¡Así VIGILAN tu PANTALLA los HACKERS! | ScreenCrab

chavales pues Bienvenidos a un nuevo vídeo bueno bueno pues llevábamos ya una larga temporada sin traer un poquito de Hardware hacking al Canal no que sé que es una sección que os gusta mucho hasta ahora ya sabéis que hemos estado analizando y cacharreando con el USB verdad aquí el Bugs Bunny y el cake croc dispositivos la verdad muy muy recomendados pero es que hay otro que hasta ahora no hemos visto y con el que se pueden hacer cositas y es este dispositivo de aquí el Screen crack un capturador de pantalla nuevamente de hacksfire que se implanta en el medio de dispositivos con conexión HDMI actuando como Man in the middle y permitiéndonos como atacantes interceptar las conexiones de vídeo antes de entrar en detalle con este dispositivo deciros que después de un año y pico literal de espera ya tenemos en nuestras manos este dispositivo de aquí el flipper 0 vamos a estar muy pronto analizándolo y viendo todo lo que se puede hacer con él que sea lo que te puedes estar pensando dirás oye no llegas un poco tarde Bueno pues puede pero sí que os puedo decir que el vídeo que tenemos en mente pensado hacer compensará todo lo que estado esperando así que bueno vamos a estar hablando un poquito en el vídeo de hoy acerca de este cacharro y vamos a ver cómo se puede tensar la cosa todo esto y mucho más en breve pero primero que nada mensajito ahí de nuestro queridísimo inigualable e inimitable sponsor casefam te gustaría reconfigurar tu ordenador con un nuevo sistema y un nuevo software de Office aprovecha la promoción de año nuevo de Case Funk y empieza a hacer uso de un conjunto de softwares que te dejarán fascinado usando el código de cupón S4 v50 dispondréis de una oferta especial del 50% de descuento para toda la serie de Windows y por otro lado con el código de cupón s4v62 dispondréis de un 62% de descuento tanto para los productos de la serie Microsoft Office como para los van del products el proceso de pago es bastante sencillo simplemente tenéis que coger el producto que más os interese añadirlo al carrito posteriormente aplicar el código de descuento correspondiente y ya en este punto pues finalmente realizar la compra con tu tarjeta de crédito en caso de cualquier problema ya sabéis que disponen de un servicio de atención al cliente 24/7 y postventa de por vida la verdad una excelente oportunidad para renovar el sistema operativo y mejorar el rendimiento y la seguridad gracias a casefam por patrocinar este vídeo y ahora continuemos con el vídeo de hoy bueno el screencrap No es que sea un dispositivo digamos muy complicado de entender no al igual que vimos justamente con el key croc este dispositivo se conecta en mes de en medio de dispositivos USB Pues de dispositivos HDMI como podéis apreciar la composición de la screen crack Está compuesto por una antena WIFI que estáis viendo por aquí una ranura HDMI de entrada así como una ranura HDMI de salida un pequeño compartimento justo encima de la antena para introducir una tarjeta Micro SD un botón un tanto diminuto el cual de ser presionado nos permitirá parar de grabar la pantalla víctima Y por último un puerto de carga usb-c ahora bien El único requisito de lo que tú necesitas como atacante para llevar a cabo toda la operación es por un lado una tarjeta microsd Card yo en este caso tengo esta de aquí una sandisk Ultra de 64gb de capacidad en donde estaré justamente pues almacenando toda la información que recopile esta tarjetita pues La idea es que la introduzcas en esta pequeña ranurita que habíamos visto de antes y una vez hecho pues ya sería conectar los HDMI ahora bien como atacante también necesitarás un cable HDMI adicional al del propio monitor vale o sea que tenéis que disponer de otro más y Bueno pues ya con esto podríamos proceder ahora bien cómo va todo el sistema de cableado Bueno pues poneros en

