El ARMA FAVORITA de los HACKERS | Rubber Ducky

si os muestro estos dos dispositivos puede parecer de primeras que la única diferencia entre estos dos pendrives está en el color no Uno es negro y el otro es de color azul de hecho podríais llegar a pensar que la función que ambos cumplen es la misma la de almacenar información para llevar los datos de un ordenador a otro de forma sencilla sin embargo si los abrimos para mirar un poco los componentes internos enseguida nos percatamos de que el de color negro cuenta con una estructura un tanto diferente al de color azul además de contar con una tarjeta de memoria flash extraíble la cual misteriosamente podemos extraer pues chavales hoy vamos a estar hablando del arma favorita de los hackers el USB raveldaki un dispositivo de ciberataque tan popular que ha llegado a aparecer en series de hackers muy conocidas como Mr robot donde se ve como de conectarlo a un equipo se puede llegar a tensar la cosa bastante fuerte hoy vamos a estar analizando un poco este cacharro con el objetivo de determinar su alcance y sobre todo entender el impacto de lo que puede llegar a suponer que este dispositivo se ha conectado tanto en un entorno empresarial como en un equipo personal luego estoy mucho más en breve pero primero que nada un mensajito ahí de nuestro sponsor wondershare Wonder Cherry cover it es la herramienta más efectiva del mercado para recuperar todo tipo de archivos en pocos minutos de forma rápida y sencilla con Wonder puedes recuperar fácilmente todos los archivos borrados tanto de tu ordenador como de un dispositivo externo ya sea un pendrive o una tarjeta SD entre otra entre los productos destacados una vez te instalas la herramienta Contamos con esta primera función la cual nos permite escanear nuestro dispositivo para obtener una vista previa de los archivos que encuentre antes de recuperarlos por otro lado tendríamos la función de recuperación de archivos para ordenadores que cuenten con fallos en el sistema de forma que en caso de que veas que tu ordenador se encuentre bloqueado o tenga fallas te permiten crear una unidad USB de arranque a través de la cual poder acceder a todos tus datos Y por último una función de recuperación avanzada de vídeos donde podréis escanear y recopilar vídeos corruptos de calidad Ultra HD 4k y 8k garantizando que la gran mayoría puedan ser incluido aquellos que hayan sufrido de daños accidentales en ciertos fragmentos para que veáis una prueba en mi caso voy a borrar el contenido de este directorio donde tengo un documento PDF bastante importante que voy a tratar de recuperar una vez borrado voy a asegurarme de haberlo eliminado también de la papelera de reciclaje y ya en este punto entraría en juego la herramienta recovery dado que en este caso es una carpeta concreta lo que quiero analizar vamos a pinchar en seleccionar carpeta Vamos a darle la ruta de la carpeta y ya en este punto vamos a esperar a ver si me recupera el documento PDF que acabo de borrar como veis ahí nos lo está mostrando en la previsualización y ya en este punto podemos recuperarlo para volverlo a tener accesible en la descripción de este vídeo os compartiremos un enlace de descarga del Software recovery donde podréis utilizarlo y recuperar hasta un máximo de 100 megas de forma gratuita Muchas gracias a gundershare por patrocinar este vídeo y ahora continuemos con el vídeo de hoy un Rover de aquí podríamos decir que no es más que un pendrive modificado es un Hardware creado por have Five el cual simula ser un pendrive pero en realidad por detrás Es una herramienta la cual inyecta pulsaciones de teclado Qué quiere decir con esto cuando tú conectas el pendrive al ordenador este es reconocido como un Driver ADN de esta forma el pendrive es detectado por el sistema como un teclado normal claro para no levantar sospechas y evitar que se ha bloqueado por el antivirus o el firewall ejecutando a

