de enviarte tu dinero digamos que te dejan utilizar de manera gratuita el Bot pero se quedan una comisión también porque te te facilitan todo el tema de los pagos y blanquearte el dinero Por ejemplo si eres un nuevo cliente insisto por llamar así se quedan un 33 por de lo que hayas estafado a la víctima Y si eres un cliente habitual y que produce resultados es decir un cliente Premium cobra la comisión de ellos baja al 23 por pero no te lo pierdas que también tienen una comisión por referidos sí sí siendo tú mismo un cliente si traes a nuevos estafadores te llevas un 2% de lo que ellos vayan estafando a su vez esto es la bomba una estafa piramidal dentro de una estafa en sí Lo nunca ha visto pero bueno más cositas fishing mediante el envío de correos electrónicos falsos aquí convenientemente el Bot configurará los parámetros del email en base a la web que estás intentando impersonar para que todo tenga sentido una vez más tú no tienes que hacer nada más que dar el cor de tu víctima bueno o lista de correos electrónicos que tengas y el Bot se encarga de todo crea la plantilla perfecta Configura los dominios y links falsos envía los correos electrónicos lo dicho no tienes que hacer absolutamente nada más que darle la lista de correos electrónicos de las personas a las que estás intentando estafar por supuesto otra funcionalidad que ofrece si prefieres o es más adecuado en base a la web que estás falseando como te puedes comunicar con las víctimas vía SMS en vez de email no tienes que usar un burner phone ni tienes que comprar números de teléfono no tienes que pagar por el envío de tus mensajes tú simplemente das la lista de números de teléfono de tus víctimas y listo incluso con soporte para múltiples idiomas una auténtica pasada pero vayamos a cosas más chulas renderizado de imágenes customizadas y para qué me dirás tú querido oyente pues por

ejemplo para la creación de capturas de pantalla falsas que puedes enviar a tu víctima como comprobante de un envío por ejemplo de un paquete algo típico no cuando compras algún particular en alguno de los mercados online por ejemplo compras algo por Ebay y es típico que a quien le hayas comprado algo justo antes de enviar el paquete te envía una foto antes de llevarlo a correos pero también bien sirve para crear una captura de pantalla falsa de tu móvil que también es típico no sacar pues una captura de pantalla de la imagen de cuando te envían una factura online de correos o por ejemplo la típica notificación que te llega de que el paquete ha sido enviado o la justificación se me ocurre por ejemplo de del Tracker del identificador del paquete pues sueles hacer una captura de pantalla desde el móvil y se la envías a quien te lo ha comprado no para que para que vea que lo has hecho pues esto también te lo puede falsear pero es que no solo te crean la captura de pantalla sino que lo customiza automáticamente con el texto acorde a la estafa que has hecho me explico customiza la captura de pantalla la editan para que la cantidad del pago que te ha hecho tu víctima esté reflejada el nombre de tu víctima esté reflejado el nombre del producto que ha comprado también está introducido y customizado en esta captura de pantalla muy top la verdad y todo para evitar que tengas que usar Pues algo de Photoshop no para rellenar la plantilla porque podían pasarte la plantilla y que tú introduzcas el texto no no lo hacen por ti pero Espérate que esto no es todo también falsifican fotos de los albaranes que pegas al paquete antes de enviarlo eh con la dirección y tal para que puedas enviar también fotos de esto a la víctima insisto la foto customizada con el texto de la dirección de tu víctima para que no tengas que hacer absolutamente nada pero hay más aún falsificación de cheques bancarios toma ya el código del Bot de Telegram hace referencia concretamente a a cheques ahora mismo del banco ruso sbank de este modo si tu estafa es en vez de vender productos falsos comprarlos puedes engañar a la víctima para que te envíe el producto y piense que le has pagado mediante cheque bancario porque este Bot tú le das los datos y te va a crear una captura de pantalla de un cheque bancario falso con los datos específicos de tu víctima una auténtica pasada como ves querido oyente con esta noticia hemos aprendido que estafar online hoy en día está al alcance de cualquiera la moralidad de las personas es prácticamente la única Barrera que queda entre ser un estafador y no serlo no sigas pensando que nadie va a estafarte porque piensas que eso solo le pasa a la gente que tiene mucho dinero o es una persona de interés por alguna razón los ataques y las estafas online están más automatizadas que nunca automatizadas y customizadas de tal manera