el caso de una empresa por ejemplo donde hay un trabajador que está operando diferente a su ordenador si está empleando un monitor lo más probable es que este monitor esté conectado por HDMI a la torre Bueno pues nosotros como atacante lo que haríamos sería aprovechar un momento de ausencia en el que la víctima por ejemplo se vaya al baño a cagar para desconectar el HDMI del monitor conectarlo al HDMI de entrada que es el que justamente está al lado de la antena WIFI del screencrap y luego a través de otro cable HDMI conectarlo desde la salida del HDMI del dispositivo Hasta El Monitor de la víctima si os fijáis lo que se vería por detrás una vez lo tengas todo montado sería algo como esto es por esto que tú como atacante debes de disponer de un cable adicional HDMI ahora bien Esto de primeras no es conectarlo y ya está ya está todo operando al igual justamente que hemos visto con el resto de dispositivos de hack Five esto necesita de un archivito de configuración del cual leer para interpretar las órdenes de lo que tienen que hacer lo normal de primera sería conectar esta Micro SD Card al ordenador yo para ello ya sabéis que tenemos nuestro all in one de confianza simplemente metemos la Micro SD Card a este aparato y lo conectamos posteriormente al ordenador una vez conectado el Alien One al equipo bueno dado que mi Micro SD Card ha sido formateada recientemente pues no tiene nada está vacío pero la idea es que bueno una vez lo conectes y te lo detecte create un nuevo archivo por ejemplo y vamos a llamarlo config.txter vamos a abrirlo y es aquí donde justamente pues vamos a cargar toda la configuración correspondiente en mi caso por ejemplo fijaros voy a cargar esta pequeña configuración destacar que hay dos modos de captura vale uno es el modo de captura en modo imagen y otro en modo vídeo obviamente pues bueno haréis la idea de para qué es cada cosa no vamos a empezar por ejemplo con el modo de captura en imágenes vale fijaros esto de capture interval 5 esto lo que hace alusión es a que quiero que cada cinco segundos el propio screen crack se encargue de sacar una captura de pantalla del usuario víctima y que me lo almacene en la SD Card lo como ves que tú puedes especificar Cada cuánto a intervalos regulares de tiempo quieres que te saque la captura de pantalla y bueno que hace el Screen crack pues te crea un directorio con nombre lut y dentro internamente Pues almacena en la Micro SD Card pues todas las imágenes imágenes o vídeos que puedes indicar también la resolución si quieres que sea con calidad baja media o alta que luego lo haremos por tanto Bueno fijaros vamos en este caso a guardar esta configuración vamos a extraer esto de forma segura Vamos a darle a expulsar Y bueno pues en este punto vamos a extraer el all in one y vamos a meter la Micro SD car dentro del screencraft lo único que tendríamos que hacer sería conectarlo todo correctamente para dejarlo por operando y ya a partir de aquí pues esperar el tiempo que consideremos oportuno la gran pregunta que os podréis estar haciendo Oye Tito sabi la víctima puede ver su pantalla normalmente como si no estuviera pasando nada sí la víctima no se va a dar cuenta de nada va a ver su pantalla normalmente De hecho no interpretáis lo de captura de pantalla como la típica captura de pantalla de Windows no tiene nada que ver esto lo gestiona automáticamente de forma interna el screencrap para sacar la captura de pantalla y el usuario pues lo dicho no ve nada es todo bastante sigiloso ahora bien una vez tengamos todo operando por detrás la idea sería volver a aprovechar algún otro momento de ausencia en el que la víctima se vaya otra vez al baño a cagar para desconectar el Screen crack volver a poner el HDMI que va de la Torre al monitor y ya con el Screen crack Pues bueno extraer la Micro SD Card y ver qué hay dentro yo en este caso acabo de conectar de vuelta el all in one con la Micro SD Card al ordenador y os daréis cuenta de que me acabo de crear una carpetita lud la cual tiene una serie de imágenes no y dos archivos ahí que a estos no les vamos a prestar atención si yo me abro por ejemplo esta primera imagen se ve mi