posteriori todas las teclas que le hayas cargado a nivel de código y sé lo que te puedes estar preguntando dirá Oye Tito salí y como de complicado es el meter instrucciones en un cacharro como este no bien pues Acompáñame suponer el siguiente escenario práctico esto de aquí es una máquina Windows 10 esta máquina corresponde a la máquina victima la cual vamos a tratar de comprometer empleando este dispositivo de aquí vale el ravelda aquí por otro lado tendríamos esto de aquí una máquina Linux la cual va a actuar como la máquina de atacante la idea de lo que pretendemos hacer en este ejercicio es la siguiente esto de aquí es mi máquina Linux de atacante y esto de aquí es la máquina Windows victima No desde mi máquina Linux voy a estar estar compartiendo un recurso malicioso el cual pretendo ejecutar desde la máquina Windows este recurso lo voy a estar compartiendo a través de un servicio http que me voy a montar por el puerto 80 por otro lado en la misma máquina de atacante lo que voy a hacer es que me voy a poner en escucha con netcat una herramienta de red por el puerto 443 en espera de recibir datos estos datos van a corresponder Ni más ni menos que a una consola interactiva que desde la máquina victima me voy a enviar a mi máquina de atacante todo esto a través de la ejecución de una Script en Power shell que voy a ejecutar desde la máquina victima el cual Estoy compartiendo justamente por el servicio http tras su ejecución Pues debería de ganar acceso al sistema y ya lo deberíamos de tener comprometido claro todo esto es muy bonito pero tenemos un pequeño inconveniente Y es que esta máquina cuenta con el Windows defender habilitado de forma que de Cara a la ejecución de nuestro Script malicioso lo más probable es que el defender nos chape ahí nos bloquee por tanto tendríamos que buscar alguna forma de mediante el empleo de este dispositivo del Rover de aquí Deshabilitar por un defender y por otro lado allá Pues ejecutar finalmente nuestro Script para ganar acceso al sistema Cómo podríamos hacer esto Bueno tú tienes que pararte a pensar en todo momento que esto es un teclado de forma que tú como atacante lo que tendrías que tratar de probar es ver de qué forma mediante el empleo de atajos de teclado Deshabilitar por un lado el defender y ya por otro lado pues cargar nuestra instrucción maliciosa a mí por ejemplo lo que se me ocurre para Deshabilitar el defender sería ser un control escape Esto me abre esta parte de aquí si escribo PR ahí vemos esto de protección antivirus y contra amenazas Vamos a darle al enter todo esto con el teclado La idea es no utilizar el ratón bueno la idea sería bajar hasta donde pone administrar la configuración Cómo podríamos hacer esto tap tap tap tap espacio y ya con eso ahí estamos en la parte que me interesa que es donde vamos a Deshabilitar pues cada una de estas cositas para Deshabilitar cada uno de estos botoncitos simplemente con el espacio ahí lo estamos deshabilitando y bueno Yo como el usuario que tengo es el único usuario del sistema y es administrador por defecto tu usuario si tú haces clic derecho ejecutar como administrador te sale esto típico le das que sí y ya está No pues yo voy a hacer izquierda espacio y ya está deshabilitado y ahora pues tap espacio tap espacio tap tap espacio y creo que ya está esto lo voy a mirar con el ratón pero creo que ya no hay más efectivamente ahora la idea sería cerrar esta ventana que solo puedes hacer con alt F4 y ya por último con Windows r la idea sería en este recuadro que vemos por ahí abajo cargar nuestra instrucción maliciosa en Power shell por tanto ya sabríamos que atajos de teclado tendríamos que utilizar para Deshabilitar por un lado el defender y ya luego pues ejecutar nuestra instrucción maliciosa no Cabe destacar que todo esto se podría hacer perfectamente con powershell eh que ya vio en los comentarios Oye pero esto no más rápido con power shield sí obviamente lo sé pero es para que veáis sobre todo el impacto de todo lo que puedes hacer con este cacharro que tienes ahí movilidad absoluta bien pues lo que vamos a hacer es que nos vamos a dirigir a la web de Duck toolkit.com en este caso me voy a dirigir a la pestañita