que tú podrías llegar a ser la siguiente víctima mantente alerta desconfía si huele mal y como dice aquel si lo que ves es una oferta increíble Probablemente lo sea nadie da duros a pesetas como decimos en España esto es un servicio no sé cómo lo han llamado Pero yo lo llamaría estafadoras a service no te dan la plataforma tal cual tío es que por eso me pareció muy relevante traer esta noticia porque es para es perfecta para demostrar que no hace falta atacantes sofisticados que hoy en día ya te lo dan todo hecho no tienes que hacer nada y simplemente pagas una pequeña comisión es que Esto suena Al fin y al cabo como lo del ransomware que al principio era ransomware luego ya es un crimen organizado ya está ransomware service toda esta can of cúpulas y y y los los que desarrollan el Software que no se mojan los digamos los líderes de las minib bandas y luego los que realmente hacen el siguen el guion porque esto Al fin y al cabo es seguir un guion aquí lo que parece que se han han automatizado todo ese guion y ya cualquiera puede ser parte de este estafador de service modelo de negocio y tanto porque ya te digo lo que comentaba de las comisiones y sobre todo lo del referal en plan Oye que Cuanto más traigas estás haciendo ingresos pasivos porque te llevas un 2% de lo que stafen tus amigos O sea que esto es un chollo Esto me recuerda también cuando salió al principio toda la esta la moda de los llms Open Ai y todo eso a stable diffusion si no me equivoco era solo permitía obtener las imágenes a través de Telegram o a través de

discord o algo así así que me recuerda un poquito también Supongo que están usando en todo lo que comentas de modificar la imagen on the Fly y los cheques y todo eso ahí están usando Ai probablemente no no sé qué opinas pero me suena que hay mucho de eso y por eso el tema del lm ha facilitado mucho más toda esta automatización esto también recientemente me me casi último comentario con esto cierro eh he visto una noticia que el FBI ha dicho que últimamente hay muchos ataques de Phantom hacker que están enfocándose en en personas adultas pero lo que hacen es llamarlas directamente Aunque no es una técnica que sea nueva Pero supongo que ahora la hacen más efectiva y lo que estaba leyendo también que hay gente que no es nativa en un idioma pero gracias de nuevo a los llm y las traducciones que hacen tan buenas y convincentes entonces solo leen el Script y son efectivos otro tema más como el que comentas de de que esto a ver siempre cualquier herramienta se puede utilizar para mal no el los llms y Ai yo creo que que tiene futuro para bien Pero supongo que en este caso como comentas Martín y en este del Phantom hacker scam calls eh se utiliza para mal Así que mucho cuidado sí como venimos diciendo hace tiempo en varios episodios la Ai es buena pero también tiene su parte mala no solo tiene su parte mala pero tampoco tiene solo su parte buena Pues nada vamos con la siguiente noticia que va de blacktech un grupo chino que ha estado haciendo de las suyas atacando routers Cisco de filiales en países de África Pues nada Martín pasamos con la siguiente noticia que va sobre un grupo de ciberamenazas chino llamado blacktech que ha estado comprometiendo routers Cisco en empresas filiales ubicadas en África principalmente Y es que recientemente las agencias de ciberseguridad de Japón y Estados Unidos como la nsa la cisa y el FBI han emitido un aviso de seguridad conjunto sobre este grupo apt chino como digo llamado blacktech que está comprometiendo filiales extranjeras de empresas estadounidenses y japones para luego pivotar a través de ellas y poder infiltrarse a sus sedes corporativas el tema es que estos cibercriminales abusan de la relación de confianza de los enrutadores de las sucursales dentro de la red corporativa objetivo luego utilizan estos routers expuestos a internet de sucursales comprometidas o filiales como parte de su infraestructura para utilizarlos como Proxy mezclarse con el tráfico de la red corporativa y pivotar para car a otros sistemas en la misma red corporativa en la sede de la empresa principal digámoslo así según Los investigadores han determinado que el grupo apt chino detrás de estos ataques es blacktech también se conoce como Palmer warm temp overboard Circuit Panda y Radio Panda y tiene un historial de operaciones contra objetivos en el este de asia específicamente Taiwán Japón y Hong Kong al menos desde s este grupo es bastante listo Y en lugar de atacar directamente a los sistemas de las sedes de las empresas a las que quiere comprometer se enfoca en las filiales que están en otros países las cuales como ocurre en muchas empresas tienen una menor seguridad por ser más pequeñas menos importantes con menos