pantalla izquierda que es la que tengo por aquí con un bloc de notas Bueno yo me he abierto el blog de notas antes y estuve escribiendo algunas cosas por tanto si todo ha ido bien cada cinco segundos me tiene que haber sacado fotos no capturas de pantalla bien pues son estos de aquí aquí por ejemplo pues fijaros me acabo de pillar el Hola pero después de 5 segundos Pues bueno traté de escribir lento Pero como se escribís rápido el efecto es el mismo ahí ya había terminado y por eso las restantes son las mismas Pero bueno fijaros Que ahí lo estamos viendo y se ve la verdad pues bastante bien todo esto obviamente pues de forma totalmente sigilosa y sin que la víctima se dé cuenta de nada Si volvemos a abrir el archivo config os daréis cuenta de que bueno el archivo ha cambiado un poco no Nos mantiene la estructura de lo que lo habíamos indicado pero nos ha añadido un par de información o de líneas adicionales son todo comentarios pero bueno Esto es como para que te hagas la idea de qué cositas adicionales pues le puedes incorporar no yo en este caso ahora lo que me interesa es entrar en el modo de captura en vídeo en vez de imágenes vale por tanto donde pone image Vamos a ponerle vídeo lo de capture interval Cabe destacar que lo podemos comentar Ya necesario y bueno de resto en cuanto a vídeo bitrate esto de 2 megabits por segundo 4 megabits por segundo bueno Esto de medium esto haría alusión al tradicional HD y 16 megabits por segundo Pues sería 4k o Ultra HD obviamente pues Bueno a mí me interesa capturarlo todo en alta calidad así que bueno justo debajo de Button Eyed si tal podríamos poner aquí lo de vídeo barra baja bitrate y vamos a meterle un hype vale por tanto Bueno vamos a esto guardarlo y bueno vamos a conectar la Micro SD Card de vuelta al screencrap y a ver si nos captura todo lo que nos interesa yo en este caso voy a estar ahora compartiendo esta pantalla de aquí para ser un poquito de actividad y pues comparar con lo que me he capturado Así que vamos a ello Bueno pues yo lo acabo de conectar y se supone que ya debería de estar grabando Vale entonces Bueno vamos a hacer un poquito de actividad aquí por ejemplo en mayúsculas Esto es una prueba estamos grabando o qué pedo vamos a abrirnos el libre Wolf de navegador pongo esto por aquí pongo Master no que luego el copyright Salta pero yo que sé un poquito de movimiento por aquí y listo Hasta luego vamos ahora a quitar la SD Card de el Screen crack vamos a conectarlo al Alien One y a ver qué nos ha capturado Bueno pues acabo de conectar de vuelta el Alien One vamos a irnos a la carpeta loot y bueno fijaros que ahora hay por ahí algunos vídeos no que se acaban de grabar ahí vemos las previews Bueno vamos a abrirnos por ejemplo el primero te lo grabo de forma fragmentada Cabe destacar que seguramente se puede hacer que te lo grabe todo en una misma toma Pero bueno en este caso es lo mismo si por ejemplo nos abrimos este vamos a ver si nos captura el momento exacto en el que nos ponemos a escribir fijaros esto es vale eso sería una parte vamos a irnos Aquí bueno Esto es una prueba estamos grabando o qué pedo Luego me había abierto el librewalls ahí se ve que me estoy moviendo bueno como veis es que se ve espectacular se ve en muy buena calidad en este caso te lo hace de forma fragmentada como os comenté anteriormente Pero bueno lo importante es que veáis que se ve lo que la víctima está haciendo quiero pensar que a lo mejor es lo de capture interval aunque sea para fotos esto más bien me parece que por ejemplo le establecemos un intervalo de captura de 30 segundos vamos a ver por casualidad si ahora me graba 30 segundos la pantalla de la víctima bueno ahí le he conectado de vuelta vamos a poner por ejemplo Hola Esto es una prueba dura el vídeo 30 segundos ahora seguimos escribiendo bueno Cualquier cosa volvemos a abrirnos el librewolf voy a buscar por ejemplo YouTube otra vez vamos a poner por aquí un poquito de movimiento y vale vamos a ver si por casualidad igual es esto y ahora me lo ha grabado durante 30 segundos voy a conectarlo de vuelta vamos a echar un ojo a la carpeta loot otra vez y vale esto tiene mejor pinta una única toma