encoder y es aquí en este punto donde vamos a inyectar todas las instrucciones que queremos que sean ejecutadas del lado del raveldaki obviamente yo esto ya lo ha ido puliendo poco a poco antes de hacer el y todas las instrucciones que voy a cargar son estas que estamos viendo por aquí os voy a hacer un poquito más de zoom y vamos a ir comentando rápidamente cada cosa que es lo que hace bueno esto que estamos viendo las dos primeras líneas de Rem no es más que una forma de indicar un comentario esto no va a ser interpretado y es una forma de nosotros tener como una pequeña traza para saber qué va a pasar en este punto posteriormente esto de delay mil lo único que hace referencia es a que cuando inyecte el USB quiero que espere un segundo antes de arrancar con el resto de instrucciones esto es una buena práctica porque en ocasiones si lo conectas y empiezas ya a meterle todas las instrucciones hay veces que las primeras no te las interpretan posteriormente Pues ejecutaríamos el atajo control escape que recordad que esto En primera instancia lo que hacía era abrirnos una ventanita abajo a la izquierda donde luego introducir los caracteres PR y obviamente después le daríamos al enter no en este punto esperaríamos un segundo Por si acaso para que se nos abran todas las ventanas correspondientes y luego ejecutaríamos 4 taps una vez hecho al hacer tap tap tap tap le daríamos al enter y ya estando en la sección correspo donde vamos a poder Deshabilitar el defender tendríamos que presionar la tecla espacio de la nueva ventana que se nos Abre Tendremos que darle a la izquierda y luego al enter y ya posteriormente Deshabilitar el resto de opciones con tap espacio tap espacio espacio dos tabs espacio y ya alt F4 para cerrar la ventana ya en este punto Pues bueno con Wii r estaríamos haciendo Windows r para abrir esa ventanita donde cargar nuestra instrucción en Power shell y este Comalito de Power shell lo que se va a encargar tú con la palabra String le dice qué caracteres quieres introducir y yo quiero cargar toda esta instrucción especialmente diseñada la cual se va a encargar de digamos interpretar un recurso el cual estoy yo compartiendo en mi servicio http que es esto de aquí el ps1 este recurso para que veáis en qué consiste es esto de aquí un Script de Power shell que en la última línea va a estar inyectando esta instrucción que es la que me va a enviar una consola interactiva a mi IP de atacante por el puerto 443 por tanto yo lo que tendría que hacer es por un lado para ofrecer este recurso a nivel de Red porque la máquina Windows en este caso con la misma red que yo si fuera un equipo externo habría que hacerlo a través de un servidor o algo que tengas montado en la nube pues yo me voy a montar un servidor Http con python por el puerto 80 de esta forma tengo una página web un servidor web que me ofrece el recurso el cual tengo por aquí el PS punto ps1 que es el que quiero que la máquina victima me ejecute por otro lado La idea es que voy a cargar una instrucción para Connect Cat ponerme en el puerto 443 porque justamente aquí donde voy a ganar acceso al sistema algo importante destacar es que dado que el teclado es español hay que darle en la parte de Language a Spain tenemos que seleccionar esta opción dado que de lo contrario Es probable que ciertos caracteres especiales como paréntesis comillas y demás no nos carguen una vez hecho le damos a encode Pay loot le damos a aceptar y nos descargamos estos dos archivitos el inject punto bim y el duki code.xt estos dos archivos van a ser los que vamos a tener que meter aquí dentro la idea una vez llegados a este punto es retirar la Micro SD Card que está contenida dentro del ravelda aquí para en mi caso introducirla en un dispositivo como esto que es un all in one para que así al conectarlo este tipo me pille este medio yo por ejemplo acabo de conectarlo al equipo y ahora en cuestión de unos instantes debería de salir una nueva unidad lógica que creo que se llama e esta de aquí ravelda aquí y hoy en el rabberdaki tengo metidos estos dos archivos que tenía de antes pero los voy a eliminar y voy a meter los nuevos lo que voy a hacer simplemente es arrastrar el