presupuesto y menos personal de seguridad el objetivo principal de blacktech son routers de Cisco bueno y os estaréis preguntando y cómo se infiltran en estos routers Cisco antes de deciros Cómo lo han hecho quiero comentar que según empresas de inteligencia de amenazas hay cuatro técnicas que son las más utilizadas por cibercriminales para obtener el acceso inicial a un dispositivo o a una red y son las siguientes la primera es fishing ya sea para robar credenciales o para entregar el malware que la víctima detonaría ejecutaría la segunda es abusar de sistemas o aplicaciones expuestas en internet es decir explotando alguna vulnerabilidad o saltándose el tema de la autenticación En tercer lugar tenemos el compromiso de productos de terceros en la cadena de suministro lo que se conoce en inglés como supply Chain attacks y en último lugar tenemos dispositivos externos como memorias USB esto no creo que os venga de nuevo y vemos ejemplos en las noticias cada dos por tres de estas técnicas sin embargo alguno de vosotros puede estar preguntándose Oye pero las acciones con usbs maliciosos ya no funcionan esto que me estás contando Alexis este

Esta última técnica de acceso inicial pues aparte de los USB explosivos que hemos cubierto anteriormente en el podcast os acordáis en el episodio 89 de hecho comentábamos esto que cadenas de noticias ecuatorianas recibían estos dispositivos usbs que una vez conectados a un ordenador pues algunos explotaban no bueno Esta técnica no es tanto de acceso inicial sino de causar daño y terror pero recientemente surgió una noticia que comentaba que las infecciones a través de usbs maliciosos se han puesto de moda de nuevo todo gracias a otro grupo de ciberamenazas chino se lo demos todo a los chinos en la conferencia de seguridad m wise de mandiant hace un par de semanas investigadores de seguridad presentaron sus hallazgos sobre un grupo de amenazas con vínculos con el gobierno chino que ha estado utilizando dispositivos USB para difundir malware este grupo denominado como unc 53 Ha logrado infiltrarse en al menos 29 organizaciones desde enero de 2022 infectando sistemas con variantes de malware conocido como sogu que tiene más de 10 años de vida las víctimas se extienden por Estados Unidos Europa y Asia pero muchas de las infecciones se originan en en sucursales de organizaciones multinacionales con sede en África en países como Egipto zimbabwe tanzania Kenia ghana y Madagascar en algunos casos el malware parece haber viajado a través de dispositivos de almacenamiento USB desde ordenadores compartidos en atención imprentas y cibercafés eso que las víctimas deben de haber ido a un cibercafé y conectado sus usbs para descargarse documentos y luego lo conectan a sus sistemas corporativos Y si ese cibercafé el sistema en ese cibercafé estab ADO pues se lleva la infección al sistema corporativo o van a una imprenta a imprimir algún documento de alguna reunión de negocio Y de nuevo vuelven a seguir utilizando el USB en su ordenador después de haber impreso dicho documento Y de nuevo se traen el malware con ellos a al ordenador corporativo lo curioso y lo que une ambos grupos el unc 53 y el blacktech es que tienen una estrategia similar infectar a sistemas de usuarios o empresas en países en los que las legislaciones y regulaciones no son tan estrictas en temas de ciberseguridad y donde los niveles de seguridad de las empresas y concienciación incluso de los usuarios puede ser menor por lo que estos ataques de tipo ingeniería social a través de dispositivos USB son más efectivos que en otras partes como Norteamérica o Europa o eso queremos pensar verdad en cualquier caso estas infecciones a través de dispositivos USB son modas van y vienen se utilizaron mucho en los años 2000 sobre todo en el 2008 cuando conficker de los gusanos más famosos utilizó la función de autoejecutivo de que no bajé la guardia y no deis por sentado que los vectores de ataque antiguos nunca se van a volver a usar de nuevo aprendamos del pasado y bueno volviendo a la noticia de blacktech estos cibercriminales utilizaron una de estas cuatro técnicas la de abusar de dispositivos expuestos en internet Cisco dice que para llevar a cabo el compromiso inicial en sus routers blacktech no aprovechó ninguna vulnerabilidad en estos productos es decir no explotó ninguna vulnerabilidad que se encontraban en estos routers sino que simplemente utilizó credenciales de administrador débiles o lo más probable robadas que probablemente compraran en foros de cibercriminales Okay ya tienen nivel administrador en el router después de eso lo que los cibercriminales hicieron fue cargar un firmware que ellos mismos habían desarrollado con una puerta trasera y cómo pudieron Modificar