si esto lo abro efectivamente bueno la cámara Ahí está 25 24 23 es una toma de 30 segundos clavados efectivamente Y ahí vemos toda la actividad del usuario incluso al principio cuando estábamos escribiendo esto lo de seguimos escribiendo nada espectacular y como veis la calidad es que es asombrosa no se ve bastante bastante bien y la víctima es que no se da cuenta de nada tú conectas el skin crack detrás del monitor o por detrás hay entre el tablerío de la Torre con los cables por detrás Y es que en verdad no te das cuenta de que te están espiando ahora bien otra gran pregunta que os podáis estar haciendo No Oye Tito por qué tienes tú una antena si no la hemos usado hasta ahora Bueno pues si hay algo chulo que tiene el Screen crack es que a través de esta antena puede conectarse a un punto de acceso para tener conectividad con internet y transmitir en tiempo real lo que es la pantalla de la víctima a un C2 a un command control este coma no encontró Por ejemplo yo lo voy a correr en local en mi red local y bueno lo podéis Descargar y adquirir de la web de hatfight vale simplemente lo deja Descargar tenéis que rellenar vuestros datos y demás y una vez descargado Pues bueno sería ejecutarlo en local yo tengo este comandito ya preparado voy a darle al enter y esto lo que hace es que en mi equipo por el puerto 4646 pues me monta un servicio web Le voy a ponerlo por aquí localhost 4646 Bueno pues esto que estáis viendo por aquí es mi command and control Vale mi C2 que está corriendo en local en este equipo en cuestión La idea es que tú esté como en control lo puedes instalar en la nube en un vps por ejemplo en un servidor que por ahí disponible en línea y bueno tienes que configurar unas credenciales No yo ya las he seteado por tanto voy a poner mi usuario y contraseña te conectas y Bueno Este es tu panel de control principal en un principio yo no tengo ningún dispositivo conectado por tanto Vamos a darle activais y bien vamos a poner como nombre de dispositivo screencraft YouTube por ejemplo vale tipo de dispositivo como veis podéis conectar la gran mayoría de dispositivos de hack Five O sea que espectacular en mi caso obviamente pues screencrap es el que me interesa Y bien nombre descriptivo screencrap Demon por ejemplo no vamos a darle a the device para Añadir este nuevo dispositivo y bien ya con esto hecho si pinchas aquí te darás cuenta que al darle a Setup pues te pone Download no que te descargas Bueno si presionamos en Download os daréis cuenta de que me acabe de descargar un archivo device.com este archivo de configuración tienes que meterlo en la raíz de la Micro SD Card de esta forma pues le dirás al screen crack Cómo se va a conectar al command and Control pero claro para que el screencrap tenga conectividad con internet los datos tienes que conectarlo a un punto de acceso por tanto vamos a conectar la Micro SD Card y vamos a cambiar un archivo de configuración Bueno ya acabo de conectar de vuelta el cacharro voy a mover este archivo el device.confic que me he descargado a la raíz y bien aislado esto el archivo config Ahora tiene que tener una estructura como esta vale Yo ya lo he puesto tienes que poner WiFi ssid el nombre de la red inalámbrica entre doble comillas a la que quieres que se conecte tiene que estar en el alcance obviamente y en el campo WiFi pues la