inject punto bim y el duki code punto txt a esto de aquí una vez hecho desconectamos la Micro SD Card desde este dispositivo el all in one para volverlo nuevamente a conectar al raw verdad aquí y yang cápsularlo todo para prepararlo de cara al ataque bien pues Vamos a ponernos en situación Esta es la máquina Windows que pretendo comprometer como atacante no ya sabéis que yo por aquí estoy en escucha por el puerto 443 de forma que aquí abajo es donde voy a ganar acceso al sistema una vez se ejecuten todas las instrucciones que he definido en el rabel de aquí esto es una máquina Windows hay un usuario he visto que se ha levantado se ha ausentado al baño yo todo Sinvergüenza le cuelo el rabel de Aquí vamos a ver si funciona Ahí está yo no estoy haciendo nada ahí está está bajando la configuración Desactiva la protección en tiempo real edad perfecto baja lo quita lo quita dos tabs será esto quita listo lo cierra y ahora fijaros que rápido va a ejecutar la instrucción Ahí está y chimpum si todo ha ido bien por aquí Ahí está fijaros Juan ahí John doe que es el supuesto usuario que hemos comprometido en este caso Y si hacemos un ipeconfic fijaros que estamos en la 111 41 que si tú te vienes por aquí a la máquina Windows y haces un cmd y un ipconcic fijaros que es la 111.41 la misma IP que la que hemos comprometido por tanto el usuario John doe ha sido full owneado bueno chavales acabáis de presenciar con vuestros propios ojos como se puede llegar a tensar en cuestión de segundos con esto con un pendrive Cabe destacar que todo esto lo hemos realizado en un entorno controlado vale Ya de que no haber sido así y haberlo hecho en un equipo sin consentimiento obviamente habría sido ilegal por tanto cuidado ahí donde practicáis eh la prueba que hemos hecho ha sido bastante sencillita pero la idea es que entendáis el concepto y que esto lo podéis extrapolar hasta donde queráis la podéis utilizar para descargar malware para hacer un montón de cosas por tanto hay que tener mucho cuidado y por ello vamos a comentar unas medidas mitigadoras bueno por un lado sentido común nunca dejéis un ordenador desbloqueado a manos de cualquier persona de una extraña porque en caso de estar desbloqueado vete tú a saber si hay un hacker ahí de potencia máxima a tu alrededor y aprovecha la ocasión y te conecta y el raberd de aquí por otro lado otra práctica común a destacar es que los atacantes normalmente dispositivos como estos lo que suelen hacer es en las empresas dejar los botados en el suelo de esta forma si pones por ejemplo una etiqueta por aquí que ponga nudes o facturas o lo que corresponda algo llamativo que incita al usuario conectarlo en el equipo de empresa pues claro ya se puede llegar a tensar Por tanto la otra medida a tener en cuenta es todo sentido común no conectes dispositivos o pendrives que no sean tuyas porque a saber lo que estás conectando en tu equipo Por otra parte en una de las acciones que habíamos hecho en la máquina Windows al hacer un control escape y escribir PR para lo de protección de antivirus y contra amenazas al darle aquí a administrar la configu al tu pinchar aquí me sale esto no Claro mi usuario es el único que hay en el sistema no hay más usuarios y ni usuarios administrador por defecto esto normalmente es así tu propio usuario personal le das así y ya está si no quieres que esto sea así para que te pida una contraseña que yo creo que eso es más robusto hay que hacer una cosa vamos a hacer un Windows r vamos a escribir regedit Vamos a darle aquí a Sí hemos retocar esto de aquí donde pone consent from behavior admin está en toda esta ruta que veis por aquí la veis por ahí arriba HK y local Machine software Microsoft Windows curen de version policis y System pues una vez habíais llegado a el que nos interesa que es esto de System pincháis y en concept from the behavior admin escribir un 1 al darle a aceptar Y cerrar todo esto ahora de Cara a volver a hacer lo mismo si tú escribes por aquí por ejemplo PR te abres esto y en la parte de administrar la configuración haces esto te pido una contraseña de forma que si es incorrecta No va a avanzar hasta que la escribas Pues de forma correcta se desbloquea esto es mucho mejor y

Bueno chavales pues poco más revisando este dispositivo el rap verdad y lo dicho esto se puede llegar a tensar hasta niveles desorbitados pero eso ya os lo dejo a vosotros Dejad un comentario indicando Si os ha gustado el vídeo y deciros que si este vídeo llega a 10.000 likes vamos a estar analizando otro dispositivo similar al rabel de aquí pero más potente el Bugs Bunny con este cacharro vamos a poder hacer muchas más cosas y se va a tensar la cosa que te cagas poco más para el vídeo de hoy Espero que todo vaya bien y nos vemos en el siguiente vídeo un saludo chao