el firmware de routers Cisco tan fácil de hacer esto pues os cuento lo primero que hicieron los cibercriminales después de obtener acceso administrador al router con las credenciales robadas o compradas es Descargar firmware legítimo de Cisco de alguna versión anterior luego obviamente una vez descargado este firmware legítimo lo que hacen es cargarlo en el dispositivo en el router Cisco y reiniciarlo después acceden de nuevo al router de nuevo obviamente tien las credenciales de administrador y esta vez lo que hacen es descargar un gestor de arranque modificado por los Cyber criminales en inglés bootloader y también un firmware modificado por ellos mismos el que tiene la puerta trasera acto seguido cargan el firmware modificado y también el

bootloader modificado y finalmente reinician el router Bueno y por qué hacen un downgrade a una versión de firmware anterior de Cisco Pues porque las versiones más modernas no permiten cargar firmware modificado que no esté firmado digitalmente por Cisco y obviamente para hacer esto lo que necesitan los cibercriminales es haber robado un certificado de Cisco para tener la clave privada de Cisco y de esta forma poder firmar digitalmente el firmware Y esto no ha sucedido bueno De todas formas Por qué necesitan cargar este firmware si tienen eh nivel administrador ya podrían hacer igual algunos temas de espionaje y temas similares No pues necesitan cargar este firmware porque es la única forma de poder inyectar su código que corre a nivel privilegiado de kernel del firmware para poder inspeccionar paquetes ahora en un momento explico por qué necesitan esta funcionalidad bueno la otra pregunta igual que os estaréis haciendo es si han podido cargar el firmware modificado Por qué También tienen que cargar un bootloader modificado pues porque si no lo hacen cuando cuando se reinicie el router Cisco este no arrancaría porque el bootloader legítimo de Cisco haría comprobaciones de firmware es decir comprobaría si el firmware está firmado digitalmente por Cisco y no dejaría que se iniciara el router si no es así vale pues entonces de esta forma con el gestor de arranque modificado lo que hacen los cibercriminales es saltarse estas validaciones de firma digital del firmware al inicio del sistema fijaos que todo esto lo hacen utilizando herramientas que vienen por defecto en el propio router o como se conoce ataque de living of the Land También tenemos el tema de que los cibercriminales han modificado el firmware de tal forma que las herramientas que típicamente se utilizan para el análisis forense no muestran su actividad de esta forma se mantienen ocultos se mantienen entre las sombras digamos el informe no entra en detalle pero me imagino que herramientas que listan conexiones de red o procesos filtraran las salida del texto en la consola y no mostrarían conexiones establecidas a las direcciones ip de los cibercriminales ni tampoco procesos relacionados con la puerta trasera no solo esto sino que el firmware modificado también tiene capacidad de omitir los logs que se envían de toda actividad relacionada con los cibercriminales Y luego cómo obtienen la persistencia Pues en el firmware modificado que han cargado han incluido un servidor de ssh que se activa Solo cuando ellos así lo quieren y cómo hacen esto para no ser vistos por telepatía o cómo Bueno pues aquí es donde entra el juego de algo que se conoce como paquetes mágicos a nivel de red o por knocking que sería picar a la puerta a través de de puertos no de esta forma por defecto el servidor ssh de puerta trasera no acepta conexiones de ningún sistema entonces para que el servidor de ssh acepte conexiones de los sistemas temas de los cibercriminales lo que tienen que hacer estos es enviar una serie de paquetes tcp o udp específicos en el firmware lo que hay es un proceso corriendo que monitoriza el tráfico y la recepción de estos paquetes si se reciben paquetes a puertos predefinidos en una secuencia predeterminada Entonces el servidor ssh acepta conexiones de la dirección IP que ha enviado estos paquetes esto podríamos decirlo que es análogo a como cuando vas a hacer login a tu ordenador o a una página web tienes que introducir o enviar caracteres en una secuencia muy específica la Que obviamente Define tu nombre de usuario y contraseña por ejemplo digamos que tu usuario es Pepito Pues en el teclado Tienes que apretar dichas teclas y en ese orden P E p i t o porque obviamente podrías teclear lasas de otra forma No por ejemplo pepti Pero entonces no es es tu nombre de usuario el el sistema te va a decir eh credenciales incorrectas Pues el por knocking es similar se envían unas credenciales digamos entre comillas pero a nivel de red en paquetes tcp o udp digámoslo a nivel más crudo No tan a nivel de aplicación no como en páginas web y eh Como digo una de una secuencia predeterminada conocida tanto por el cliente en este caso el sistema del cibercriminal como por el servidor el proceso de puerta trasera corriendo en el firmware modificado en el router Cisco un ejemplo podría ser el siguiente enviar tres paquetes tcp con el flag sin activado a los puertos me lo invento 23 80 y