contraseña de la red inalámbrica vale es un punto de acceso temporal que me he montado luego lo quito por tanto bueno simplemente guárda texto y ya ahora lo que toca es la Micro SD Card desconectarla meterla en el screencrap setear todo el laboratorio con el sistema de cableado correspondiente y ver qué pasa Bueno antes que nada como sabremos que se ha conectado un nuevo cliente fijaros que en uptime history no vemos que haya ningún cliente conectado No de hecho online client 0 Bueno pues cuando se conecte veremos aquí lo más probable un piquito para arriba vale Así que nada vamos a conectarlo bien pues fijaros acabo de conectarse a un cliente ahí veo que ha habido una conexión aquí en online clients me pone que es cero no sé por qué pero se acaba de conectar un dispositivo vamos a irnos a configuration y bien

veis Esto de streaming images y streaming no yo aquí ahora mismo en mi pantalla izquierda tengo esto que como lo estoy moviendo Supongo que se verá aquí en breve un cambio aquí la foto se hacían Cada cuánto cada 10 segundos pone vamos a bajar esto a 5 segundos Vamos a darle capture de duplication Vamos a darle a save changes y vale fijaros Ahí está no voy a abrirme por ejemplo el bloc de notas voy a poner esto a mi izquierda y a ver si puedo ver ahora esto a la izquierda tarda 5 segunditos o algo así más o menos en actualizarse Ahí está fijaros No si escribo Ahora aquí a la izquierda Esto es una prueba tarda un poco en actualizarse Pero bueno veremos ahora que se actualiza por aquí Ahí está Esto es una prueba bueno medio a tiempo real no O sea que tú no tienes que estar desconectando la screencrap Y de forma remota en tu cámara en control pues lo ves además tienes un montón de configuraciones aquí puedes aplicar por tanto Bueno lo chulo como tal obviamente es eso no usar el comandant control lo tienes todo centralizado y Claro tú puedes conectar aquí que si el cake croc que si el share Jack que lo tocaremos y tienes aquí en tu cámara en control Pues todos los dispositivos centralizados para jugar con el que te apetezca así que bueno Esto es todo para el screencraft como veis un dispositivo bastante bastante potente Y claro imaginaros que tenemos el Screen crack conectado para ver la pantalla de la víctima pero también tenemos el key croc conectado para poder registrar todas las pulsaciones del teclado en tiempo real Lo tendríamos al usuario rotos Porque podríamos saber todo lo que está haciendo y nada La verdad es que estos cacharros están bastante bien Lo único son muy caros este cacharro que creo que nos lo dije en la web de hack Five está por 200 dólares La verdad es que se pasan un poco para lo que es en cuanto a tema de precio Yo creo que es más por el renombre de la marca que otra cosa Eso es lo que pagas hay una cosa que no os dije Y esto es importante porque igual no funciona al lado del HDMI veréis que hay una pequeña ranura que es un USB c Bueno pues tenéis que tenerlo conectado a la corriente porque de por a través de los HDMI Esto no se alimenta de nada tenéis que además Pues eso conectarle un USB c conectado a una toma de corriente para que esto tenga energía Y a partir de ella pues todo te va a funcionar te va a mostrar la pantalla y todo correcto Así que eso para que lo tengáis en cuenta no vaya a ser que lo conectéis los HDMI y veáis que la pantalla pues no se ve y Bueno pues poco más para este vídeo Espero que os haya gustado dejado un like ahí si os ha molado esta sección de Hardware hacking hacía tiempo que no traíamos un dispositivo Y bueno pues Próximamente a ver si podemos traer este otro el flipper 0 le tengo unas ganas tremendas Pero bueno hay que estudiarlo es un aparato muy muy extenso y complejo Pero bueno pronto espero que os vaya todo bien que estéis ahí aprobando esos exámenes que creo que estáis de temporada de examen y poco más nos vemos en el siguiente vídeo un saludo chao