443 en este orden y bua la puerta trasera ssh permitiría conexiones desde la dirección IP que envió estos paquetes tcp recalco que Esta técnica de por knocking no es nueva y se lleva utilizando ya desde principios de los 2000 pero es una buena forma de no exponer la puerta trasera a todo el mundo y de esta forma pasar desapercibido lo más curioso es que según la alerta de seguridad la puerta trasera ssh incluye un nombre de usuario especial que no requiere autenticación adicional Supongo que los cibercriminales se plantearon bueno Y para qué vamos a Añadir una contraseña si la combinación de paquetes el por knocking que permite el acceso a s ya hace como de contraseña no bueno pues así lo han hecho finalmente los cibercriminales se infiltran en las redes corporativas con prometiendo sistemas y llevando a cabo sus objetivos a través de herramientas que se encuentran en los dispositivos y actividades normales del sistema operativo y de la red esto como digo de nuevo se le conoce como living of the Land y que es lo que les permite evadir la detección de los edrs estos end Point detection and response productos esta alerta de seguridad deja a Cisco en bastante mal lugar porque deja en entredicho la seguridad de los dispositivos de red de esta empresa tan grande que se podría decir que es gracias a la que tenemos internet pues en respuesta a esto Cisco ha revisado el informe y ha resaltado unos puntos que os comento primero comentan que el vector de acceso inicial más frecuente en estos ataques implica credenciales administrativas débiles o robadas esto ya os lo he contado antes no pero lo recalca Cisco y dicen que como se describe en el informe ciertos cambios de configuración como Deshabilitar el registro y descargar firmware y cargarlo y además el bootloader requieren credenciales administrativas es decir Cisco quiere con esto decir que Oye no es que con unas credenciales cualquieras se pueda hacer esto sino que requieren credenciales de administrador Okay bueno Vale pero si estas credenciales son débiles o se venden en internet eh poco se puede hacer en este aspecto no Okay el segundo punto es que Cisco dice que no hay indicios de que se haya aprovechado ninguna vulnerabilidad de dispositivos Cisco los atacantes utilizaron únicamente credenciales comprometidas para realizar cambios de software y configuración a nivel administrativo Okay esto nos deja bastante tranquilos de que no es un tema de alguna vulnerabilidad que se tiene que parchear sino que hay que tener más cuidado principalmente con eh estas credenciales administrativas y ahora entro en un momento en temas de cómo mitigar esto lo siguiente que Comenta cco es que sus dispositivos modernos incluyen capacidades de arranque seguro que se conoce como secure Boot que no permiten la carga y ejecución de binarios de firmware o bootloader modificados que no estén firmados por certificados digitales de Cisco también relacionado dicen que en el informe se comenta que los cibercriminales utilizaron certificados digitales robados para firmar cierto código malicioso y para hacer que parezca software legítimo sin embargo en la alerta No se menciona qué software se firmó digitalmente de esta forma y Cisco quiere aclarar y comentar que estos certificados robados no son de Cisco al menos no tienen constancia de que les hayan robado certificados digitales y por tanto esta parte del informe queda un poco como Enigma y lo dejamos Bueno ahí en el tintero Bueno ahora os comento un poquito las recomendaciones sobre cómo mitigar este ataque en lo que se refiere a medidas de detección se podría implementar lo siguiente primero monitorear conexiones entrantes y salientes en estos dispositivos de red y de esta forma analizar el tráfico inusual destinado al router incluido ssh en interfaces expuestas en internet porque parémonos a pensar esto las interfaces de administración de dispositivos de red no deberían estar expuestas en internet algo que también se puede monitorear son las las descargas no autorizadas de cargadores de arranque o bootloaders e imágenes de firmware también se pueden monitorear logs de dispositivo para identificar acciones maliciosas Como por ejemplo reinicios no planeados cambios en la versión del sistema operativo cambios en la configuración o intentos de actualizar el firmware y también monitorear intentos de inicio de sesión exitosos

y fallidos en lo que se refiere a medidas de protección se podría implementar lo sigi lo primero es como siempre recomendamos el doble factor y no vía SMS sino vía aplicación de autenticación aplicar segmentación de red y permitir conexiones entrantes a servicios de administración como ssh solo en redes vvan exclusivamente de administración en la que no hayan usuarios normales para que no puedan abusar de estos servicios también bloqueo de todas las conexiones salientes desde dispositivos de red excepto aquellas destinadas a dispositivos de red cercanos o sistemas de administración pensadlo bien en general los dispositivos de red solo se conectan a dispositivos cercanos para intercambiar información de enrutamiento o topología de red o con sistemas administrativos para por ejemplo sincronización horaria envío delog autenticación o actualizaciones de firmware y bootloader luego También tenemos el tema de verificar de forma periódica la integridad del firmware y el bootloader esto sobre todo se refiere a verificar que la firma digital del firmware y el bootloader corresponde con una autorizada cuando exista la sospecha de que una contraseña se ha visto comprometida pues cambiar todas las contraseñas y claves del dispositivo finalmente tenemos el tema de actualizar los dispositivos reemplazarlos por dispositivos que tengan capacidades de arranque seguro secure Boot con mejores controles de integridad y autenticidad para los bootloaders y el firmware esto puede ser costoso Pero puede ser mejor invertir algo de dinero en cambiar routers que tener que pagar millones en ransomware o en multas de la ley lopd o gdpr por fugas de información de clientes el aviso no proporciona ningún indicador de compromiso como direcciones ips nombres de sistema o dominio o hashes de los firmwares modificados o los bootloaders modificados que los administradores pudieran utilizar para determinar si han sido atacados o infectados o incluso prevenirse de esta infección Así que lo mejor es implementar las medidas que he mencionado de prevención y detección finalmente a pesar de que tanto el compromiso de dispositivos de red expuestos en internet como la modificación de su firmware y bootloader para poder continuar llevando a cabo actividades cibercriminales sin ser detectadas no son hechos nuevos la alerta de seguridad quería hacer énfasis en que los cibercriminales están llevando a cabo estos ataques enfocándose en dispositivos de filiales menos seguras para pivotar a través de ellas y comprometer sus sedes sus redes corporativas más grandes y ya concluyo esta noticia diciéndoselo sucursales más pequeñas no las dejéis de lado no las dejéis olvidadas dadles cariño y cierro ya con una frase que leí en internet recientemente y que me gustó bastante Y dice lo siguiente el perímetro de una organización no es el límite de su red sino el límite de su telemetría Así que la idea es complementar una buena seguridad medidas de prevención con una buena visibilidad de sistemas y alerta temprana medidas de detección es un poco aquello de lo del eslabón más débil que siempre siempre se habla en ciberseguridad que suele ser el el Humano No pues aquí tenemos el ejemplo de las sucursales Claro porque por muy pequeña que sea la oficina que está ahí en medio de un pueblo perdido de la mano de Dios realmente siguen teniendo acceso a la red interna igual que la tiene su headquarter por tanto es un objetivo mucho más jugoso porque si bien tiene el mismo acceso no va a tener la misma seguridad ni física probablemente ni perimetral Así que mucho cuidado hay que tener el mismo baremo de seguridad en todas las filiales en todas las sucursales que se tiene en headquarter headquarter digamos que debería ser el baremo por mínimo Por así decirlo muy importante porque está claro que los atacantes van a pasar tiempo haciendo la fase de recones no de reconocimiento antes de ponerse a atacar a ciegas para encontrar Cuál es la mejor manera o la manera más fácil o la manera manera más débil de entrar y que no tenga tanta fricción y así que su ataque pues sea lo más productivo posible pues hasta aquí Hemos llegado esperos que os haya gustado el episodio recordad sobre todo si nos escucháis en iboxx que nos podéis votar en tierr hackers.com bar votar os lo agradeceríamos un montón y si queréis

aprender sobre ciberseguridad concretamente sobre todo tipo de vulnerabilidades que suceden Cómo suceden Y cómo solucionarlas en el entorno web tenéis mi curso de Cyber Security for web developers que voy a impartir de manera presencial en Barcelona el 7 y 8 de noviembre y podéis obtener más información en tierradel 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